Standar Nasional Indonesia

SNI ISO/IEC 27002:2022
(Ditetapkan oleh BSN tahun 2022)

Keamanan informasi, keamanan siber, dan proteksi privasi — Kontrol keamanan informasi

Information security, cybersecurity and privacy protection — Information security controls

(ISO/IEC 27002:2022, IDT)

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

ICS 35.030

BADAN STANDARDISASI NASIONAL

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

© ISO/IEC 2022 – All rights reserved
© BSN 2022 untuk kepentingan adopsi standar © ISO/IEC menjadi SNI – Semua hak dilindungi

Hak cipta dilindungi undang-undang. Dilarang mengumumkan dan memperbanyak sebagian atau seluruh isi dokumen ini dengan cara dan dalam bentuk apapun serta dilarang mendistribusikan dokumen ini baik secara elektronik maupun tercetak tanpa izin tertulis BSN

BSN
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Daftar Isi

Daftar Isi i
Prakata iv
Pendahuluan v
1 Ruang lingkup 1
2 Rujukan normatif 1
3 Istilah, definisi, dan singkatan 1
3.1 Istilah dan definisi 1
3.2 Singkatan 7
4 Struktur dokumen ini 8
4.1 Pasal 8
4.2 Tema dan atribut 8
4.3 Tata letak kontrol 9
5 Kontrol organisasi 10
5.1 Kebijakan keamanan informasi 10
5.2 Peran dan tanggung jawab keamanan informasi 12
5.3 Segregasi tugas 13
5.4 Tanggung jawab manajemen 14
5.5 Kontak dengan otoritas 15
5.6 Kontak dengan kelompok kepentingan khusus 15
5.7 Intelijen ancaman 16
5.8 Keamanan informasi dalam manajemen proyek 17
5.9 Inventori informasi dan aset terkait lainnya 19
5.10 Penggunaan yang akseptabel dari informasi dan aset terkait lainnya 21
5.11 Pengembalian aset 22
5.12 Klasifikasi informasi 23
5.13 Pelabelan informasi 24
5.14 Transfer informasi 26
5.15 Kontrol akses 28
5.16 Manajemen identitas 30
5.17 Informasi autentikasi 31
5.18 Hak akses 33
5.19 Keamanan informasi dalam hubungan pemasok 34
5.20 Menangani keamanan informasi dalam perjanjian pemasok 36
5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK 38
5.22 Pemonitoran, reviu, dan manajemen perubahan layanan pemasok 40
5.23 Keamanan informasi untuk penggunaan layanan *cloud* 41
5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi 43
5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi 45
5.26 Respons terhadap insiden keamanan informasi 46
5.27 Belajar dari insiden keamanan informasi 47
5.28 Pengumpulan bukti 47

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.29 Keamanan informasi selama disrupsi 48
5.30 Kesiapan TIK untuk kontinuitas bisnis 49
5.31 Persyaratan legal, statutori, regulatori, dan kontraktual 51
5.32 Hak kekayaan intelektual 52
5.33 Proteksi rekaman 53
5.34 Privasi dan proteksi PII 55
5.35 Reviu independen terhadap keamanan informasi 56
5.36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi 57
5.37 Prosedur operasi terdokumentasi 58
6 Kontrol orang 59
6.1 Skrining 59
6.2 Syarat dan ketentuan ketenagakerjaan 60
6.3 Kesadaran, pendidikan, dan pelatihan keamanan informasi 61
6.4 Proses kedisiplinan 63
6.5 Tanggung jawab setelah terminasi atau perubahan pekerjaan 64
6.6 Perjanjian konfidensialitas atau nirungkap 65
6.7 Telekarya (*Remote working*) 66
6.8 Pelaporan peristiwa keamanan informasi 67
7 Kontrol fisik 68
7.1 Perimeter keamanan fisik 68
7.2 Entri Fisik 69
7.3 Mengamankan kantor, ruangan, dan fasilitas 71
7.4 Pemonitoran Keamanan fisik 71
7.5 Memproteksi dari ancaman fisik dan lingkungan 72
7.6 Bekerja di area aman 74
7.7 Meja bersih dan layar bersih 74
7.8 Penempatan dan proteksi peralatan 75
7.9 Keamanan aset di luar premis 76
7.10 Media penyimpanan 77
7.11 Utilitas pendukung 79
7.12 Keamanan perkabelan 79
7.13 Pemeliharaan peralatan 80
7.14 Pemusnahan atau penggunaan kembali peralatan dengan aman 81
8 Kontrol teknologi 82
8.1 Perangkat titik akhir pengguna 82
8.2 Hak akses privilese 84
8.3 Pembatasan akses informasi 86
8.4 Akses ke kode sumber 87
8.5 Autentikasi aman 88
8.6 Manajemen kapasitas 90
8.7 Proteksi terhadap perangkat perusak 91
8.8 Manajemen kerentanan teknis 93
8.9 Manajemen konfigurasi 96
8.10 Penghapusan informasi 98

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.11 Penyamaran (*masking*) data 100
8.12 Pencegahan kebocoran data 101
8.13 Pencadangan informasi 103
8.14 Redundansi fasilitas pemrosesan informasi 104
8.15 Membuat log 106
8.16 Pemonitoran aktivitas 108
8.17 Sinkronisasi jam 110
8.18 Penggunaan program utilitas privilese 111
8.19 Instalasi perangkat lunak pada sistem operasional 112
8.20 Keamanan jaringan 113
8.21 Keamanan layanan jaringan 114
8.22 Segregasi jaringan 115
8.23 Pemfilteran web 116
8.24 Penggunaan kriptografi 117
8.25 Siklus hidup pengembangan yang aman 119
8.26 Persyaratan keamanan aplikasi 120
8.27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman 122
8.28 Pengkodean yang aman 124
8.29 Pengujian keamanan dalam pengembangan dan penerimaan 126
8.30 Pengembangan yang dialihdayakan 128
8.31 Pemisahan lingkungan pengembangan, uji, dan produksi 129
8.32 Manajemen perubahan 130
8.33 Informasi uji 131
8.34 Proteksi sistem informasi selama pengujian audit 132
Lampiran A (Informatif) Penggunaan atribut 134
A.1 Umum 134
A.2 Pandangan organisasi 147
Lampiran B (informatif) Padanan ISO/IEC 27002:2022 (dokumen ini) dengan ISO/IEC 27002:2013 148
Bibliografi 156

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Prakata

Standar Nasional Indonesia (SNI) ISO/IEC 27002:2022 dengan judul Keamanan informasi, keamanan siber, dan proteksi privasi — Kontrol keamanan informasi, merupakan adopsi identik dari ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls,* dengan metode terjemahan dua bahasa. Standar ini merupakan revisi dari SNI ISO/IEC 27002:2014, Teknologi informasi – Teknik keamanan – Panduan praktik kendali keamanan informasi (ISO/IEC 27002:2013, IDT) dan SNI ISO/IEC 27002:2014/Corr. 1:2016, Teknologi informasi – Teknik keamanan – Petunjuk praktik kendali keamanan informasi (RALAT1) (ISO/IEC 27002:2013/Corr. 1:2014, IDT).

Standar ini disusun oleh Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi. Standar ini telah dibahas dan disetujui dalam rapat konsensus nasional di Jakarta pada tanggal 11 Oktober 2022. Konsensus tersebut dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah.

Standar ini telah melalui tahap jajak pendapat pada tanggal 25 Oktober 2022 sampai dengan 24 November 2022 dengan hasil akhir disetujui menjadi SNI.

Tidak terdapat standar ISO/IEC yang digunakan sebagai acuan dalam standar ini.

Kosakata yang digunakan dalam standar ini mengikuti bentuk baku yang dicantumkan dalam Kamus Besar Bahasa Indonesia (KBBI), tetapi ada beberapa kosakata yang belum ada di dalam KBBI.

Untuk satu kata yang sama, terjemahan yang digunakan dalam standar ini dapat berbeda dengan terjemahan yang digunakan dalam standar lain. Terjemahan yang berbeda tersebut antara lain:

a) *control* diterjemahkan menjadi “kontrol” dalam standar ini dan menjadi “pengendalian” dalam standar lain;
b) *disruption* diterjemahkan menjadi “disrupsi” dalam standar ini dan menjadi “gangguan” dalam standar lain;
c) *record* diterjemahkan menjadi “rekaman” dalam standar ini dan menjadi “arsip” dalam standar lain;
d) *review* diterjemahkan menjadi “reviu” dalam standar ini dan menjadi “tinjauan” dalam standar lain.

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari dokumen standar ini dapat berupa hak paten. Badan Standardisasi Nasional tidak bertanggung jawab untuk pengidentifikasian salah satu atau seluruh hak paten yang ada.

Apabila pengguna menemukan keraguan dalam standar ini, disarankan untuk melihat standar aslinya yaitu ISO/IEC 27002:2022 (E) dan/atau dokumen terkait lain yang menyertainya.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pendahuluan

0.1 Latar belakang dan konteks

Dokumen ini dirancang untuk organisasi dari semua tipe dan ukuran. Dokumen ini dapat digunakan sebagai referensi untuk menentukan dan mengimplementasikan kontrol penanganan risiko keamanan informasi dalam sistem manajemen keamanan informasi (SMKI) berdasarkan ISO/IEC 27001. Dokumen ini juga dapat digunakan sebagai dokumen panduan untuk organisasi dalam menentukan dan mengimplementasikan kontrol keamanan informasi yang diterima secara umum. Selanjutnya, dokumen ini dimaksudkan untuk digunakan dalam mengembangkan pedoman manajemen keamanan informasi untuk industri dan organisasi spesifik, dengan mengambil konsiderasi lingkungan risiko keamanan informasi khusus industri dan organisasi spesifik tersebut . Pengendalian organisasi atau lingkungan spesifik selain yang termasuk dalam dokumen ini dapat ditentukan melalui asesmen risiko jika diperlukan.

Organisasi dari semua tipe dan ukuran (termasuk sektor publik dan privat , komersial dan tanpa profit) membuat, mengumpulkan, memproses, menyimpan, mengirimkan, dan memusnahkan informasi dalam berbagai bentuk, termasuk elektronik, fisik, dan verbal (misalnya percakapan dan presentasi).

Nilai informasi lebih dari kata-kata tertulis, angka, dan gambar: pengetahuan, konsep, ide, dan merek adalah contoh bentuk yang tidak berwujud dari informasi. Dalam dunia yang saling terhubung, informasi dan aset terkait lainnya layak atau mensyaratkan proteksi dari berbagai sumber risiko, baik natural , sengaja, atau tidak sengaja.

Keamanan informasi dicapai dengan mengimplementasikan serangkaian kontrol yang cocok , termasuk kebijakan, aturan, proses, prosedur, struktur organisasi dan fungsi perangkat lunak dan perangkat keras. Untuk memenuhi sasaran keamanan dan bisnis spesifiknya, organisasi sebaiknya mendefinisikan, menerapkan, memonitor, mereviu , dan meningkatkan kontrol ini jika diperlukan. SMKI seperti yang ditentukan dalam ISO/IEC 27001 mengambil pandangan holistik dan terkoordinasi tentang risiko keamanan informasi organisasi untuk menentukan dan mengimplementasikan serangkaian kontrol keamanan informasi yang komprehensif dalam kerangka keseluruhan sistem manajemen yang koheren.

Banyak sistem informasi, termasuk manajemen dan operasinya, belum dirancang agar aman dalam hal SMKI sebagaimana ditentukan dalam ISO/IEC 27001 dan dokumen ini. Level keamanan yang dapat dicapai melalui langkah-langkah teknologi saja adalah terbatas dan sebaiknya didukung oleh aktivitas manajemen dan proses organisasi yang tepat. Mengdentifikasi kontrol mana yang sebaiknya ada memerlukan perencanaan yang cermat dan perhatian terhadap detail saat melakukan penanganan risiko.

SMKI yang sukses membutuhkan dukungan dari semua personel dalam organisasi. Diperlukan juga partisipasi dari pihak lain yang berkepentingan, seperti pemegang saham atau pemasok. Saran dari pakar dapat juga diperlukan.

Suatu sistem manajemen keamanan informasi yang cocok, cukup, dan efektif memberikan keyakinan bagi manajemen organisasi dan pihak lain yang berkepentingan bahwa informasi dan aset terkait lainnya milik mereka telah disimpan dengan cukup aman dan terlindung dari ancaman dan bahaya, sehingga memberdayakan organisasi untuk mencapai sasaran bisnis yang dinyatakan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

0.2 Persyaratan keamanan informasi

Organisasi sangat perlu menentukan persyaratan keamanan informasinya. Ada tiga sumber utama persyaratan keamanan informasi:

a) asesmen risiko terhadap organisasi, dengan memperhitungkan strategi dan sasaran bisnis organisasi secara keseluruhan. Asesmen risiko ini dapat difasilitasi atau didukung melalui asesmen risiko spesifik keamanan informasi. Asesmen risiko spesifik keamanan informasi tersebut sebaiknya menghasilkan penetapan kontrol yang diperlukan untuk memastikan bahwa risiko residual bagi organisasi memenuhi kriteria penerimaan risikonya;
b) persyaratan hukum, statutori, regulatori, dan kontraktual yang sebaiknya dipatuhi oleh organisasi dan pihak yang berkepentingan (mitra dagang, penyedia layanan, dll.) dan lingkungan sosial budaya mereka;
c) seperangkat prinsip, sasaran, dan persyaratan bisnis dalam seluruh langkah dari siklus hidup informasi yang telah dikembangkan suatu organisasi untuk mendukung operasinya.

0.3 Kontrol

Sebuah kontrol didefinisikan sebagai suatu cara untuk memodifikasi atau memelihara risiko. Beberapa kontrol dalam dokumen ini adalah kontrol yang memodifikasi risiko, sementara yang lain memelihara risiko. Kebijakan keamanan informasi, sebagai contoh, hanya dapat memelihara risiko, sedangkan kepatuhan terhadap kebijakan keamanan informasi dapat memodifikasi risiko. Selain itu, beberapa kontrol menggambarkan cara generik yang sama dalam konteks risiko yang berbeda. Dokumen ini menyediakan bauran generik dari kontrol keamanan informasi organisasi, orang, fisik, dan teknologi yang berasal dari praktik terbaik yang diakui secara internasional.

0.4 Menentukan kontrol

Penentuan kontrol bergantung pada keputusan organisasi setelah asesmen risiko, dengan ruang lingkup yang telah didefinisikan dengan jelas. Keputusan terkait risiko yang teridentifikasi sebaiknya didasarkan pada kriteria penerimaan risiko, opsi penanganan risiko, dan pendekatan manajemen risiko yang diterapkan oleh organisasi. Penentuan kontrol sebaiknya mengambil regulasi semua legislasi dan regulasi nasional dan internasional yang relevan. Penentuan kontrol juga bergantung pada bagaimana berbagai kontrol saling berinteraksi satu sama lain untuk memberikan pertahanan secara menyeluruh.

Organisasi dapat mendesain kontrol sesuai yang dipersyaratkan atau mengidentifikasinya dari sumber manapun. Dalam melakukan spesifikasi kontrol tersebut, organisasi sebaiknya mempertimbangkan sumber daya dan investasi yang dibutuhkan untuk mengimplementasikan dan mengoperasikan kontrol dibandingkan dengan nilai bisnis yang direalisasikan. Lihat ISO/IEC TR 27016 untuk panduan tentang keputusan mengenai investasi dalam SMKI dan konsekuensi ekonomi dari keputusan tersebut dalam konteks berbagai persyaratan untuk sumber daya.

Sebaiknya terdapat keseimbangan antara sumber daya yang digelar untuk mengimplementasikan kontrol dan potensi dampak bisnis yang dihasilkan dari insiden keamanan dengan tidak adanya kontrol tersebut. Hasil asesmen risiko sebaiknya membantu memandu dan menentukan tindakan manajemen yang tepat, prioritas untuk memanajemeni risiko keamanan informasi dan untuk mengimplementasikan kontrol yang dianggap perlu untuk memproteksi dari risiko tersebut .

Beberapa kontrol dalam dokumen ini dapat dianggap sebagai prinsip pemandu untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

manajemen keamanan informasi dan berlaku untuk sebagian besar organisasi. Informasi lebih lanjut tentang penentuan kontrol dan pilihan penanganan risiko lainnya dapat ditemukan di ISO/IEC 27005.

0.5 Mengembangkan pedoman organisasi spesifik

Dokumen ini dapat dianggap sebagai titik awal untuk mengembangkan pedoman organisasi spesifik . Tidak semua kontrol dan panduan dalam dokumen ini dapat berlaku untuk semua organisasi. Kontrol dan pedoman tambahan yang tidak termasuk dalam dokumen ini juga mungkin diperlukan untuk mengatasi kebutuhan spesifik organisasi dan risiko yang telah diidentifikasi. Saat mengembangkan dokumen yang berisi pedoman atau kontrol tambahan, memasukkan referensi silang terhadap pasal dalam dokumen ini dapat berguna untuk rujukan di masa mendatang.

0.6 Konsiderasi siklus hidup

Informasi memiliki siklus hidup, mulai dari pembuatan hingga pemusnahan . Nilai dari dan risiko terhadap informasi dapat beragam sepanjang siklus hidup tersebut (misalnya pengungkapan yang takberhak atau pencurian akun finansial perusahaan tidak signifikan setelah dipublikasikan, tetapi integritas tetap kritis) oleh karena itu, keamanan informasi tetap penting sampai batas tertentu di semua tahap.

Sistem informasi dan aset lain yang terkait dengan keamanan informasi memiliki siklus hidup dimana informasi dan aset tersebut dikumpulkan, dispesifikasikan, didesain dikembangkan, diuji, diimplementasikan, digunakan, dipelihara, dan akhirnya dihentikan dari layanan dan dimusnahkan. Keamanan informasi sebaiknya dipertimbangkan pada setiap tahap. Proyek pengembangan sistem baru dan perubahan pada sistem yang ada memberikan kesempatan untuk meningkatkan kontrol keamanan sambil mempertimbangkan risiko organisasi dan pelajaran yang diperoleh dari insiden.

0.7 Standar Internasional Terkait

Meskipun dokumen ini menawarkan panduan dalam cakupan yang luas tentang berbagai kontrol keamanan informasi yang umum diterapkan di banyak organisasi yang berbeda, dokumen lain dalam keluarga ISO/IEC 27000 memberikan saran pelengkap atau persyaratan tentang aspek lain dari keseluruhan proses memanajemeni keamanan informasi.

Untuk pengenalan umum tentang SMKI dan keluarga dokumen tersebut dapat merujuk ke ISO/IEC 27000. ISO/IEC 27000 menyediakan kosa kata, yang mendefinisikan sebagian besar istilah yang digunakan di seluruh keluarga dokumen ISO/IEC 27000, dan menjelaskan ruang lingkup dan sasaran untuk setiap anggota keluarga.

Terdapat standar sektor spesifik yang memiliki kontrol tambahan yang bertujuan untuk menangani area spesifik (misalnya ISO/IEC 27017 untuk layanan *cloud*, ISO/IEC 27701 untuk privasi, ISO/IEC 27019 untuk energi, ISO/IEC 27011 untuk organisasi telekomunikasi, dan ISO 27799 untuk kesehatan). Standar tersebut tertera dalam Bibliografi dan beberapa di antaranya dirujuk dalam bagian panduan dan informasi lainnya dalam Pasal 5 - 8

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Keamanan informasi, keamanan siber, dan proteksi privasi — Kontrol keamanan informasi

1 Ruang lingkup

Dokumen ini menyediakan serangkaian rujukan kontrol keamanan informasi generik termasuk panduan implementasi. Dokumen ini didesain untuk digunakan oleh organisasi:

a) dalam konteks sistem manajemen keamanan informasi (SMKI) berdasarkan ISO/IEC 27001;
b) untuk mengimplementasikan kontrol keamanan informasi berdasarkan praktik terbaik yang diakui secara internasional;
c) untuk mengembangkan pedoman manajemen keamanan informasi organisasi spesifik.

2 Rujukan normatif

Tidak ada rujukan normatif dalam dokumen ini.

3 Istilah, definisi, dan singkatan

3.1 Istilah dan definisi

Untuk tujuan dokumen ini, istilah dan definisi berikut berlaku.
ISO dan IEC memelihara basis data istilah untuk digunakan dalam standardisasi di alamat berikut:

— ISO *Online Browsing Platform* : tersedia di https://www.iso.org/obp
— IEC *Electropedia*: tersedia di https://www.electropedia.org/

3.1.1
kontrol akses
cara untuk memastikan bahwa akses fisik dan logikal ke aset (3.1.2) terotorisasi dan dibatasi berdasarkan persyaratan keamanan bisnis dan informasi

3.1.2
aset
segala hal yang memiliki nilai bagi organisasi
Catatan 1 untuk entri: Dalam konteks keamanan informasi, dapat dibedakan dua macam aset:

— aset utama:
  — informasi;
  — *proses* (3.1.27) dan aktivitas bisnis;
— aset pendukung (yang aset utama bergantung padanya) dari semua tipe, misalnya:
  — perangkat keras;
  — perangkat lunak;
  — jaringan;
  — *personel* (3.1.20);
  — situs;
  — struktur organisasi.

3.1.3
serangan
upaya takterotorisasi yang berhasil atau takberhasil untuk menghancurkan, mengubah, melumpuhkan, mendapatkan akses ke suatu aset (3.1.2) atau upaya apa pun untuk mengekspos, mencuri, atau menggunakan aset (3.1.2) secara takterotorisasi

3.1.4
autentikasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

pemberian keyakinan bahwa sebuah karakteristik yang diklaim dari suatu entitas (3.1.11) adalah benar

3.1.5
autentisitas
bahwa suatu entitas (3.1.11) sesuai dengan apa yang diklaimnya

3.1.6 rantai kustodi (*chain of custody*)
kepemilikan, pergerakan, penanganan, dan lokasi materi yang dapat ditunjukkan dari satu titik waktu ke titik waktu lainnya

Catatan 1 untuk entri: Materi mencakup informasi dan aset terkait lainnya (3.1.2) dalam konteks ISO/IEC 27002.

[SUMBER: ISO/IEC 27050 -1:2019, 3.1, dimodifikasi — "Catatan 1 untuk entri" ditambahkan]

3.1.7
informasi konfidensial
informasi yang tidak dimaksudkan untuk tersedia atau diungkapkan kepada individu, *entitas*, (3.1.11) atau *proses* (3.1.27) takterotorisasi

3.1.8
kontrol
tindakan yang memelihara dan/atau memodifikasi risiko

Catatan 1 untuk entri: kontrol termasuk, tetapi tidak terbatas pada, *proses* (3.1.27), *kebijakan* (3.1.24), perangkat, praktik, atau kondisi dan/atau tindakan apa pun yang mempertahankan dan/atau memodifikasi risiko.

Catatan 2 untuk entri: kontrol tidak selalu memberikan dampak memodifikasi yang dimaksudkan atau diasumsikan.

[SUMBER: ISO 31000:2018, 3.8]

3.1.9
disrupsi
insiden, baik yang terantisipasi maupun takterantisipasi, yang menyebabkan deviasi negatif takterencana terhadap penyampaian produk dan layanan yang diharapkan sesuai dengan sasaran organisasi

[SUMBER: ISO 22301:2019, 3.10]

3.1.10
perangkat titik akhir
perangkat keras teknologi informasi dan komunikasi (TIK) yang terhubung melalui jaringan

Catatan 1 untuk entri: Perangkat titik akhir dapat merujuk pada komputer *desktop*, laptop, ponsel pintar, tablet, *thin clients*, pencetak, atau perangkat keras khusus lain termasuk meteran cerdas dan peranti *Internet of Things* (IoT).

3.1.11
entitas
item yang relevab untuk tujuan pengoperasian suatu domain yang memiliki keberadaan khusus yang dapat dikenali
Catatan 1 untuk entri: Suatu entitas dapat berwujud fisik atau logikal.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

CONTOH Seseorang, organisasi, perangkat, sekelompok item, *subscriber* manusia suatu layanan telekomunikasi, kartu SIM, paspor, kartu antarmuka jaringan, aplikasi perangkat lunak, layanan atau situs web.

[SUMBER: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
fasilitas pemrosesan informasi
setiap sistem pemrosesan informasi, layanan atau infrastruktur , atau lokasi fisik yang menaunginya

[SUMBER: ISO/IEC 27000:2018, 3.27, dimodifikasi — "*facilities*" telah diganti dengan *facility*.]

3.1.13
pelanggaran keamanan informasi
pembobolan keamanan informasi yang mengarah pada kerusakan, kerugian, perubahan, pengungkapan, atau akses yang tidak diinginkan terhadap informasi terlindungi yang dikirimkan, disimpan, atau diproses

3.1.14
peristiwa keamanan Informasi
peristiwa yang mengindikasikan suatu kemungkinan *pelanggaran keamanan informasi* (3.1.13) atau kegagalan *kontrol* (3.1.8)

[SUMBER: ISO/IEC 27035-1:2016, 3.3, dimodifikasi — "*breach of information security*" telah diganti dengan "*information security breach*"]

3.1.15
insiden keamanan informasi
satu atau beberapa *peristiwa keamanan informasi* (3.1.14) terkait dan teridentifikasi yang dapat membahayakan *aset* (3.1.2) organisasi atau membobol operasinya

[SUMBER: ISO/IEC 27035-1:2016, 3.4]

3.1.16
manajemen insiden keamanan informasi
penerapan pendekatan yang konsisten dan efektif untuk penanganan *insiden keamanan informasi* (3.1.15)

[SUMBER: ISO/IEC 27035-1:2016, 3.5]

3.1.17
sistem informasi
seperangkat aplikasi, layanan, *aset* teknologi informasi (3.1.2), atau komponen lain penanganan informasi

[SUMBER: ISO/IEC 27000:2018, 3.35]

3.1.18
pihak berkepentingan
pemangku kepentingan
orang atau organisasi yang dapat memengaruhi, dipengaruhi, atau menganggap dirinya dipengaruhi oleh suatu keputusan atau aktivitas

[SUMBER: ISO/IEC 27000:2018, 3.37]

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3.1.19
nirsangkal
kemampuan untuk membuktikan terjadinya suatu peristiwa atau tindakan yang diklaim dan *entitas* (3.1.11) asalnya

3.1.20
person
orang-orang yang melakukan pekerjaan di bawah arahan organisasi.

Catatan 1 untuk entri: Konsep personel meliputi anggota organisasi, seperti penanggung jawab tata kelola manajemen puncak, pegawai, staf temporer, kontraktor, dan sukarelawan

3.1.21
informasi pengidentifikasi personal
personally identifiable information
PII
segala informasi yang (a) dapat digunakan untuk membangun hubungan antara informasi tersebut dengan orang perorangan yang terkait dengan informasi semacam itu, atau (b) terkait atau dapat dikaitkan secara langsung atau tidak langsung dengan orang perorangan.

Catatan 1 untuk entri: "Orang perorangan" dalam definisi ini adalah PII *principal* (3.1.22). Untuk menentukan apakah PII *principal* dapat teridentifikasi, sebaiknya diperhitungkan segala cara yang dapat digunakan secara wajar oleh pemangku kepentingan privasi yang memegang data, atau oleh pihak lain mana pun, untuk menetapkan hubungan antara seperangkat PII dan orang perseorangan tersebut.

[SUMBER: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22
PII *principal*
orang perorangan yang terkait dengan *personally identifiable information* (PII) (3.1.21)

Catatan 1 untuk entri: Bergantung pada yurisdiksi dan legislasi proteksi data dan privasi tertentu, sinonim "subjek data" juga dapat digunakan sebagai pengganti istilah "PII *principal*".

[SUMBER: ISO/IEC 29100:2011, 2.11]

3.1.23
prosesor PII
pemangku kepentingan privasi yang memproses *personally identifiable information* (PII) (3.1.21) atas nama dan sesuai dengan instruksi pengontrol PII

[SUMBER : ISO/IEC 29100:2011, 2.12]

3.1.24
kebijakan
maksud dan arah suatu organisasi, sebagaimana diungkapkan secara formal oleh manajemen puncak nya [SUMBER: ISO/IEC 27000:2018, 3.53]

3.1.25
asesmen dampak privasi
privacy impact assessment
PIA
keseluruhan *proses* (3.1.27) untuk mengidentifikasi, menganalisis, mengevaluasi, mengonsultasikan, mengomunikasikan, dan merencanakan penanganan kemungkinan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dampak privasi sehubungan dengan pemrosesan *personally identifiable information* (PII) (3.1.21), yang disusun dalam kerangka kerja manajemen risiko organisasi yang lebih luas

[SUMBER : ISO/IEC 29134:2017, 3.7, dimodifikasi — Catatan 1 untuk entri dihapus.]

3.1.26
prosedur
cara yang ditentukan untuk melakukan suatu aktivitas atau *proses* (3.1.27)

[SUMBER : ISO 30000:2009, 3.12]

3.1.27
proses
seperangkat aktivitas yang saling terkait atau berinteraksi yang menggunakan atau mentransformasi input untuk memberikan hasil

[SUMBER: ISO 9000:2015, 3.4.1, dimodifikasi - Catatan untuk entri dihapus.]

3.1.28
rekaman
informasi yang dibuat, diterima, dan dipelihara sebagai bukti dan sebagai *aset* (3.1.2) oleh organisasi atau orang, dalam rangka obligasi legal atau dalam transaksi bisnis

Catatan 1 untuk entri: Obligasi legal dalam konteks ini mencakup semua persyaratan hukum, statutori, regulatori, dan kontrak.

[SUMBER : ISO 15489 -1:2016, 3.14, dimodifikasi - "Catatan 1 untuk entri" ditambahkan.]

3.1.29
sasaran titik pemulihan
recovery point objective
RPO
titik waktu saat data dipulihkan setelah disrupsi(3.1.9) terjadi

[SUMBER: ISO/IEC 27031:2011, 3.12, dimodifikasi — "*must*" diganti dengan "*are to be*".]

3.1.30
sasaran waktu pemulihan
recovery time objective
RTO
jangka waktu saat level minimum layanan dan/atau produk serta sistem, aplikasi, atau fungsi pendukung dipulihkan setelah terjadinya suatu disrupsi (3.1.9)

[SUMBER : ISO/IEC 27031:2011, 3.13, dimodifikasi — "must" diganti dengan "are to be".]

3.1.31
reliabilitas
properti perilaku dan hasil yang konsisten sesuai intensi

3.1.32
aturan
prinsip atau instruksi yang berterima yang menyatakan ekspektasi organisasi tentang apa yang sebaiknya dilakukan, apa yang diperbolehkan atau tidak diperbolehkan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Catatan 1 untuk entri: Aturan dapat dinyatakan secara formal dalam *kebijakan topik spesifik* (3.1.35) dan dalam tipe dokumen lainnya.

3.1.33
informasi sensitif
informasi yang perlu diproteksi dari ketaktersediaan, akses yang takterotorisasi, modifikasi, atau pengungkapan publik karena potensi efek buruk terhadap individu, organisasi, keamanan nasional, atau keselamatan publik

3.1.34
ancaman
potensi penyebab insiden yang tidak diinginkan, yang dapat mengakibatkan bahaya pada sistem atau organisasi

[SUMBER: ISO/IEC 27000:2018, 3.74]

3.1.35
kebijakan topik spesifik
intensi dan arah mengenai subjek atau topik spesifik, sebagaimana dinyatakan secara formal oleh level manajemen yang tepat

Catatan 1 untuk entri: Kebijakan topik spesifik dapat secara formal menyatakan *aturan* (3.1.32) atau standar organisasi.

Catatan 2 untuk entri: Beberapa organisasi menggunakan istilah lain untuk kebijakan topik spesifik ini.

Catatan 3 untuk entri: Kebijakan topik spesifik yang dimaksud dalam dokumen ini terkait dengan keamanan informasi.

CONTOH Kebijakan topik spesifik tentang *kontrol akses* (3.1.1), kebijakan topik spesifik tentang meja bersih (*clear desk)* dan layar bersih *(clear screen*) .

3.1.36
pengguna
pihak berkepentingan (3.1.18) dengan akses ke *sistem informasi* (3.1.17) organisasi

Contoh *Personel* (3.1.20), pelanggan, pemasok

3.1.37
perangkat titik akhir pengguna
perangkat titik akhir (3.1.10) yang digunakan oleh pengguna untuk mengakses layanan pemrosesan informasi

Catatan 1 untuk entri: Perangkat titik akhir pengguna dapat merujuk ke komputer *desktop*, laptop, ponsel pintar, tablet, *thin client* , dan lain-lain.

3.1.38
kerentanan
kelemahan suatu *aset* (3.1.2) atau *kontrol* (3.1.8) yang dapat dieksploitasi oleh satu atau lebih *ancaman* (3.1.34)

[SUMBER : ISO/IEC 27000:2018, 3.77]

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3.2 Singkatan

ABAC *attribute-based access control* (kontrol akses berbasis atribut)

ACL *access control list* (daftar kontrol akses)

BIA *business impact analysis* (analisis dampak bisnis)

BYOD *bring your own device* (bawa peranti anda sendiri)

CAPTCHA *completely automated public Turing test to tell computers and humans apart* (uji Turing publik yang sepenuhnya otomatis untuk membedakan komputer dan manusia)

CPU *central processing unit* (unit pemrosesan pusat)

DAC *discretionary access control* (kontrol akses diskresioner)

DNS *domain name system* (sistem nama domain)

GPS *global positioning system* (sistem pemosisi global)

IAM *identity and access management* (manajemen identitas dan akses)

ICT *information and communication technology* (teknologi informasi dan komunikasi)

ID *identifier* (pengidentifikasi)

IDE *integrated development environment* (lingkungan pengembangan terpadu)

IDS *intrusion detection system* (sistem deteksi intrusi)

IoT *Internet of Things*

IP *internet protocol* (protokol internet)

IPS *intrusion prevention system* (sistem pencegahan intrusi)

IT *information technology* (teknologi informasi)

ISMS *information security management system* (sistem manajemen keamanan *informasi* – SMKI)

MAC *mandatory access control* (kontrol akses wajib)

NTP *network time protocol* (protokol waktu jaringan)

PIA *privacy impact assessment* (asesmen dampak privasi)

PII *personally identifiable information* (informasi pengidentifikasi personal)

PIN *personal identification number* (nomor identifikasi pribadi)

PKI *public key infrastructure* (infrastruktur kunci publik)

PTP *precision time protocol* (protokol waktu presisi)

RBAC *role-based access control* (kontrol akses berbasis peran)

RPO *recovery point objective* (sasaran titik pemulihan)

RTO *recovery time objective* (sasaran waktu pemulihan)

SAST *static application security testing* (pengujian keamanan aplikasi statis)

SD *secure digital* (digital yang aman)

SDN *software-defined networking* (jaringan yang ditentukan perangkat lunak)

SD-WAN *software-defined wide area networking* (jaringan area luas yang ditentukan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

	perangkat lunak)
SIEM	*security information and event management* (informasi keamanan dan manajemen peristiwa)
SMS	*short message service* (layanan pesan singkat)
SQL	*structured query language* (bahasa kueri terstruktur)
SSO	*single sign on*
SWID	*software identification* (identifikasi perangkat lunak)
UEBA	*user and entity behaviour analytics* (analisis perilaku pengguna dan entitas)
UPS	*uninterruptible power supply* (sumber daya tanpa interupsi)
URL	*uniform resource locator* (lokator sumber seragam)
USB	*universal serial bus*
VM	*virtual machine* (mesin virtual)
VPN	*virtual private network* (jaringan pribadi virtual)
WiFi	*wireless fidelity* (fidelitas nirkabel)

4 Struktur dokumen ini

4.1 Pasal

Dokumen ini disusun sebagai berikut:
a) kontrol organisasi (Pasal 5)
b) kontrol orang (Pasal 6)
c) kontrol fisik (Pasal 7)
d) kontrol teknologi (Pasal 8)

Ada 2 lampiran informatif:
— Lampiran A — Penggunaan atribut
— Lampiran B — Padanan dengan ISO/IEC 27002: 2013

Lampiran A menjelaskan bagaimana organisasi dapat menggunakan atribut (lihat 4.2) untuk membuat pandangannya sendiri berdasarkan atribut kontrol yang didefinisikan dalam dokumen ini atau yang dibuatnya sendiri.

Lampiran B menunjukkan padanan antara kontrol dalam ISO/IEC 27002 edisi ini dan edisi 2013.

4.2 Tema dan atribut

Kategorisasi kontrol yang diberikan dalam Pasal 5 hingga 8 disebut sebagai tema.
Kontrol dikategorikan sebagai:
a) orang, jika menyangkut orang;
b) fisik, jika menyangkut objek fisik;
c) teknologi, jika menyangkut teknologi;
d) selain itu maka dikategorikan sebagai organisasi.

Organisasi dapat menggunakan atribut untuk membuat pandangan yang berbeda yang merupakan kategorisasi kontrol yang berbeda seperti yang dilihat dari perspektif berbeda mengenai tema tersebut. Atribut dapat digunakan untuk memfilter, mengurutkan, atau menyajikan kontrol dalam pandangan yang berbeda untuk audiens yang berbeda. Lampiran

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

A menjelaskan bagaimana hal tersebut dapat dicapai dan memberikan contoh dari sebuah pandangan.

Sebagai contoh, setiap kontrol dalam dokumen ini telah diasosiasikan pada lima atribut dengan nilai atribut yang sepadan (didahului dengan "#" agar dapat ditelusuri), sebagai berikut:

a) Tipe kontrol
Tipe kontrol adalah atribut untuk melihat kontrol dari perspektif kapan dan bagaimana kontrol memodifikasi risiko sehubungan dengan terjadinya insiden keamanan informasi. Nilai atribut terdiri dari Preventif (kontrol yang dimaksudkan untuk mencegah terjadinya insiden keamanan informasi), Detektif (kontrol berperan saat insiden keamanan informasi terjadi) dan Korektif (kontrol berperan setelah insiden keamanan informasi terjadi).

b) Properti keamanan informasi
Properti keamanan informasi adalah atribut untuk melihat kontrol dari perspektif karakteristik informasi mana yang akan dipreservasi dengan kontrol tersebut. Nilai atribut terdiri dari Konfidensialitas, Integritas, dan Availabilitas.

c) Konsep keamanan siber
Konsep keamanan siber adalah atribut untuk melihat kontrol dari perspektif keterkaitan kontrol dengan konsep keamanan siber yang didefinisikan dalam kerangka kerja keamanan siber yang dijelaskan dalam ISO/IEC TS 27110. Nilai atribut terdiri dari Mengidentifikasi, Memproteksi, Mendeteksi, Merespons, dan Memulihkan.

d) Kapabilitas operasional
Kapabilitas operasional adalah atribut untuk melihat kontrol dari perspektif praktisi mengenai kapabilitas keamanan informasi. Nilai atribut terdiri dari Tata_kelola, Manajemen_aset, Proteksi_informasi, Keamanan_SDM, Keamanan_fisik, Keamanan_sistem_dan_jaringan, Keamanan_aplikasi, Konfigurasi_yang_aman, Manajemen_identitas_dan_akses, Manajemen_Ancaman_dan_kerentanan, Kontinuitas, Keamanan_hubungan_pemasok, Hukum_dan_kepatuhan, Manajemen_peristiwa_keamanan_informasi, dan keyakinan_keamanan_informasi.

e) Domain keamanan
Domain keamanan adalah atribut untuk melihat kontrol dari perspektif empat domain keamanan informasi: "Tata Kelola dan Ekosistem" mencakup "Tata Kelola Keamanan Sistem Informasi & Manajemen Risiko" dan "Manajemen keamanan siber ekosistem" (termasuk pemangku kepentingan internal dan eksternal); "Proteksi" mencakup "Arsitektur Keamanan TI", "Administrasi Keamanan TI", "Manajemen Identitas dan akses", "Pemeliharaan Keamanan TI" dan "Keamanan fisik dan lingkungan"; "Pertahanan" mencakup "Deteksi" dan "Manajemen Insiden Keamanan Komputer"; "Resiliensi" mencakup "Kontinuitas operasi" dan "Manajemen Krisis". Nilai atribut terdiri dari Tata_kelola_dan_Ekosistem, Proteksi, Pertahanan, dan Resiliensi.

Atribut yang diberikan dalam dokumen ini dipilih karena dianggap cukup generik untuk digunakan oleh berbagai tipe organisasi. Organisasi dapat memilih untuk mengabaikan satu atau beberapa atribut yang diberikan dalam dokumen ini. Organisasi juga dapat membuat atributnya sendiri (dengan nilai atribut yang sesuai) untuk membuat pandangan organisasinya sendiri. Pasal A.2 mencakup contoh atribut tersebut.

4.3 Tata letak kontrol

Tata letak untuk setiap kontrol berisi hal-hal berikut:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

— **Judul kontrol:** Nama singkat kontrol;
— **Tabel atribut**: Tabel menunjukkan nilai dari setiap atribut untuk kontrol yang diberikan;
— **kontrol:** Apa kontrolnya;
— **Tujuan**: Mengapa kontrol sebaiknya diimplementasikan ;
— **Panduan:** Bagaimana kontrol sebaiknya diimplementasikan;
— **Informasi lain:** Teks penjelasan atau rujukan ke dokumen terkait lainnya.

Subjudul digunakan dalam teks panduan beberapa kontrol untuk mempermudah keterbacaan panduan yang panjang dan membahas beberapa topik. Judul seperti itu tidak selalu digunakan dalam semua teks panduan. Subjudul digarisbawahi.

5 Kontrol organisasi

5.1 Kebijakan keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem #Resiliensi

Kontrol
Kebijakan keamanan informasi dan kebijakan topik spesifik sebaiknya didefinisikan, disetujui oleh manajemen, dipublikasikan, dikomunikasikan, dan diakui oleh personel terkait dan pihak berkepentingan terkait, dan direviu secara berkala sesuai rencana dan jika terjadi perubahan yang signifikan.

Tujuan
Untuk memastikan kesinambungan kecocokan, kecukupan, efektivitas arahan dan dukungan manajemen untuk keamanan informasi selaras dengan persyaratan bisnis, hukum, statutori , regulatori, dan kontraktual.

Panduan
Pada level tertinggi, organisasi sebaiknya mendefinisikan "kebijakan keamanan informasi" yang disetujui oleh manajemen puncak dan yang mengemukakan pendekatan organisasi dalam memanajemeni keamanan informasinya.

Kebijakan keamanan informasi sebaiknya mengambil konsiderasi persyaratan yang berasal dari:
a) strategi dan persyaratan bisnis;
b) regulasi, legislasi, dan kontrak;
c) risiko dan ancaman keamanan informasi saat ini dan yang diproyeksikan.

Kebijakan keamanan informasi sebaiknya berisi pernyataan mengenai:
a) definisi keamanan informasi;
b) sasaran keamanan informasi atau kerangka kerja untuk menetapkan sasaran keamanan informasi;
c) prinsip untuk memandu semua aktivitas yang berkaitan dengan keamanan informasi;
d) komitmen untuk memenuhi persyaratan yang berlaku terkait keamanan informasi;
e) komitmen untuk peningkatan berkelanjutan atas sistem manajemen keamanan informasi;
f) penugasan tanggung jawab manajemen keamanan informasi untuk berbagai peran yang didefinisikani;
g) prosedur untuk menangani pembebasan dan eksepsi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Manajemen puncak sebaiknya menyetujui setiap perubahan pada kebijakan keamanan informasi.

Pada level yang lebih rendah, kebijakan keamanan informasi sebaiknya didukung oleh kebijakan topik spesifik sesuai kebutuhan, untuk mengamanatkan secara lebih lanjut implementasi kontrol keamanan informasi. Kebijakan topik spesifik biasanya disusun untuk memenuhi kebutuhan kelompok target tertentu dalam organisasi atau untuk mencakup area keamanan tertentu. Kebijakan topik spesifik sebaiknya selaras dengan dan melengkapi kebijakan keamanan informasi organisasi.

Contoh topik spesifik tersebut antara lain:
a) kontrol akses;
b) keamanan fisik dan lingkungan;
c) manajemen aset;
d) transfer informasi;
e) konfigurasi dan penanganan peranti titik akhir pengguna yang aman;
f) keamanan jaringan;
g) manajemen insiden keamanan informasi;
h) pencadangan;
i) kriptografi dan manajemen kunci;
j) klasifikasi dan penanganan informasi;
k) manajemen kerentanan teknis;
l) pengembangan yang aman.

Tanggung jawab pengembangan, reviu, dan persetujuan kebijakan topik spesifik sebaiknya diberikan kepada personel yang terkait berdasarkan level otoritas dan kompetensi teknis yang tepat. Reviu tersebut sebaiknya mencakup asesmen peluang peningkatan kebijakan keamanan informasi dan kebijakan topik spesifik organisasi dan manajemen keamanan informasi dalam menanggapi perubahan atas:
a) strategi bisnis organisasi;
b) lingkungan teknis organisasi;
c) regulasi, statuta legislasi, dan kontrak;
d) risiko keamanan informasi;
e) lingkungan ancaman keamanan informasi saat ini dan yang diproyeksikan;
f) pelajaran yang diperoleh dari peristiwa dan insiden keamanan informasi.

Reviu kebijakan keamanan informasi dan kebijakan topik spesifik sebaiknya memperhitungkan hasil tinjauan dan audit manajemen. Tinjauan dan pembaruan kebijakan terkait lainnya sebaiknya dipertimbangkan ketika satu kebijakan diubah untuk memelihara konsistensi.

Kebijakan keamanan informasi dan kebijakan topik spesifik sebaiknya dikomunikasikan kepada personel terkait dan pihak yang berkepentingan dalam bentuk yang relevan, dapat diakses, dan dimengerti oleh pembaca yang dimaksudkan. Penerima kebijakan sebaiknya dipersyaratkan untuk mengakui bahwa mereka memahami dan setuju untuk mematuhi kebijakan yang berlaku. Organisasi dapat menentukan format dan nama dokumen kebijakan sesuai dengan kebutuhan organisasi. Di beberapa organisasi, kebijakan keamanan informasi dan kebijakan topik spesifik dapat terangkum dalam satu dokumen. Organisasi dapat menyebut kebijakan topik spesifik ini sebagai standar, arahan, kebijakan, atau lainnya.

Jika kebijakan keamanan informasi atau kebijakan topik spesifik apa pun didistribusikan keluar organisasi, perlu kehati-hatian untuk tidak mengungkapkan informasi konfidensial secara tidak layak .

Tabel 1 menggambarkan perbedaan antara kebijakan keamanan informasi dan kebijakan topik spesifik.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel 1 — Perbedaan antara kebijakan keamanan informasi dan kebijakan topik spesifik

	Kebijakan keamanan informasi	Kebijakan topik spesifik
Level kedetailan	Umum atau level tinggi	Spesifik dan mendetail
Didokumentasikan dan disetujui secara resmi oleh	Manajemen puncak	Level manajemen yang tepat

Informasi lain
Kebijakan topik spesifik dapat beragam di berbagai organisasi.

5.2 Peran dan tanggung jawab keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem #Proteksi #Resiliensi

Kontrol
Peran dan tanggung jawab keamanan informasi sebaiknya didefinisikan dan dialokasikan sesuai dengan kebutuhan organisasi.

Tujuan
Untuk menetapkan struktur yang didefinisikan, disetujui, dan dipahami untuk implementasi, pengoperasian, dan manajemen keamanan informasi dalam organisasi.

Panduan
Alokasi peran dan tanggung jawab keamanan informasi sebaiknya dilakukan sejalan dengan kebijakan keamanan informasi dan kebijakan topik spesifik (lihat 5.1). Organisasi sebaiknya mendefinisikan dan memanajemeni tanggung jawab untuk:

a) perlindungan informasi dan aset terkait lainnya;
b) melaksanakan proses keamanan informasi spesifik;
c) aktivitas manajemen risiko keamanan informasi dan khususnya penerimaan risiko residual (misalnya kepada pemilik risiko);
d) semua personel yang menggunakan informasi organisasi dan aset terkait lainnya.

tanggung jawab tersebut sebaiknya dilengkapi, jika diperlukan, dengan panduan yang lebih mendetail untuk situs dan fasilitas pemrosesan informasi tertentu. Individu dengan tanggung jawab keamanan informasi yang dialokasikan dapat memberikan tugas keamanan kepada orang lain. Namun, mereka tetap bertanggung jawab dan sebaiknya memastikan bahwa setiap tugas yang didelegasikan telah dilakukan dengan benar.

Setiap area keamanan yang menjadi tanggung jawab individu sebaiknya didefinisikan, didokumentasikan, dan dikomunikasikan. Level otorisasi sebaiknya didefinisikan dan didokumentasikan. Individu yang mengambil peran keamanan informasi spesifik sebaiknya memiliki pengetahuan dan keterampilan yang diperlukan untuk peran tersebut dan sebaiknya didukung untuk mengikuti perkembangan yang terkait dengan peran tersebut dan diperlukan untuk memenuhi tanggung jawab peran tersebut.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Banyak organisasi menunjuk manajer keamanan informasi untuk bertanggung jawab secara keseluruhan atas pengembangan dan implementasi keamanan informasi dan untuk mendukung identifikasi risiko dan memitigasi kontrol.

Namun, tanggung jawab untuk mencari sumber daya dan mengimplementasikan kontrol sering kali tetap berada pada manajer individu. Salah satu praktik yang umum yaitu menunjuk pemilik setiap aset yang kemudian bertanggung jawab atas perlindungannya sehari-hari.

Bergantung pada ukuran dan sumber daya organisasi, keamanan informasi dapat ditangani oleh peran atau tugas khusus yang dilakukan di samping peran yang ada.

5.3 Segregasi tugas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Protek	#Tata_kelola #Manajemen_identitas_dan_akses	#Tata_kelola_dan_Ekosistem

Kontrol
Tugas yang bertentangan dan bidang tanggung jawab yang bertentangan sebaiknya dipisahkan.

Tujuan
Untuk mengurangi risiko kecurangan, kesalahan, dan pemintasan kontrol keamanan informasi.

Panduan
Segregasi tugas dan bidang tanggung jawab bertujuan untuk memisahkan tugas yang bertentangan antara individu yang berbeda untuk mencegah seorang individu melaksanakan tugas yang mungkin bertentangan secara sendirian.

Organisasi sebaiknya menentukan tugas dan bidang tanggung jawab mana yang perlu dipisahkan. Berikut ini adalah contoh aktivitas yang mungkin memerlukan segregasi:
a) memulai, menyetujui, dan melaksanakan perubahan;
b) meminta, menyetujui, dan mengimplementasikan hak akses;
c) merancang, menerapkan, dan mereviu kode;
d) mengembangkan perangkat lunak dan menjadi admin sistem produksi;
e) menggunakan dan menjadi admin aplikasi;
f) menggunakan aplikasi dan menjadi admin pangkalan data;
g) mendesain, mengaudit, dan memberi keyakinan kontrol keamanan informasi.

Kemungkinan adanya kolusi sebaiknya dipertimbangkan dalam mendesain kontrol segregasi. Organisasi kecil dapat mengalami segregasi tugas sulit untuk dicapai, tetapi prinsip tersebut sebaiknya diterapkan sebisa mungkin. Setiap kali sulit untuk melakukan segregasi, kontrol lain sebaiknya dipertimbangkan, seperti pemonitoran aktivitas, jejak audit, dan supervisi manajemen.

Perlu kehati-hatian ketika menggunakan sistem kontrol akses berbasis peran untuk memastikan bahwa para person tidak diberi peran yang bertentangan. Ketika terdapat peran dalam jumlah besar, organisasi sebaiknya mempertimbangkan untuk menggunakan alat otomatis untuk mengidentifikasi konflik dan memfasilitasi penghapusannya. Peran sebaiknya didefinisikan dan disediakan dengan hati-hati untuk meminimalkan masalah akses jika peran

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dipindahkan atau ditugaskan kembali.

Informasi lain
Tidak ada informasi lain.

5.4 Tanggung jawab manajemen

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem

Kontrol
Manajemen sebaiknya mensyaratkan semua personel untuk menerapkan keamanan informasi sesuai dengan kebijakan keamanan informasi, kebijakan topik spesifik, dan prosedur organisasi yang ditetapkan.

Tujuan
Untuk memastikan manajemen memahami peran mereka dalam keamanan informasi dan melakukan tindakan yang bertujuan untuk memastikan semua personel menyadari dan memenuhi tanggung jawab keamanan informasinya.

Panduan
Manajemen sebaiknya menunjukkan dukungan terhadap kebijakan keamanan informasi, kebijakan topik spesifik, prosedur, dan kontrol keamanan informasi.

Tanggung jawab manajemen sebaiknya mencakup memastikan bahwa personel:
a) diberi pengarahan yang layak tentang peran dan tanggung jawab keamanan informasi mereka sebelum diberikan akses ke informasi organisasi dan aset terkait lainnya
b) diberi pedoman yang menyatakan ekspektasi keamanan informasi dari peran mereka dalam organisasi;
c) diwajibkan untuk memenuhi kebijakan keamanan informasi dan kebijakan topik spesifik organisasi;
d) mencapai level kesadaran keamanan informasi yang sesuai dengan peran dan tanggung jawab mereka dalam organisasi (lihat 6.3);
e) kepatuhan terhadap syarat dan ketentuan kerja, kontrak atau perjanjian, termasuk kebijakan keamanan informasi organisasi dan metode kerja yang tepat;
f) terus memiliki keterampilan dan kualifikasi keamanan informasi yang tepat melalui pendidikan profesional yang berkelanjutan;
g) jika dapat dipraktikkan, diberi kanal konfidensial untuk melaporkan pelanggaran kebijakan keamanan informasi, kebijakan topik spesifik, atau prosedur keamanan informasi ("*whistleblowing*"). Hal ini dapat mengizinkan pelaporan secara anonim, atau memiliki ketentuan untuk memastikan bahwa informasi tentang identitas pelapor hanya diketahui oleh mereka yang berkepentingan dengan laporan tersebut;
h) diberi sumber daya dan waktu perencanaan proyek yang cukup untuk mengimplementasikan proses dan kontrol terkait keamanan organisasi.

Informasi lain
Tidak ada informasi lain.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.5 Kontak dengan otoritas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi #Merespons #Memulihkan	#Tata_kelola	#Pertahanan #Resiliensi

Kontrol
Organisasi sebaiknya menjalin dan memelihara kontak dengan otoritas terkait.

Tujuan
Untuk memastikan berlangsungnya arus informasi yang tepat sehubungan dengan keamanan informasi antara organisasi dan otoritas legal, regulatori, dan pengawasan yang terkait.

Panduan
Organisasi sebaiknya menentukan kapan dan oleh siapa otoritas (misalnya penegak hukum, badan regulatori, otoritas pengawasan) sebaiknya dihubungi, serta bagaimana insiden keamanan informasi yang teridentifikasi sebaiknya dilaporkan secara tepat waktu.

Kontak dengan otoritas juga sebaiknya digunakan untuk memfasilitasi pemahaman tentang ekspektasi otoritas tersebut saat ini dan yang akan datang (misalnya regulasi keamanan informasi yang berlaku).

Informasi lain

Organisasi yang diserang dapat meminta otoritas untuk mengambil tindakan terhadap sumber serangan.

Memelihara kontak tersebut dapat menjadi persyaratan untuk mendukung manajemen insiden keamanan informasi (lihat 5.24 hingga 5.28) atau proses perencanaan kontingensi dan kontinuitas bisnis (lihat 5.29 dan 5.30). Kontak dengan badan regulatori juga berguna untuk mengantisipasi dan mempersiapkan perubahan yang akan datang dalam hukum atau regulasi terkait yang memengaruhi organisasi. Kontak dengan otoritas lainnya termasuk utilitas, layanan darurat, pemasok listrik, serta kesehatan dan keselamatan [misalnya pemadam kebakaran (sehubungan dengan kontinutitas bisnis), penyedia telekomunikasi (sehubungan dengan perutean jalur dan availabilitas) dan pemasok air (sehubungan dengan fasilitas pendingin untuk peralatan)].

5.6 Kontak dengan kelompok kepentingan khusus

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons #Memulihkan	#Tata_kelola	#Pertahanan

Kontrol
Organisasi sebaiknya menjalin dan memelihara kontak dengan kelompok kepentingan khusus atau forum keamanan spesialis lainnya dan asosiasi profesional.

Tujuan
Untuk memastikan arus informasi yang tepat terjadi sehubungan dengan keamanan informasi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan
Keanggotaan kelompok atau forum kepentingan spesial sebaiknya dipertimbangkan sebagai sarana untuk:
a) meningkatkan pengetahuan tentang praktik terbaik dan mengikuti informasi keamanan yang relevan;
b) memastikan pemahaman tentang lingkungan keamanan informasi saat ini;
c) menerima peringatan dini tentang peringatan, saran, dan tambalan yang berkaitan dengan serangan dan kerentanan;
d) mendapatkan akses saran ke spesialis keamanan informasi;
e) berbagi dan bertukar informasi tentang teknologi, produk, layanan, ancaman, atau kerentanan baru;
f) menyediakan narahubung yang cocok ketika berurusan dengan insiden keamanan informasi (lihat 5.24 hingga 5.28).

Informasi lain
Tidak ada informasi lain.

5.7 Intelijen ancaman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #mendeteksi #Merespons	#Manajemen_ancaman_dan_kerentanan	#Pertahanan #Resiliensi

Kontrol
Informasi yang berkaitan dengan ancaman keamanan informasi sebaiknya dikumpulkan dan dianalisis untuk menghasilkan intelijen ancaman.

Tujuan
Untuk Memberikan kesadaran tentang lingkungan ancaman organisasi sehingga dapat dilakukan tindakan mitigasi yang tepat.

Panduan
Informasi tentang ancaman yang ada atau yang muncul dikumpulkan dan dianalisis untuk:
a) memfasilitasi tindakan terinformasi untuk mencegah ancaman yang membahayakan bagi organisasi;
b) mengurangi dampak ancaman tersebut.

Intelijen ancaman dapat dibagi menjadi tiga lapisan, yang seluruhnya sebaiknya dipertimbangkan:
a) intelijen ancaman strategis: pertukaran informasi level tinggi tentang lanskap ancaman yang berubah (misalnya tipe penyerang atau tipe serangan);
b) intelijen ancaman taktis: informasi tentang metodologi, alat, dan teknologi yang digunakan penyerang;
c) intelijen ancaman operasional: detail tentang serangan spesifik, termasuk indikator teknis.

Intelijen ancaman sebaiknya:
a) relevan (yaitu terkait dengan proteksi organisasi);
b) berwawasan luas (yaitu memberikan pemahaman yang akurat dan mendetail kepada organisasi tentang lanskap ancaman);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

c) kontekstual, untuk memberikan kesadaran situasional (yaitu menambahkan konteks ke informasi berdasarkan waktu peristiwa, tempat peristiwa, pengalaman sebelumnya, dan prevalensi dalam organisasi serupa);
d) dapat ditindaklanjuti (yaitu organisasi dapat bertindak berdasarkan informasi dengan cepat dan efektif).

Aktivitas intelijen ancaman sebaiknya mencakup:
a) menetapkan sasaran untuk menghasilkan intelijen ancaman;
b) mengidentifikasi, memeriksa, dan memilih sumber informasi internal dan eksternal yang diperlukan serta tepat untuk menyediakan informasi yang disyaratkan untuk produksi intelijen ancaman;
c) mengumpulkan informasi dari sumber yang terpiliih, baik internal maupun eksternal;
d) memproses informasi yang terkumpul agar siap untuk dianalisis (misalnya dengan menerjemahkan, memformat, atau mempertegas informasi);
e) menganalisis informasi untuk memahami hubungan dan maknanya bagi organisasi;
f) mengomunikasikan dan membagikannya kepada individu yang relevan dalam format yang dapat dipahami.

Intelijen ancaman sebaiknya dianalisis dan kemudian digunakan:
a) dengan mengimplementasikan proses untuk memasukkan informasi yang dikumpulkan dari sumber intelijen ancaman ke dalam proses manajemen risiko keamanan informasi organisasi;
b) sebagai input tambahan untuk kontrol teknis preventif dan detektif seperti *firewall*, sistem deteksi intrusi (*intrusion detection system*), atau solusi anti perangkat perusak;
c) sebagai input untuk proses dan teknik uji keamanan informasi.

Organisasi sebaiknya berbagi intelijen ancaman dengan organisasi lain atas dasar saling menguntungkan untuk meningkatkan intelijen ancaman secara keseluruhan.

Informasi lain
Organisasi dapat menggunakan intelijen ancaman untuk mencegah, mendeteksi, atau merespons ancaman. Organisasi dapat menghasilkan intelijen ancaman, tetapi umumnya lebih sering menerima dan memanfaatkan intelijen ancaman yang dihasilkan oleh sumber lain.

Intelijen ancaman sering kali disediakan oleh penyedia atau advisor independen, lembaga pemerintah, atau kelompok intelijen ancaman kolaboratif.

Efektivitas kontrol seperti 5.25, 8.7, 8.16, atau 8.23, bergantung pada kualitas intelijen ancaman yang tersedia.

5.8 Keamanan informasi dalam manajemen proyek

Tipe kontrol	Properti Keamanan informasi	Konsep Keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Tata_kelola	#Tara_kelola_dan_Ekosistem #Proteksi

Kontrol
Keamanan informasi sebaiknya diintegrasikan ke dalam manajemen proyek.

Tujuan
Untuk memastikan risiko keamanan informasi yang terkait dengan proyek dan hasil kerja ditangani secara efektif dalam manajemen proyek sepanjang siklus hidup proyek.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan

Keamanan informasi sebaiknya diintegrasikan ke dalam manajemen proyek untuk memastikan risiko keamanan informasi ditangani sebagai bagian dari manajemen proyek. Ini dapat diterapkan pada segala tipe proyek terlepas dari kompleksitas, ukuran, durasi, disiplin, atau area aplikasi (misalnya proyek untuk proses bisnis inti, TIK, manajemen fasilitas, atau proses pendukung lainnya).

Manajemen proyek yang digunakan sebaiknya mensyaratkan bahwa:

a) risiko keamanan informasi dinilai dan ditangani pada tahap awal dan secara periodik sebagai bagian dari risiko proyek sepanjang siklus hidup proyek;
b) persyaratan keamanan informasi [misalnya persyaratan keamanan aplikasi (8.26), persyaratan untuk mematuhi hak kekayaan intelektual (5.32), dll.] ditangani pada tahap awal proyek;
c) risiko keamanan informasi yang terkait dengan pelaksanaan proyek, seperti keamanan aspek komunikasi internal dan eksternal dipertimbangkan dan ditangani sepanjang siklus hidup proyek;
d) progres penanganan risiko keamanan informasi direviu dan efektivitas penanganan dievaluasi serta diuji.

Ketepatan dari konsiderasi dan aktivitas keamanan informasi sebaiknya ditindaklanjuti pada tahap yang telah ditentukan oleh orang atau penanggung jawab tata kelola yang cocok, seperti komite pengarah proyek.

Tanggung jawab dan otoritas untuk keamanan informasi yang relevan dengan proyek sebaiknya didefinisikan dan dialokasikan untuk berbagai peran spesifik .

Persyaratan keamanan informasi untuk produk atau layanan yang akan disampaikan oleh proyek sebaiknya ditentukan menggunakan beragam metode, termasuk mengambil persyaratan kepatuhan dari kebijakan keamanan informasi, kebijakan topik spesifik, dan regulasi. Persyaratan keamanan informasi lebih lanjut dapat diturunkan dari aktivitas seperti pemodelan ancaman, reviu insiden, penggunaan ambang batas kerentanan, atau perencanaan kontingensi, sehingga memastikan bahwa arsitektur dan desain sistem informasi diproteksi dari ancaman yang diketahui berdasarkan lingkungan operasional.

Persyaratan keamanan informasi sebaiknya ditentukan untuk semua tipe proyek, tidak hanya proyek pengembangan TIK. Hal-hal berikut juga sebaiknya dipertimbangkan saat menentukan persyaratan ini:

a) informasi apa yang terlibat (penentuan informasi), kebutuhan keamanan informasi apa saja yang sepadan (klasifikasi; lihat 5.12), dan potensi dampak bisnis negatif yang dapat diakibatkan oleh kurangnya keamanan yang cukup;
b) kebutuhan proteksi informasi dan aset terkait lainnya yang dipersyaratkan, terutama dalam hal konfidensialitas, integritas, dan availabilitas ;
c) level kepercayaan atau keyakinan yang diperlukan terhadap identitas entitas yang diklaim untuk memperoleh persyaratan autentikasi;
d) proses penyediaan akses dan otorisasi, untuk pelanggan dan pengguna bisnis potensial lainnya serta untuk pengguna istimewa atau pengguna teknis seperti anggota proyek yang relevan, staf operasi potensial, atau pemasok eksternal;
e) menginformasikan kepada pengguna tentang tugas dan tanggung jawabnya;
f) persyaratan yang berasal dari proses bisnis, seperti pembuatan log dan pemonitoran transaksi, persyaratan nirsangkal;
g) persyaratan yang mandatkan oleh kontrol keamanan informasi lainnya (misalnya antarmuka untuk pembuatan log dan pemonitoran atau sistem deteksi kebocoran data);
h) kepatuhan terhadap lingkungan hukum, statutori, regulatori, dan kontraktual yang berlaku bagi pengoperasian organisasi;
i) level kepercayaan atau keyakinan yang dipersyaratkan bagi pihak ketiga untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

memenuhi kebijakan keamanan informasi dan kebijakan topik spesifik organisasi termasuk pasal keamanan yang relevan dalam segala perjanjian atau kontrak.

Informasi lain
Pendekatan pengembangan proyek, seperti siklus hidup *waterfall* atau siklus hidup *agile*, sebaiknya mendukung keamanan informasi dengan cara terstruktur yang dapat disesuaikan dengan level keparahan risiko keamanan informasi yang dinilai, berdasarkan karakter proyek. Konsiderasi awal persyaratan keamanan informasi untuk produk atau layanan (misalnya pada tahap perencanaan dan desain), dapat mengarah pada solusi yang lebih efektif dan hemat biaya untuk kualitas serta keamanan informasi. ISO 21500 dan ISO 21502 memberikan panduan tentang konsep dan proses manajemen proyek yang penting untuk kinerja proyek.

ISO/IEC 27005 memberikan panduan tentang penggunaan proses manajemen risiko dalam mengidentifikasi kontrol untuk memenuhi persyaratan keamanan informasi.

5.9 Inventori informasi dan aset terkait lainnya

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Manajemen_aset	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Suatu inventori informasi dan aset terkait lainnya, termasuk pemiliknya, sebaiknya dikembangkan dan dipelihara.

Tujuan
Untuk mengidentifikasi informasi organisasi dan aset terkait lainnya dalam rangka menjaga keamanan informasinya dan menetapkan kepemilikan yang tepat.

Panduan
Inventori
Organisasi sebaiknya mengidentifikasi informasinya dan aset terkait lainnya serta menentukan level kepentingannya dalam hal keamanan informasi. Dokumentasi sebaiknya dipelihara pada inventori khusus atau yang sudah ada dengan tepat.

Inventori informasi dan aset terkait lainnya sebaiknya akurat, mutakhir, konsisten, dan selaras dengan inventori lainnya. Beberapa opsi untuk memastikan keakuratan inventori informasi dan aset terkait lainnya meliputi:

a) melakukan reviu reguler dari informasi terindentifikasi dan aset terkait lainnya terhadap inventori aset;
b) secara otomatis memberlakukan pemutakhiran inventaris dalam proses pemasangan, perubahan, atau pemindahan aset.

Lokasi aset sebaiknya dicantumkan ke dalam inventori dengan tepat.
Inventori tidak perlu berupa daftar tunggal dari informasi dan aset terkait lainnya. Mempertimbangkan bahwa inventori sebaiknya dipelihara oleh fungsi yang relevan, maka inventori dapat dilihat sebagai seperangkat inventori dinamis, seperti inventori untuk aset informasi, perangkat keras, perangkat lunak, mesin virtual (*virtual machine* - VM), fasilitas, personel, kompetensi, kapabilitas, dan rekaman.

Setiap aset sebaiknya diklasifikasikan berdasarkan klasifikasi informasi (lihat 5.12) yang terkait dengan aset tersebut.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Granularitas inventori informasi dan aset terkait lainnya sebaiknya berada pada level yang tepat untuk kebutuhan organisasi. Terkadang *instance* aset spesifik dalam siklus hidup informasi tidak fisibel untuk didokumentasikan karena sifat aset tersebut. Contoh aset yang berumur pendek adalah *instance* VM yang siklus hidupnya berdurasi pendek.

Kepemilikan
Untuk informasi teridentifikasi dan aset terkait lainnya, kepemilikan aset sebaiknya diberikan kepada individu atau kelompok serta klasifikasi sebaiknya diidentifikasi (lihat 5.12, 5.13). Proses untuk memastikan penetapan kepemilikan aset secara tepat waktu sebaiknya diimplementasikan. Kepemilikan sebaiknya diberikan ketika aset dibuat atau ketika aset ditransfer ke organisasi. Kepemilikan aset sebaiknya ditetapkan kembali jika diperlukan ketika pemilik aset saat ini meninggalkan atau berubah peran kerja .

Tugas pemilik
Pemilik aset sebaiknya bertanggung jawab atas manajemen aset yang layak selama seluruh siklus hidup aset dengan memastikan bahwa:
a) informasi dan aset terkait lainnya diinventarisasi;
b) informasi dan aset terkait lainnya diklasifikasikan serta diproteksi dengan tepat;
c) klasifikasi direviu secara periodik;
d) komponen yang mendukung aset teknologi didaftarkan dan dihubungkan, seperti pangkalan data, penyimpanan, komponen dan subkomponen perangkat lunak;
e) persyaratan untuk penggunaan yang akseptabel atas informasi dan aset terkait lainnya (lihat 5.10) ditetapkan;
f) pembatasan akses sepadan dengan klasifikasi, efektif dan direviu secara periodik;
g) informasi dan aset terkait lainnya, ketika dihapus atau dimusnahkan, ditangani dengan cara yang aman dan dipindahkan dari inventori;
h) pemilik aset terlibat dalam identifikasi dan manajemen risiko yang terkait dengan asetnya;
i) pemilik aset mendukung personel yang memiliki peran dan tanggung jawab memanajemeni informasi mereka.

Informasi lain
Inventori informasi dan aset terkait lainnya sering diperlukan untuk memastikan proteksi informasi yang efektif dan dapat dipersyaratkan untuk tujuan lain, seperti kesehatan dan keselamatan, asuransi, atau alasan finansial. Inventori informasi dan aset terkait lainnya juga mendukung manajemen risiko, aktivitas audit, manajemen kerentanan, respons insiden, dan perencanaan pemulihan.

Tugas dan tanggung jawab dapat didelegasikan (misalnya kepada kustodian yang menjaga aset setiap hari), namun orang atau kelompok yang mendelegasikannya tetap akuntabel.

Tugas dan tanggung jawab dapat berguna untuk menunjuk kelompok informasi dan aset terkait lainnya yang bertindak bersama untuk menyediakan layanan tertentu. Dalam hal ini, pemilik layanan ini bertanggung jawab atas penyerahan layanan, termasuk pengoperasian asetnya.

Lihat ISO/IEC 19770-1 untuk informasi tambahan tentang manajemen aset teknologi informasi (TI). Lihat ISO 55001 untuk informasi tambahan tentang manajemen aset.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.10 Penggunaan yang akseptabel dari informasi dan aset terkait lainnya

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_aset #Proteksi_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Resiliensi

Kontrol
Aturan penggunaan yang akseptabel dan prosedur untuk menangani informasi dan aset terkait lainnya sebaiknya diidentifikasi, didokumentasikan, dan diimplementasikan.

Tujuan
Untuk memastikan informasi dan aset terkait lainnya diproteksi, digunakan, dan ditangani dengan tepat.

Panduan
Personel dan pengguna pihak eksternal yang menggunakan atau memiliki akses ke informasi dan aset terkait lainnya milik organisasi sebaiknya diberi tahu tentang persyaratan keamanan informasi untuk memproteksi dan menangani informasi dan aset terkait lainnya milik organisasi Mereka sebaiknya bertanggung jawab atas penggunaan segala fasilitas pemrosesan informasi.

Organisasi sebaiknya menetapkan kebijakan topik spesifik tentang penggunaan informasi dan aset terkait lainnya secara berterima serta mengomunikasikannya kepada siapa pun yang menggunakan atau menangani informasi dan aset terkait lainnya. Kebijakan topik spesifik tentang penggunaan yang akseptabel sebaiknya memberikan arahan yang jelas tentang bagaimana individu diharapkan untuk menggunakan informasi dan aset terkait lainnya. Kebijakan topik spesifik sebaiknya menyatakan:

a) perilaku individu yang diharapkan dan yang tidak akseptabel dari perspektif keamanan informasi;
b) penggunaan informasi dan aset terkait lainnya yang diizinkan dan yang dilarang ;
c) memonitor aktivitas yang dilakukan oleh organisasi.

Prosedur penggunaan yang akseptabel sebaiknya dibuat untuk siklus hidup informasi lengkap sepadan dengan klasifikasinya (lihat 5.12) dan risiko yang ditentukan. Hal-hal berikut sebaiknya dipertimbangkan:

a) pembatasan akses yang mendukung persyaratan proteksi untuk setiap level klasifikasi;
b) pemeliharaan rekaman pengguna terotorisasi untuk informasi dan aset terkait lainnya;
c) proteksi salinan informasi sementara atau permanen selevel dengan proteksi informasi asli;
d) penyimpanan aset yang terkait dengan informasi sepadan dengan spesifikasi pabrikan (lihat 7.8);
e) penanda yang jelas untuk semua salinan media penyimpanan (elektronik atau fisik) agar menjadi perhatian penerima yang terotorisasi (lihat 7.10);
f) otorisasi pemusnahan informasi dan aset terkait lainnya dan metode penghapusan yang didukung (lihat 8.10).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Terdapat kasus ketika aset yang bersangkutan tidak langsung menjadi milik organisasi, seperti layanan *cloud* publik. Penggunaan aset pihak ketiga tersebut dan setiap aset organisasi yang terkait dengan aset eksternal tersebut (misalnya informasi, perangkat lunak) sebaiknya dianggap berlaku dan dikontrol, misalnya, melalui perjanjian dengan penyedia layanan *cloud*. Selain itu, perlu kehati-hatian saat menggunakan lingkungan kerja kolaboratif.

5.11 Pengembalian aset

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_aset	#Proteksi

Kontrol
Personel dan pihak berkepentingan lainnya yang tepat sebaiknya mengembalikan semua aset organisasi yang dalam kepemilikan mereka setelah perubahan atau pemutusan hubungan kerja, kontrak, atau perjanjian mereka.

Tujuan
Untuk memproteksi aset organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja, kontrak, atau perjanjian.

Panduan
Proses perubahan atau terminasi sebaiknya disusun dengan mencakup pengembalian semua aset fisik dan elektronik yang telah dikeluarkan sebelumnya yang dimiliki atau dipercayakan kepada organisasi.

Dalam hal personel dan pihak berkepentingan lainnya membeli peralatan organisasi atau menggunakan peralatan pribadi mereka sendiri, sebaiknya diikuti prosedur untuk memastikan bahwa semua informasi yang relevan ditelusuri dan ditransfer ke organisasi dan dihapus dengan aman dari peralatan (lihat 7.14).

Dalam hal personel dan pihak berkepentingan lainnya memiliki pengetahuan yang penting untuk operasi yang sedang berlangsung, informasi tersebut sebaiknya didokumentasikan dan ditransfer ke organisasi.

Selama periode pemberitahuan dan setelahnya, organisasi sebaiknya mencegah penyalinan takterotorisasi atas informasi yang relevan (misalnya kekayaan intelektual) oleh personel yang telah menerima pemberitahuan pemutusan hubungan kerja.

Organisasi sebaiknya dengan jelas mengidentifikasi dan mendokumentasikan semua informasi dan aset terkait lainnya yang akan dikembalikan yang dapat mencakup:
a) perangkat titik akhir pengguna ;
b) perangkat penyimpanan portabel;
c) perangkat spesialis;
d) perangkat keras autentikasi (misalnya kunci mekanis, token fisik, dan kartu pintar) untuk sistem informasi, situs, dan arsip fisik;
e) salinan fisik informasi.

Informasi lain
Sulit untuk mengembalikan informasi yang tersimpan pada aset yang tidak dimiliki oleh organisasi. Dalam kasus tersebut, perlu untuk membatasi penggunaan informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

menggunakan kontrol keamanan informasi lainnya seperti manajemen hak akses (5.18) atau penggunaan kriptografi (8.24).

5.12 Klasifikasi informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Proteksi_informasi	#Proteksi #Pertahanan

Kontrol
Informasi sebaiknya diklasifikasikan sesuai dengan kebutuhan keamanan informasi organisasi berdasarkan konfidensialitas, integritas, availabilitas, dan persyaratan pihak berkepentingan yang relevan.

Tujuan
Memastikan identifikasi dan pemahaman kebutuhan proteksi informasi sesuai dengan kepentingannya bagi organisasi.

Panduan
Organisasi sebaiknya menetapkan kebijakan topik spesifik tentang klasifikasi informasi dan mengomunikasikannya kepada semua pihak berkepentingan yang relevan.

Organisasi sebaiknya memperhitungkan persyaratan konfidensialitas, integritas, dan availabilitas dalam skema klasifikasi.

Klasifikasi dan kontrol proteksi terkait untuk informasi sebaiknya memperhitungkan kebutuhan bisnis untuk membagikan atau membatasi informasi, untuk memproteksi integritas informasi, dan untuk menjamin availabilitas, serta persyaratan legal mengenai konfidensialitas, integritas, atau availabilitas informasi. Aset selain informasi juga dapat diklasifikasikan sesuai dengan klasifikasi informasi, yang disimpan dalam, diproses dengan, ditangani, atau diproteksi oleh aset.

Pemilik informasi sebaiknya akuntabel atas klasifikasi tersebut.

Skema klasifikasi sebaiknya mencakup konvensi untuk klasifikasi dan kriteria untuk mereviu klasifikasi pada waktu tertentu. Hasil klasifikasi sebaiknya diperbarui sesuai dengan perubahan nilai, sensitivitas, dan kekritisan informasi melalui siklus hidupnya.

Skema ini sebaiknya diselaraskan dengan kebijakan topik spesifik tentang kontrol akses (lihat 5.1) dan sebaiknya dapat mengatasi kebutuhan bisnis spesifik organisasi.

Klasifikasi dapat ditentukan oleh level dampak yang dimiliki oleh pembobolan informasi bagi organisasi. Setiap level yang didefinisikan dalam skema tersebut sebaiknya diberi nama yang sesuai dalam konteks penerapan skema klasifikasi.

Skema tersebut sebaiknya konsisten di seluruh organisasi dan termasuk dalam prosedurnya sehingga semua orang mengklasifikasikan informasi dan aset terkait lainnya yang berlaku dengan cara yang sama. Dengan cara ini, setiap orang memiliki pemahaman yang sama tentang persyaratan proteksi dan menerapkan proteksi yang tepat.

Skema klasifikasi yang digunakan dalam suatu organisasi dapat berbeda dengan skema yang digunakan oleh organisasi lain, bahkan jika nama untuk level serupa. Selain itu, informasi yang berpindah di antara organisasi dapat beragam dalam klasifikasi tergantung pada konteksnya

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

di setiap organisasi, bahkan jika skema klasifikasi mereka identik. Oleh karena itu, perjanjian dengan organisasi lain termasuk berbagi informasi sebaiknya mencantumkan prosedur untuk mengidentifikasi klasifikasi informasi tersebut dan mengintrepretasikan level klasifikasi dari organisasi lain. Hubungan antara skema yang berbeda dapat ditentukan dengan mencari kesetaraan dalam metode penanganan dan proteksi terkait.

Informasi lain
Klasifikasi memberikan indikasi ringkas bagi orang yang berurusan dengannya tentang cara menangani dan memproteksi informasi. Ini dapat difasilitasi dengan membentuk kelompok informasi dengan kebutuhan proteksi yang sama dan menspesifikasikan prosedur keamanan informasi yang berlaku untuk semua informasi dalam setiap kelompok. Pendekatan ini mengurangi kebutuhan asesmen risiko kasus per kasus dan desain kontrol khusus.

Informasi mungkin tidak lagi sensitif atau kritis setelah jangka waktu tertentu. Misalnya, ketika informasi telah dipublikasikan, informasi tersebut tidak lagi memiliki persyaratan konfidensialitas tetapi masih mungkin mensyaratkan proteksi untuk properti integritas dan availabilitasnya. Aspek-aspek ini sebaiknya diperhitungkan, karena klasifikasi berlebihan dapat menyebabkan implementasi kontrol yang tidak perlu sehingga mengakibatkan biaya tambahan atau, sebaliknya, klasifikasi rendah dapat menyebabkan kontrol yang tidak cukup untuk memproteksi informasi dari pembobolan.

Sebagai contoh, skema klasifikasi konfidensialitas informasi dapat didasarkan pada empat level sebagai berikut:
a) pengungkapan tidak menyebabkan bahaya;
b) pengungkapan menyebabkan kerusakan reputasi minor atau dampak operasional minor;
c) pengungkapan memiliki dampak jangka pendek yang signifikan terhadap operasi atau sasaran bisnis;
d) pengungkapan memiliki dampak serius pada sasaran bisnis jangka panjang atau menempatkan risiko pada kontinuitas hidup organisasi.

5.13 Pelabelan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Proteksi_informasi	#Proteksi #Pertahanan

Kontrol
Seperangkat prosedur yang tepat untuk pelabelan informasi sebaiknya dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.

Tujuan
Untuk memfasilitasi komunikasi klasifikasi informasi dan mendukung otomatisasi pemrosesan dan manajemen informasi.

Panduan
Prosedur untuk pelabelan informasi sebaiknya mencakup seluruh format informasi dan aset terkait lainnya. Pelabelan sebaiknya merefleksikan skema klasifikasi yang ditetapkan dalam 5.12. Label sebaiknya mudah dikenali. Prosedur sebaiknya memberikan panduan tentang di mana dan bagaimana label dilampirkan dengan mempertimbangkan bagaimana informasi diakses atau aset ditangani bergantung pada tipe media penyimpanan. Prosedur dapat menentukan:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) kasus ketika pelabelan diabaikan (misalnya pelabelan informasi tidak konfidensial untuk mengurangi beban kerja);
b) cara memberi label informasi yang dikirim atau disimpan pada sarana elektronik atau fisik, atau format lainnya;
c) cara menangani kasus ketika pelabelan tidak dimungkinkan (misalnya karena pembatasan teknis).

Contoh teknik pelabelan antara lain:
a) label fisik;
b) kepala (*header)* dan kaki (*footer)*;
c) metadata;
d) tanda air (*watermark)*;
e) cap.

Informasi digital sebaiknya menggunakan metadata untuk mengidentifikasi, memanajemeni, dan mengontrol informasi, terutama yang berkaitan dengan konfidensialitas. Metadata juga sebaiknya memungkinkan pencarian informasi yang efisien dan benar. Metadata sebaiknya memfasilitasi sistem untuk berinteraksi dan membuat keputusan berdasarkan label klasifikasi terkait.

Prosedur tersebut sebaiknya menjelaskan cara melampirkan metadata pada informasi, label yang akan digunakan, dan cara menangani data, sejalan dengan model informasi organisasi dan arsitektur TIK.

Metadata tambahan yang relevan sebaiknya ditambahkan oleh sistem ketika memproses informasi bergantung pada properti keamanan informasinya.

Personel dan pihak berkepentingan lainnya sebaiknya diberi tahu tentang prosedur pelabelan. Semua personel sebaiknya diberi pelatihan yang diperlukan untuk memastikan bahwa informasi diberi label dan ditangani dengan benar.

Keluaran dari sistem yang berisi informasi yang diklasifikasikan sensitif atau kritis sebaiknya memiliki label klasifikasi yang tepat.

Informasi lain
Pelabelan informasi konfidensial adalah persyaratan utama untuk berbagi informasi.

Metadata lainnya yang dapat bermanfaat dilampirkan pada informasi yaitu proses organisasi mana yang menghasilkan informasi dan pada waktu kapan .

Pelabelan informasi dan aset terkait lainnya terkadang dapat memiliki dampak negatif. Aset yang diklasifikasikan dapat lebih mudah diidentifikasi oleh aktor berbahaya untuk potensi penyalahgunaan.

Beberapa sistem tidak melabeli fail individual atau rekaman pangkalan data dengan klasifikasinya tetapi memproteksi semua informasi pada level klasifikasi tertinggi dari setiap informasi yang terkandung di dalamnya atau diizinkan untuk terkandung di dalamnya. Biasa dalam sistem tersebut untuk menentukan dan kemudian melabeli informasi ketika dieskpor.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.14 Transfer informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_aset #Proteksi_informasi	#Proteksi

Kontrol
Aturan, prosedur, atau perjanjian transfer informasi sebaiknya diterapkan untuk semua tipe fasilitas transfer dalam organisasi dan antara organisasi dan pihak lain

Tujuan
Untuk memelihara keamanan informasi yang dikirimkan di dalam organisasi dan dengan setiap pihak eksternal yang berkepentingan.

Panduan
Umum
Organisasi sebaiknya menetapkan kebijakan topik spesifik tentang transfer informasi dan mengomunikasikannya kepada semua pihak berkepentingan yang relevan. Aturan, prosedur, dan perjanjian untuk memproteksi informasi dalam transit sebaiknya merefleksikan klasifikasi informasi yang terlibat. Jika informasi ditransfer antara organisasi dan pihak ketiga, perjanjian transfer (termasuk autentikasi penerima) sebaiknya ditetapkan serta dipelihara untuk memproteksi semua bentuk informasi dalam transit (lihat 5.10).

Transfer informasi dapat terjadi melalui transfer elektronik, transfer media penyimpanan fisik, dan transfer verbal.

Untuk semua tipe transfer informasi, aturan, prosedur, dan perjanjian sebaiknya mencakup:

e) kontrol yang didesain untuk memproteksi informasi yang ditransfer dari penyadapan, akses takterotorisasi, penyalinan, modifikasi, salah perutean, destruksi, dan penolakan layanan, termasuk level kontrol akses yang setara dengan klasifikasi informasi yang terlibat dan kontrol spesial yang dipersyaratkan untuk memproteksi informasi sensitif, seperti penggunaan teknik kriptografi (lihat 8.24);
f) kontrol untuk memastikan ketertelusuran dan nirsangkal, termasuk memelihara rantai kustodi informasi saat dalam transit;
g) identifikasi kontak yang tepat terkait dengan transfer, termasuk pemilik informasi, pemilik risiko, pejabat keamanan dan kustodian informasi, sebagaimana berlaku;
h) tanggung jawab dan kewajiban dalam hal terjadi insiden keamanan informasi, seperti hilangnya media penyimpanan fisik atau data;
i) penggunaan sistem pelabelan yang disepakati untuk informasi sensitif atau kritis, memastikan bahwa makna label segera dipahami dan informasi tersebut diproteksi dengan tepat (lihat 5.13);
j) reliabilitas dan availabilitas layanan transfer;
k) kebijakan atau pedoman topik spesifik tentang penggunaan fasilitas transfer informasi yang akseptabel (lihat 5.10);
l) pedoman retensi dan pemusnahan untuk semua rekaman bisnis, termasuk pesan;

CATATAN Mungkin ada legislasi dan regulasi lokal mengenai retensi dan pemusnahan rekaman bisnis.

m) konsiderasi legal, statutori, regulatori, dan kontraktual lainnya yang relevan (lihat 5.31, 5.32, 5.33, 5.34) yang terkait dengan transfer informasi (misalnya persyaratan untuk tanda tangan elektronik).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Transfer elektronik

Aturan, prosedur, dan perjanjian sebaiknya juga mempertimbangkan hal-hal berikut ketika menggunakan fasilitas komunikasi elektronik untuk transfer informasi:

a) deteksi dan proteksi terhadap perangkat perusak yang dapat ditransmisikan melalui penggunaan komunikasi elektronik (lihat 8.7);
b) proteksi terhadap informasi elektronik sensitif yang dikomunikasikan dalam bentuk lampiran;
c) pencegahan terhadap pengiriman dokumen dan pesan yang dikomunikasikan ke alamat atau nomor yang salah;
d) mendapatkan persetujuan sebelum menggunakan layanan publik eksternal seperti pesan instan, jejaring sosial, berbagi fail, atau penyimpanan *cloud*;
e) level autentikasi yang lebih kuat ketika mentransfer informasi melalui jaringan yang dapat diakses publik;
f) pembatasan yang terkait dengan fasilitas komunikasi elektronik (misalnya mencegah penerusan surat elektronik secara otomatis ke alamat surat eksternal);
g) menyarankan personel dan pihak lain yang berkepentingan untuk tidak mengirim *short message service* (SMS) atau pesan singkat dengan informasi kritis karena dapat dibaca di tempat umum (dan oleh pihak yang tidak berwenang) atau disimpan di peranti yang tidak diproteksi secara cukup;
h) menyarankan personel dan pihak berkepentingan lainnya tentang masalah terkait penggunaan mesin faks atau layanan faks, yaitu:
    1) akses takterotorisasi ke penyimpanan pesan internal untuk memperoleh pesan;
    2) pemrograman mesin yang disengaja atau tidak disengaja untuk mengirim pesan ke nomor spesifik.

Transfer media penyimpanan fisik

Saat mentransfer media penyimpanan fisik (termasuk kertas), aturan, prosedur, dan perjanjian sebaiknya juga mencakup:

a) tanggung jawab untuk mengontrol dan menotifikasi tentang transmisi, pengiriman, dan penerimaan;
b) memastikan pengalamatan dan transportasi pesan yang benar;
c) kemasan yang memproteksi konten dari kerusakan fisik yang mungkin timbul selama transit dan sesuai dengan spesifikasi pabrikan misalnya memproteksi terhadap faktor lingkungan yang dapat mengurangi keefektifan pemulihan media penyimpanan seperti paparan panas, kelembapan, atau medan elektromagnetik; menggunakan standar teknis minimum untuk kemasan dan transmisi (misalnya penggunaan amplop buram);
d) daftar terotorisasi kurir yang reliabel yang disepakati oleh manajemen;
e) standar identifikasi kurir;
f) tergantung pada level klasifikasi informasi dalam media penyimpanan yang akan dikirimkan, gunakan kontrol yang jelas atau tahan terhadap gangguan (misalnya tas, kontainer);
g) prosedur untuk memverifikasi identifikasi kurir;
h) daftar pihak ketiga yang menyediakan layanan transportasi atau kurir yang disetujui tergantung pada klasifikasi informasi;
i) menyimpan log untuk mengidentifikasi konten media penyimpanan, proteksi yang diterapkan, serta mencatat daftar penerima yang terotorisasi, waktu transfer ke kustodian transit, dan tanda terima pada destinasi.

Transfer verbal

Untuk memproteksi transfer informasi secara verbal, personel dan pihak berkepentingan lainnya sebaiknya diingatkan bahwa mereka sebaiknya:

a) tidak melakukan percakapan verbal konfidensial di tempat umum atau melalui saluran komunikasi yang tidak aman karena ini dapat didengar oleh orang yang takterotorisasi;
b) tidak meninggalkan pesan yang berisi informasi konfidensial pada mesin penjawab atau pesan suara karena dapat diputar ulang oleh orang yang takterotorisasi, disimpan pada

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

sistem komunal, atau disimpan secara tidak benar sebagai akibat dari salah sambung;
c) diseleksi hingga level yang tepat untuk mendengarkan percakapan;
d) memastikan bahwa kontrol ruangan yang tepat diimplementasikan (misalnya kedap suara, pintu tertutup);
e) memulai percakapan sensitif dengan penafian sehingga mereka yang hadir mengetahui level klasifikasi dan persyaratan penanganan apa yang akan mereka dengar.

Informasi lain
Tidak ada informasi lain.

5.15 Kontrol akses

Tipe kontrol	Properti keamanan informasi	Konsep Keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Aturan untuk mengontrol akses fisik dan logikal ke informasi dan aset terkait lainnya sebaiknya ditetapkan dan diimplementasikan berdasarkan persyaratan bisnis dan keamanan informasi.

Tujuan
Untuk memastikan akses yang terotorisasi dan untuk mencegah akses yang takterotorisasi ke informasi dan aset terkait lainnya.

Panduan
Pemilik informasi dan aset terkait lainnya sebaiknya menentukan keamanan informasi dan persyaratan bisnis yang terkait dengan kontrol akses. Kebijakan topik spesifik tentang kontrol akses sebaiknya definisikan dengan memperhitungkan persyaratan ini dan sebaiknya dikomunikasikan kepada semua pihak yang terkait yang relevan.

Persyaratan ini dan kebijakan topik spesifik sebaiknya mempertimbangkan hal-hal berikut:
a) penentuan entitas yang mensyaratkan tipe akses terhadap informasi dan aset terkait lainnya;
b) keamanan aplikasi (lihat 8.26);
c) akses fisik, yang perlu didukung oleh kontrol masuk fisik yang tepat (lihat 7.2, 7.3, 7.4);
d) diseminasi informasi dan otorisasi (misalnya prinsip kebutuhan untuk mengetahui) dan level keamanan informasi dan klasifikasi informasi (lihat 5.10, 5.12, 5.13);
e) pembatasan akses privilese (lihat 8.2);
f) segregasi tugas (lihat 5.3);
g) legislasi, regulasi, dan setiap kewajiban kontraktual yang relevan mengenai pembatasan akses data atau layanan (lihat 5.31, 5.32, 5.33, 5.34, 8.3);
h) segregasi fungsi kontrol akses (misalnya permintaan akses, otorisasi akses, administrasi akses);
i) otorisasi formal atas permintaan akses (lihat 5.16 dan 5.18);
j) manajemen hak akses (lihat 5.18);
k) pembuatan log (lihat 8.15).

Aturan kontrol akses sebaiknya diimplementasikan dengan mendefinisikan dan memetakan hak akses dan pembatasan yang sesuai untuk entitas yang relevan (lihat 5.16). Entitas dapat mewakili pengguna manusia serta item teknis atau logis (misalnya mesin, peranti, atau layanan). Untuk menyederhanakan manajemen kontrol akses, dapat ditetapkan peran spesifik ke grup entitas.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Hal-hal berikut sebaiknya diperhitungkan saat mendefinisikan dan mengimplementasikan aturan kontrol akses:

a) konsistensi antara hak akses dan klasifikasi informasi;
b) konsistensi antara hak akses dan kebutuhan dan persyaratan keamanan perimeter fisik;
c) mempertimbangkan semua tipe koneksi yang tersedia di lingkungan terdistribusi sehingga entitas hanya diberi akses ke informasi dan aset terkait lainnya, termasuk jaringan dan layanan jaringan, yang diotorisasi untuk digunakan;
d) mempertimbangkan bagaimana elemen atau faktor yang relevan dengan kontrol akses dinamis dapat direfleksikan.

Informasi lain

Sering kali terdapat banyak prinsip menyeluruh yang digunakan dalam konteks kontrol akses. Dua prinsip yang paling sering digunakan adalah:

a) kebutuhan-untuk-mengetahui (*need-to-know*): suatu entitas hanya diberikan akses ke informasi dimana entitas syaratkan untuk melaksanakan tugasnya (tugas atau peran yang berbeda berarti informasi kebutuhan untuk mengetahui yang berbeda sehingga memerlukan profil akses yang berbeda);
b) kebutuhan-untuk-menggunakan (*need-to-use*): suatu entitas hanya diberikan akses ke infrastruktur teknologi informasi yang menjadi kebutuhannya.

Perlu kehati-hatian ketika menspesifikasikan aturan kontrol akses dengan mempertimbangkan:

a) penetapan aturan berdasarkan premis privilese terendah, "Semuanya secara umum dilarang kecuali diizinkan secara tegas", daripada aturan yang lebih lemah, "Semuanya secara umum diizinkan kecuali dilarang secara tegas";
b) perubahan dalam label informasi (lihat 5.13) yang dimulai secara otomatis oleh fasilitas pemrosesan informasi dan yang diinisiasi atas diskresi pengguna;
c) perubahan izin pengguna yang diinisiasi secara otomatis oleh sistem informasi dan yang dimulai oleh administrator;
d) kapan mendefinisikan dan secara reguler mereviu persetujuan.

Aturan kontrol akses sebaiknya didukung oleh prosedur yang terdokumentasi (lihat 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) dan tanggung jawab yang didefinisikan (lihat 5.2, 5.17).

Ada beberapa cara untuk mengimplementasikan kontrol akses, seperti MAC (*mandatory access control*), DAC (*discretionary access control*), RBAC (*role-based access control*), dan ABAC (*attribute-based access control*).

Aturan kontrol akses juga dapat berisi elemen dinamis (misalnya fungsi yang mengevaluasi akses masa lalu atau nilai lingkungan tertentu). Aturan kontrol akses dapat diimplementasikan dalam granularitas yang berbeda, mulai dari mencakup seluruh jaringan atau sistem hingga bidang data spesifik, dan juga dapat mempertimbangkan properti seperti lokasi pengguna atau tipe koneksi jaringan yang digunakan untuk akses. Prinsip ini dan bagaimana kontrol akses granular didefinisikan dapat memiliki dampak biaya yang signifikan. Aturan yang lebih kuat dan granularitas lebih biasanya menimbulkan biaya yang lebih tinggi. Persyaratan bisnis dan konsiderasi risiko sebaiknya digunakan untuk mendefinisikan aturan kontrol akses mana yang diterapkan dan granularitas yang dipersyaratkan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.16 Manajemen identitas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Siklus hidup penuh identitas sebaiknya dimanajemeni.

Tujuan
Untuk mengizinkan identifikasi unik dari individu dan sistem tertentu yang mengakses informasi organisasi dan aset terkait lainnya dan memungkinkan penetapan hak akses yang tepat.

Panduan
Proses yang digunakan dalam konteks manajemen identitas sebaiknya memastikan bahwa:
a) untuk identitas yang diberikan kepada orang, identitas spesifik hanya terkait dengan satu person untuk dapat membuat orang tersebut akuntabel atas tindakan yang dilakukan dengan identitas spesifik ini;
b) identitas yang diberikan kepada beberapa orang (misalnya berbagi identitas) hanya diizinkan jika diperlukan untuk alasan bisnis atau operasional dan tunduk pada persetujuan dan dokumentasi khusus;
c) identitas yang diberikan kepada entitas tanpa manusia tunduk pada persetujuan yang dipisahkan secara tepat dan pengawasan independen yang terus menerus;
d) identitas dinonaktifkan atau dipindahkan secara tepat waktu jika tidak lagi dipersyaratkan (misalnya jika entitas yang berkaitan dengan mereka dihapus atau tidak lagi digunakan, atau jika orang yang terkait dengan identitas tersebut telah meninggalkan organisasi atau berpindah tugas);
e) dalam domain tertentu, identitas tunggal dipetakan ke entitas tunggal, [yaitu pemetaan beberapa identitas ke entitas yang sama dalam konteks yang sama (duplikasi identitas) dihindari];
f) rekaman semua peristiwa penting mengenai penggunaan dan manajemen identitas pengguna dan informasi autentikasi disimpan.

Organisasi sebaiknya memiliki proses pendukung untuk menangani perubahan informasi yang terkait dengan identitas pengguna. Proses ini dapat mencakup verifikasi ulang dokumen tepercaya terkait seseorang.

Ketika menggunakan identitas yang disediakan atau diterbitkan oleh pihak ketiga (misalnya kredensial media sosial), organisasi sebaiknya memastikan identitas pihak ketiga memberikan level kepercayaan yang dipersyaratkan serta setiap risiko terkait telah diketahui dan ditangani secara memadai. Ini dapat mencakup kontrol yang terkait dengan pihak ketiga (lihat 5.19) serta kontrol yang terkait dengan informasi autentikasi terkait (lihat 5.17).

Informasi lain
Menyediakan atau mencabut akses ke informasi dan aset terkait lainnya biasanya merupakan prosedur multi-langkah:
a) mengonfirmasi persyaratan bisnis untuk identitas yang akan ditetapkan;
b) memverifikasi identitas suatu entitas sebelum mengalokasikan identitas yang logis;
c) menetapkan identitas;
mengonfigurasi dan mengaktifkan identitas. Ini juga termasuk konfigurasi dan pengaturan awal layanan autentikasi terkait;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) memberikan atau mencabut hak akses tertentu atas identitas, berdasarkan otorisasi atau keputusan hak yang tepat (lihat 5.18).

5.17 Informasi autentikasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Alokasi dan manajemen informasi autentikasi sebaiknya dikontrol dengan proses manajemen, termasuk memberi saran personel tentang penanganan informasi autentikasi yang tepat.

Tujuan
Untuk memastikan autentikasi entitas yang layak dan mencegah kegagalan proses autentikasi.

Panduan
Alokasi informasi autentikasi
Proses alokasi dan manajemen sebaiknya memastikan:
a) kata sandi pribadi atau *personal identification numbers* (PIN) yang dihasilkan secara otomatis selama proses pendaftaran sebagai informasi autentikasi konfidensial sementara tidak dapat ditebak dan unik untuk setiap orang, dan pengguna dipersyaratkan mengubahnya setelah penggunaan pertama;
b) prosedur ditetapkan untuk memverifikasi identitas pengguna sebelum memberikan informasi autentikasi baru, pengganti, atau sementara;
c) informasi autentikasi, termasuk informasi autentikasi sementara, dikirimkan kepada pengguna dengan cara yang aman (misalnya melalui saluran yang terautentikasi dan terlindungi) dan menghindari penggunaan pesan surat elektronik (teks terang) yang tidak terlindungi;
d) pengguna mengakui penerimaan informasi autentikasi;
e) informasi autentikasi bawaan sebagaimana telah ditentukan sebelumnya atau disediakan oleh pemasok diubah segera setelah instalasi sistem atau perangkat lunak;
f) rekaman peristiwa signifikan mengenai alokasi dan manajemen informasi autentikasi disimpan dan konfidensialitasnya dijaga, dan bahwa metode penyimpan-rekaman disetujui (misalnya dengan menggunakan alat pengelola kata sandi yang disetujui).

Tanggung jawab pengguna
Setiap person yang memiliki akses ke atau menggunakan informasi autentikasi sebaiknya disarankan untuk memastikan bahwa:
a) informasi autentikasi konfidensial seperti kata sandi konfidensial. Informasi autentikasi konfidensial pribadi tidak boleh dibagikan dengan siapa pun. Informasi autentikasi konfidensial yang digunakan dalam konteks identitas yang dihubungkan dengan beberapa pengguna atau dihubungkan dengan entitas non-pribadi hanya dibagikan dengan orang yang terotorisasi;
b) informasi autentikasi yang terdampak atau bobol segera diubah setelah notifikasi atau indikasi lain mengenai sebuah pembobolan;
c) ketika kata sandi digunakan sebagai informasi autentikasi, perlu dipilih kata sandi yang kuat sesuai dengan rekomendasi praktik terbaik, misalnya:
    1) kata sandi tidak didasarkan pada apa pun yang mudah ditebak atau diperoleh orang lain menggunakan informasi terkait (misalnya nama, nomor telepon, dan tanggal lahir);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

2) kata sandi tidak didasarkan pada kata kamus atau kombinasinya;
3) menggunakan kata sandi yang mudah diingat dan mencoba menyertakan karakter kombinasi abjad-angka dan karakter khusus;
4) kata sandi memiliki panjang minimum;

d) kata sandi yang sama tidak digunakan di seluruh layanan dan sistem yang berbeda;
e) kewajiban untuk mengikuti aturan ini juga termasuk dalam syarat dan ketentuan kerja (lihat 6.2).

Sistem manajemen kata sandi

Ketika kata sandi digunakan sebagai informasi autentikasi, sistem manajemen kata sandi sebaiknya:

a) memungkinkan pengguna untuk memilih dan mengubah kata sandinya sendiri dan menyertakan prosedur konfirmasi untuk mengatasi kesalahan input;
b) menerapkan kata sandi yang kuat sesuai dengan rekomendasi praktik yang baik (lihat c) "Tanggung jawab pengguna";
c) memaksa pengguna untuk mengubah kata sandi pada saat pertama kali masuk;
d) menerapkan perubahan kata sandi jika diperlukan, misalnya setelah insiden keamanan, atau setelah pemutusan hubungan kerja atau perubahan pekerjaan ketika pengguna telah mengetahui kata sandi untuk identitas yang tetap aktif (misalnya identitas bersama);
e) mencegah penggunaan ulang kata sandi sebelumnya;
f) mencegah penggunaan kata sandi yang umum digunakan dan nama pengguna yang dikompromikan, kombinasi kata sandi dari sistem yang diretas;
g) tidak menampilkan kata sandi di layar saat dimasukkan;
h) menyimpan dan mengirimkan kata sandi dalam bentuk terlindungi.

Enkripsi dan *hashing* kata sandi sebaiknya dilakukan sesuai dengan teknik kriptografi yang disetujui untuk kata sandi (lihat 8.24).

Informasi lain

Kata sandi atau frasa sandi adalah tipe informasi autentikasi yang umum digunakan dan merupakan sarana umum untuk memverifikasi identitas pengguna. Jenis informasi autentikasi lainnya adalah kunci kriptografi, data yang disimpan pada token perangkat keras (misalnya kartu pintar) yang menghasilkan kode autentikasi dan data biometrik seperti pemindaian iris atau sidik jari. Informasi tambahan dapat ditemukan di seri ISO/IEC 24760.

Mesyaratkan untuk sering mengubah kata sandi dapat menjadi masalah karena pengguna dapat terganggu oleh perubahan yang sering terjadi, lupa kata sandi baru, mencatatnya di tempat yang tidak aman, atau memilih kata sandi yang tidak aman. Penyediaan *single sign on* (SSO) atau alat manajemen autentikasi lainnya (misalnya brankas kata sandi) mengurangi jumlah informasi autentikasi yang diperlukan pengguna untuk memproteksi sehingga dapat meningkatkan efektivitas kontrol ini. Namun, alat-alat ini juga dapat meningkatkan dampak pengungkapan informasi autentikasi.

Beberapa aplikasi mensyaratkan kata sandi pengguna ditetapkan oleh otoritas independen. Dalam kasus tersebut, a), c), dan d) dari "Sistem manajemen kata sandi" tidak berlaku.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.18 Hak akses

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Hak akses terhadap informasi dan aset terkait lainnya sebaiknya disediakan, direviu, dimodifikasi, dan dipindahkan sesuai dengan kebijakan topik spesifik organisasi dan aturan tentang kontrol akses.

Tujuan
Untuk memastikan akses ke informasi dan aset terkait lainnya didefinisikan dan diotorisasi sesuai dengan persyaratan bisnis.

Panduan
Penyediaan dan pencabutan hak akses
Proses penyediaan untuk menetapkan atau mencabut hak akses fisik dan logikal yang diberikan kepada identitas terautentikasi entitas sebaiknya mencakup:
a) memperoleh otorisasi dari pemilik informasi dan aset terkait lainnya untuk penggunaan informasi dan aset terkait lainnya (lihat 5.9). Persetujuan terpisah untuk hak akses oleh manajemen juga mungkin tepat;
b) mempertimbangkan persyaratan bisnis serta kebijakan dan aturan topik spesifik organisasi tentang kontrol akses;
c) mempertimbangkan segregasi tugas, termasuk pemisahan peran persetujuan dan implementasi hak akses dan pemisahan peran yang bertentangan;
d) memastikan hak akses dipindahkan ketika seseorang tidak perlu mengakses informasi dan aset terkait lainnya, khususnya memastikan hak akses pengguna yang telah meninggalkan organisasi dipindahkan secara tepat waktu;
e) mempertimbangkan untuk memberikan hak akses temporer untuk jangka waktu terbatas dan mencabutnya pada tanggal kedaluwarsa, khususnya untuk personel temporer atau akses temporer yang diperlukan oleh personel;
f) memverifikasi bahwa level akses yang diberikan sesuai dengan kebijakan topik spesifik tentang kontrol akses (lihat 5.15) dan konsisten dengan persyaratan keamanan informasi lainnya seperti segregasi tugas (lihat 5.3);
g) memastikan bahwa hak akses diaktifkan (misalnya oleh penyedia layanan) hanya setelah prosedur otorisasi berhasil diselesaikan;
h) memelihara rekaman pusat hak akses yang diberikan kepada pengidentifikasi pengguna (identitas, logis atau fisik) untuk mengakses informasi dan aset terkait lainnya;
i) memodifikasi hak akses pengguna yang telah berubah tugas atau pekerjaan;
j) menghapus atau menyesuaikan hak akses fisik dan logikal, yang dapat dilakukan dengan pemindahan, pencabutan, atau penggantian kunci, informasi autentikasi, kartu identifikasi atau langganan;
k) memelihara rekaman perubahan terhadap hak akses logikal dan fisik pengguna.

Reviu hak akses
Reviu rutin tentang hak akses fisik dan logikal sebaiknya mempertimbangkan hal-hal berikut:
a) hak akses pengguna setelah setiap perubahan dalam organisasi yang sama (misalnya perubahan tugas, promosi, demosi) atau pemutusan hubungan kerja (lihat 6.1 hingga 6.5);
b) otorisasi untuk hak akses privilese.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Konsiderasi sebelum perubahan atau pemutusan hubungan kerja
Hak akses pengguna atas informasi dan aset terkait lainnya sebaiknya direviu dan disesuaikan atau dipindahkan sebelum perubahan atau pemutusan hubungan kerja berdasarkan evaluasi faktor risiko seperti:

a) apakah penghentian atau perubahan dimulai oleh pengguna atau oleh manajemen dan alasan penghentian;
b) tanggung jawab pengguna saat ini;
c) nilai aset yang saat ini dapat diakses.

Informasi lain
Sebaiknya diberikan konsiderasi untuk menetapkan peran akses pengguna berdasarkan persyaratan bisnis yang merangkum sejumlah hak akses ke dalam profil tipikal akses pengguna. Permintaan akses dan reviu hak akses lebih mudah dimanajemeni pada level peran tersebut daripada pada level hak tertentu.

Sebaiknya diberikan konsiderasi untuk memasukkan pasal dalam kontrak personel dan kontrak layanan yang menentukan sanksi jika personel mencoba melakukan akses yang takterotorisasi (lihat 5.20, 6.2, 6.4, 6.6).
Dalam kasus penghentian yang dimulai oleh manajemen, personel yang tidak puas atau pengguna pihak eksternal dapat dengan sengaja merusak informasi atau menyabotase fasilitas pemrosesan informasi. Dalam kasus person yang mengundurkan diri atau dibubarkan, mereka dapat tergoda untuk mengumpulkan informasi untuk digunakan di masa mendatang.

Pengklonaan adalah cara yang efisien bagi organisasi untuk menetapkan akses ke pengguna. Namun, pengklonaan sebaiknya dilakukan dengan hati-hati berdasarkan berbagai peran yang diidentifikasi oleh organisasi daripada hanya melakukan pengklonaan identitas dengan semua hak akses terkait. Pengklonaan memiliki risiko melekat yang mengakibatkan hak akses eksesif terhadap informasi dan aset terkait lainnya.

5.19 Keamanan informasi dalam hubungan pemasok

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Proses dan prosedur sebaiknya didefinisikan dan diimplementasikan untuk memanajemeni risiko keamanan informasi yang terkait dengan penggunaan produk atau layanan pemasok.

Tujuan
Untuk memelihara level keamanan informasi yang disepakati dalam hubungan pemasok.

Panduan
Organisasi sebaiknya menetapkan kebijakan topik spesifik tentang hubungan pemasok kepada semua pihak terkait yang relevan.

Organisasi sebaiknya mengidentifikasi dan mengimplementasi proses dan prosedur untuk mengurusi risiko keamanan yang terkait dengan penggunaan produk dan layanan yang disediakan oleh pemasok. Ini juga sebaiknya berlaku untuk penggunaan sumber daya organisasi penyedia layanan *cloud*. Proses dan prosedur ini sebaiknya mencakup hal yang akan diimplementasikan oleh organisasi, sejalan dengan organisasi tersebut membutuhkan pemasok untuk mengimplementasikan untuk permulaan penggunaan produk atau layanan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

pemasok atau untuk penghentian penggunaan produk dan layanan pemasok, seperti:

a) mengidentifikasi dan mendokumentasikan tipe pemasok (misalnya layanan TIK, logistik, utilitas, layanan finansial, komponen infrastruktur TIK) yang dapat memengaruhi konfidensialitas, integritas, dan availabilitas informasi organisasi;
b) menetapkan cara mengevaluasi dan memilih pemasok sesuai dengan sensitivitas informasi, produk, dan layanan (misalnya dengan analisis pasar, referensi pelanggan, reviu dokumen, asesmen di lokasi, sertifikasi);
c) mengevaluasi dan memilih produk atau layanan pemasok yang memiliki kontrol keamanan informasi yang cukup dan mereviunya; khususnya, akurasi dan kelengkapan kontrol yang diimplementasikan oleh pemasok yang memastikan integritas informasi dan pemrosesan informasi pemasok serta keamanan informasi organisasi;
d) mendefinisikan informasi organisasi, layanan TIK, dan infrastruktur fisik yang dapat diakses, dimonitor, dikontrolkan, atau digunakan oleh pemasok;
e) mendefinisikan tipe komponen dan layanan infrastruktur TIK yang disediakan oleh pemasok yang dapat mendampak konfidensialitas, integritas, dan availabilitas informasi organisasi;
f) menilai dan memanajemeni risiko keamanan informasi yang terkait dengan:
    1) penggunaan informasi organisasi dan aset terkait lainnya oleh pemasok, termasuk risiko yang berasal dari personel pemasok yang berpotensi berbahaya;
    2) kerusakan atau kerentanan produk (termasuk komponen dan subkomponen perangkat lunak yang digunakan dalam produk ini) atau layanan yang disediakan oleh pemasok;
g) memonitor kepatuhan terhadap persyaratan keamanan informasi yang ditetapkan untuk setiap tipe pemasok dan tipe akses, termasuk reviu pihak ketiga dan validasi produk;
h) mitigasi ketidakpatuhan pemasok, baik terdeteksi melalui pemonitoran atau dengan cara lain;
i) menangani insiden dan kontingensi yang terkait dengan produk dan layanan pemasok termasuk tanggung jawab organisasi dan pemasok;
j) resiliensi dan, jika perlu, langkah-langkah pemulihan dan kontingensi untuk memastikan availabilitas informasi dan pemrosesan informasi pemasok serta availabilitas informasi organisasi;
k) kesadaran dan pelatihan bagi personel organisasi yang berinteraksi dengan personel pemasok mengenai aturan keterlibatan yang tepat, kebijakan topik spesifik, proses, dan prosedur serta perilaku berdasarkan tipe pemasok dan level akses pemasok ke sistem dan informasi organisasi;
l) memanajemeni transfer informasi yang diperlukan, aset terkait lainnya, dan hal lain yang perlu diubah dan memastikan bahwa keamanan informasi terpelihara selama periode transfer;
m) persyaratan untuk memastikan pengakhiran hubungan pemasok yang aman, termasuk:
    1) pencabutan hak akses;
    2) penanganan informasi
    3) penentuan kepemilikan kekayaan intelektual yang dikembangkan selama keterlibatan;
    4) portabilitas informasi dalam hal perubahan pemasok atau swadaya;
    5) manajemen rekaman;
    6) pengembalian aset;
    7) penghapusan informasi dan aset terkait lainnya dengan aman;
    8) persyaratan konfidensialitas berkelanjutan;
n) level keamanan personel dan keamanan fisik yang diharapkan dari personel dan fasilitas pemasok.

Prosedur untuk melanjutkan pemrosesan informasi jika pemasok tidak dapat memasok produk atau layanannya (misalnya karena insiden, karena pemasok tidak lagi beroperasi, atau tidak lagi menyediakan beberapa komponen karena kemajuan teknologi) sebaiknya

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dipertimbangkan untuk menghindari keterlambatan dalam menyiapkan produk atau layanan pengganti (misalnya mengidentifikasi pemasok alternatif terlebih dahulu atau selalu menggunakan pemasok alternatif).

Informasi lain
Dalam hal tidak mungkin bagi organisasi untuk memberlakukan persyaratan pada pemasok, organisasi hendaknya:
a) mempertimbangkan panduan yang diberikan dalam kontrol ini dalam membuat keputusan tentang memilih pemasok dan produk atau layanannya;
b) mengimplementasikan kontrol kompensasi seperlunya berdasarkan asesmen risiko.

Informasi dapat berisiko di tangan pemasok dengan manajemen keamanan informasi yang tidak memadai. kontrol sebaiknya ditentukan dan diterapkan untuk memanajemeni akses pemasok ke informasi dan aset terkait lainnya. Misalnya, jika ada kebutuhan spesial untuk konfidensialitas informasi, perjanjian nirungkap atau teknik kriptografi dapat digunakan. Contoh lain adalah risiko proteksi data pribadi ketika perjanjian pemasok melibatkan transfer, atau akses ke, informasi lintas batas. Organisasi perlu menyadari bahwa tanggung jawab legal atau kontraktual untuk memproteksi informasi tetap ada pada organisasi.
Risiko juga dapat disebabkan oleh kontrol komponen infrastruktur TIK atau layanan yang disediakan oleh pemasok yang tidak memadai. Komponen atau layanan yang malafungsi atau rentan dapat menyebabkan pelanggaran keamanan informasi dalam organisasi atau ke entitas lain (misalnya, dapat menyebabkan infeksi perangkat perusak, serangan, atau bahaya lain pada entitas selain organisasi).

Lihat ISO/IEC 27036-2 untuk detail lebih lanjut.

5.20 Menangani keamanan informasi dalam perjanjian pemasok

Tipe kontrol	Properti Keamanan informasi	Konsep Keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Persyaratan keamanan informasi yang relevan sebaiknya ditetapkan dan disepakati dengan tiap pemasok berdasarkan tipe hubungan pemasok.

Tujuan
Untuk memelihara level keamanan informasi yang disepakati dalam hubungan pemasok.

Panduan
Perjanjian pemasok sebaiknya dibuat dan didokumentasikan untuk memastikan bahwa ada pemahaman yang jelas antara organisasi dan pemasok mengenai kewajiban kedua belah pihak untuk memenuhi persyaratan keamanan informasi yang relevan.

Ketentuan berikut dapat dipertimbangkan untuk dimasukkan dalam perjanjian untuk memenuhi persyaratan keamanan informasi yang diidentifikasi:
a) deskripsi informasi yang akan diberikan atau diakses dan metode pemberian atau akses informasi;
b) klasifikasi informasi menurut skema klasifikasi organisasi (lihat 5.10, 5.12, 5.13);
c) pemetaan antara skema klasifikasi organisasi sendiri dan skema klasifikasi pemasok;
d) persyaratan legal, satutori, regulatori, dan kontraktual, termasuk proteksi data, penanganan *personally identifiable information* (PII), hak kekayaan intelektual, serta hak

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

cipta dan deskripsi tentang bagaimana memastikan persyaratan tersebut terpenuhi;

e) kewajiban setiap pihak dalam kontraktrual untuk mengimplementasikan serangkaian kontrol yang disepakati, termasuk kontrol akses, reviu kinerja, pemonitoran, pelaporan dan audit, serta kewajiban pemasok untuk mematuhi persyaratan keamanan informasi organisasi;
f) aturan penggunaan yang akseptabel terhadap informasi dan aset terkait lainnya, termasuk penggunaan yang tidak akseptabel jika diperlukan;
g) prosedur atau ketentuan untuk otorisasi dan pemindahan otorisasi untuk penggunaan informasi organisasi dan aset terkait lainnya oleh personel pemasok (misalnya melalui daftar eksplisit personel pemasok yang terotorisasi untuk menggunakan informasi organisasi dan aset terkait lainnya);
h) persyaratan keamanan informasi mengenai infrastruktur TIK pemasok; khususnya, persyaratan keamanan informasi minimum untuk setiap tipe informasi dan tipe akses untuk menjadi dasar setiap perjanjian pemasok individual berdasarkan kebutuhan bisnis dan kriteria risiko organisasi;
i) ganti rugi dan perbaikan atas kegagalan kontraktor untuk memenuhi persyaratan;
j) persyaratan dan prosedur manajemen insiden (terutama notifikasi dan kolaborasi selama perbaikan insiden);
k) persyaratan pelatihan dan kesadaran untuk prosedur dan persyaratan keamanan informasi spesifik (misalnya untuk respons insiden, prosedur otorisasi);
l) ketentuan subkontrak yang relevan, termasuk kontrol yang perlu diimplementasikan, seperti perjanjian tentang penggunaan subpemasok (misalnya mensyaratkan subpemasok mematuhi kewajiban yang sama dengan pemasok, mensyaratkan pemasok memiliki daftar subpemasok, dan notifikasi sebelum perubahan);
m) kontak yang relevan, termasuk narahubung untuk masalah keamanan informasi;
n) persyaratan skrining, jika diizinkan secara legal, untuk personel pemasok, termasuk tanggung jawab untuk melakukan skrining dan prosedur notfikasi jika skrining belum selesai atau jika hasilnya menimbulkan keraguan atau kekhawatiran;
o) mekanisme bukti dan keyakinan pembuktian pihak ketiga untuk persyaratan keamanan informasi yang relevan terkait dengan proses pemasok dan laporan independen tentang efektivitas kontrol;
p) hak untuk mengaudit proses dan kontrol pemasok yang terkait dengan perjanjian;
q) kewajiban pemasok untuk secara berkala menyampaikan laporan tentang efektivitas kontrol dan perjanjian tentang perbaikan tepat waktu atas masalah yang diangkat dalam laporan;
r) penyelesaian kerusakan dan proses penyelesaian konflik;
s) menyediakan cadangan yang selaras dengan kebutuhan organisasi (dalam hal frekuensi dan tipe serta lokasi penyimpanan);
t) memastikan availabilitas fasilitas alternatif (yaitu lokasi pemulihan bencana) tidak rentan terhadap ancaman yang sama dengan fasilitas utama dan konsiderasi untuk kontrol *fall back* (kontrol alternatif) jika kontrol utama gagal;
u) memiliki proses manajemen perubahan yang memastikan notifikasi awal kepada organisasi dan kemungkinan organisasi tidak menerima perubahan;
v) kontrol keamanan fisik yang sesuai dengan klasifikasi informasi;
w) kontrol transfer informasi untuk memproteksi informasi selama transfer fisik atau transmisi logikal;
x) pasal terminasi setelah berakhirnya perjanjian termasuk manajemen arsip, pengembalian aset, penghapusan informasi dan aset terkait lainnya secara aman, dan kewajiban konfidensialitas yang sedang berlangsung;
y) penyediaan metode penghancuran informasi organisasi yang disimpan oleh pemasok segera setelah tidak lagi diperlukan secara aman;
z) memastikan, pada akhir kontrak, dukungan serah terima kepada pemasok lain atau kepada organisasi itu sendiri.

Organisasi sebaiknya menetapkan dan memelihara daftar perjanjian dengan pihak eksternal (misalnya kontrak, nota kesepahaman, perjanjian berbagi informasi) untuk melacak

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

pergerakan informasinya. Organisasi juga sebaiknya secara reguler mereviu, memvalidasi, dan memperbarui perjanjiannya dengan pihak eksternal untuk memastikan mereka masih diperlukan dan sesuai untuk tujuan dengan pasal keamanan informasi yang relevan.

Informasi lain
Perjanjian dapat sangat beragam untuk berbagai organisasi yang berbeda dan di antara berbagai tipe pemasok. Oleh karena itu, perlu kehati-hatian untuk menyertakan semua persyaratan yang relevan untuk menangani risiko keamanan informasi.

Untuk detail tentang perjanjian pemasok, lihat seri ISO/IEC 27036. Untuk perjanjian layanan *cloud*, lihat seri ISO/IEC 19086.

5.21 Memanajemeni keamanan informasi dalam rantai pasokan TIK

Tipe kontrol	Properti Keamanan informasi	Konsep Keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Proses dan prosedur sebaiknya didefinisikan dan diimplementasikan untuk memanajemeni risiko keamanan informasi yang terkait dengan rantai pasokan produk dan layanan TIK.

Tujuan
Untuk memelihara level keamanan informasi yang disepakati dalam hubungan pemasok.

Panduan
Topik berikut sebaiknya dipertimbangkan untuk membahas keamanan informasi dalam keamanan rantai pasokan TIK selain persyaratan keamanan informasi umum untuk hubungan pemasok:

a) mendefinisikan persyaratan keamanan informasi untuk diterapkan pada akuisisi produk atau layanan TIK;
b) mensyaratkan bahwa pemasok layanan TIK menginformasikan persyaratan keamanan organisasi di seluruh rantai pasokan jika mereka melakukan subkontrak untuk bagian dari layanan TIK yang diberikan kepada organisasi;
c) mensyaratkan bahwa pemasok produk TIK menyebarluaskan praktik keamanan yang sesuai di seluruh rantai pasokan jika produk-produk tersebut mencakup komponen yang dibeli atau diperoleh dari pemasok lain atau entitas lain (misalnya subkontrak developer perangkat lunak dan penyedia komponen perangkat keras);
d) meminta pemasok produk TIK memberikan informasi yang menjelaskan komponen perangkat lunak yang digunakan dalam produk;
e) meminta pemasok produk TIK memberikan informasi yang menjelaskan fungsi keamanan yang diimplementasikan dari produk mereka dan konfigurasi yang diperlukan untuk operasi yang aman;
f) implementasi proses pemonitoran dan metode yang akseptabel untuk memvalidasi bahwa produk dan layanan TIK yang dikirimkan sesuai dengan persyaratan keamanan yang dinyatakan. Contoh, metode reviu pemasok tersebut dapat mencakup pengujian penetrasi dan bukti atau validasi pengesahan pihak ketiga untuk operasi keamanan informasi pemasok;
g) implementasi proses untuk mengidentifikasi dan mendokumentasikan komponen produk atau layanan yang sangat penting untuk memelihara fungsionalitas sehingga memerlukan peningkatan perhatian, pengawasan, dan tindak lanjut yang diperlukan ketika dibangun di luar organisasi terutama jika pemasok mengalihdayakan aspek

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

produk atau komponen layanan kepada pemasok lain;
h) mendapatkan keyakinan bahwa komponen kritis dan asalnya dapat ditelusuri di seluruh rantai pasokan;
i) mendapatkan keyakinan bahwa produk TIK yang dikirimkan berfungsi sesuai harapan tanpa fitur yang tidak terduga atau tidak diinginkan;
j) mengimplementasikan proses untuk memastikan bahwa komponen dari pemasok asli dan tidak diubah dari spesifikasinya. Contoh langkah-langkahnya termasuk label anti-gangguan, verifikasi *hash* kriptografi, atau tanda tangan digital. Pemonitoran terhadap kinerja di luar spesifikasi dapat menjadi indikator adanya gangguan atau pemalsuan. Pencegahan dan deteksi gangguan sebaiknya diimplementasikan selama beberapa tahap dalam siklus hidup pengembangan sistem, termasuk desain, pengembangan, integrasi, pengoperasian, dan pemeliharaan;
k) mendapatkan keyakinan bahwa produk TIK mencapai level keamanan yang dipersyaratkan, misalnya melalui *Common Criteria Recognition Arrangement*;
l) Sertifikasi formal atau skema evaluasi seperti mendefinisikan aturan untuk berbagi informasi mengenai rantai pasokan dan potensi masalah dan pembobolan di antara organisasi dan pemasok;
m) mengimplementasikan proses spesifik untuk memanajemeni siklus hidup komponen TIK dan availabilitas serta risiko keamanan terkait, termasuk memanajemeni risiko komponen yang tidak lagi tersedia karena pemasok tidak lagi beroperasi atau pemasok tidak lagi menyediakan komponen ini karena kemajuan teknologi. Identifikasi pemasok alternatif dan proses untuk mentransfer perangkat lunak dan kompetensi ke pemasok alternatif sebaiknya dipertimbangkan.

Informasi lain
Praktik manajemen risiko rantai pasokan TIK spesifik didasarkan pada keamanan informasi umum, kualitas, manajemen proyek, dan praktik rekayasa sistem tetapi tidak serta-merta menggantinya.

Organisasi disarankan untuk bekerja sama dengan pemasok untuk memahami rantai pasokan TIK dan hal-hal yang memiliki efek penting pada produk dan layanan yang disediakan. Organisasi dapat memengaruhi praktik keamanan informasi rantai pasokan TIK dengan membuat perjanjian yang jelas dengan pemasoknya mereka tentang hal-hal yang sebaiknya ditangani oleh pemasok lain dalam rantai pasokan TIK.

TIK sebaiknya diperoleh dari sumber-sumber yang memiliki reputasi baik. Keandalan perangkat lunak dan perangkat keras adalah masalah kontrol kualitas. Meskipun umumnya tidak mungkin bagi organisasi untuk memeriksa sistem kontrol kualitas dari vendornya, organisasi dapat membuat asesmen yang dapat diandalkan berdasarkan reputasi vendor.

Rantai pasokan TIK seperti yang ditujukan di sini termasuk layanan *cloud*. Contoh rantai pasokan TIK adalah:
a) penyediaan layanan *cloud*, yaitu penyedia layanan *cloud* bergantung pada developer perangkat lunak, penyedia layanan telekomunikasi, penyedia perangkat keras;
b) IoT, yaitu layanan melibatkan pemanufaktur perangkat, penyedia layanan *cloud* (misalnya operator platform IoT), developer aplikasi seluler dan web, vendor pustaka perangkat lunak;
c) layanan *hosting*, yaitu penyedia mengandalkan meja layanan eksternal termasuk level dukungan pertama, kedua, dan ketiga.

Lihat ISO/IEC 27036-3 untuk detail lebih lanjut termasuk panduan asesmen risiko.

Tag Software identification (SWID) juga dapat membantu untuk mencapai keamanan informasi yang lebih baik dalam rantai pasokan, dengan memberikan informasi tentang sumber perangkat lunak. Lihat ISO/IEC 19770-2 untuk detail lebih lanjut.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.22 Pemonitoran, reviu, dan manajemen perubahan layanan pemasok

Tipe kontrol	Properti Keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Keamanan_hubungan_pemasok #Keyakinan_keamanan_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Pertahanan

Kontrol
Organisasi sebaiknya secara reguler memonitor, mereviu, mengevaluasi, dan memanajemeni perubahan dalam praktik keamanan informasi pemasok dan penyampaian layanan.

Tujuan
Memelihara level keamanan informasi dan penyampaian layanan yang disepakati sejalan dengan perjanjian pemasok.

Panduan
Pemonitoran, reviu dan manajemen perubahan layanan pemasok sebaiknya memastikan syarat dan ketentuan keamanan informasi dari perjanjian dipatuhi, insiden dan problem keamanan informasi dimanajemeni dengan benar, dan perubahan dalam layanan pemasok atau status bisnis tidak berdampak pada penyampaian layanan.

kontrol ini sebaiknya melibatkan proses untuk memanajemeni hubungan antara organisasi dan pemasok untuk:

a) memonitor level kinerja layanan untuk memverifikasi kepatuhan terhadap perjanjian;
b) memonitor perubahan yang dilakukan oleh pemasok termasuk:
    1) peningkatan layanan yang ditawarkan saat ini;
    2) pengembangan aplikasi dan sistem baru;
    3) modifikasi atau pembaruan kebijakan dan prosedur pemasok;
    4) kontrol baru atau yang diubah untuk menyelesaikan insiden keamanan informasi dan untuk meningkatkan keamanan informasi;
c) memonitor perubahan dalam layanan pemasok termasuk:
    1) perubahan dan peningkatan jaringan;
    2) penggunaan teknologi baru;
    3) adopsi produk baru atau versi atau keluaran yang lebih mutakhir;
    4) alat dan lingkungan pengembangan baru;
    5) perubahan fisik lokasi fasilitas pelayanan;
    6) pergantian subpemasok;
    7) subkontrak dengan pemasok lain;
d) mereviu laporan layanan yang dihasilkan oleh pemasok dan mengatur rapat kemajuan rutin sebagaimana ditentukan dalam perjanjian;
e) melakukan audit terhadap pemasok dan subpemasok, sehubungan dengan reviu laporan auditor independen, jika tersedia, dan tindak lanjut atas masalah yang diidentifikasi;
f) menyediakan informasi tentang insiden keamanan informasi dan mereviu informasi ini sebagaimana ditentukan dalam perjanjian dan pedoman serta prosedur pendukung apa pun;
g) mereviu jejak audit pemasok dan rekaman peristiwa keamanan informasi, problem operasional, kegagalan, pelacakan kesalahan, dan disrupsi yang terkait dengan layanan yang disediakan;
h) merespons dan memanajemeni peristiwa atau insiden keamanan informasi yang teridentifikasi;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

i) mengidentifikasi dan memanajemeni kerentanan keamanan informasi;
j) mereviu aspek keamanan informasi dari hubungan pemasok dengan pemasoknya sendiri;
k) memastikan bahwa pemasok memelihara kapabilitas layanan yang cukup bersama dengan rencana yang dapat diterapkan yang dirancang untuk memastikan bahwa level kontinuitas layanan yang disepakati dapat dipertahankan setelah kegagalan layanan atau bencana besar (lihat 5.29, 5.30, 5.35, 5.36, 8.14 ;
l) memastikan bahwa pemasok bertanggung jawab untuk mereviu kepatuhan dan menegakkan persyaratan perjanjian;
m) mengevaluasi secara reguler bahwa pemasok memelihara level keamanan informasi yang cukup.

Tanggung jawab untuk memanajemeni hubungan pemasok sebaiknya diberikan kepada individual atau tim yang ditunjuk. Keterampilan teknis dan sumber daya yang cukup sebaiknya disediakan untuk memonitor bahwa persyaratan perjanjian, khususnya persyaratan keamanan informasi, dipenuhi. Tindakan yang tepat sebaiknya diambil ketika diketahui adanya defisiensi dalam penyampaian layanan.

Informasi lain
Lihat ISO/IEC 27036-3 untuk detail lebih lanjut.

5.23 Keamanan informasi untuk penggunaan layanan *cloud*

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Proses untuk akuisisi, penggunaan, manajemen, dan keluar dari layanan *cloud* sebaiknya ditetapkan sesuai dengan persyaratan keamanan informasi organisasi.

Tujuan
Untuk menentukan dan memanajemeni keamanan informasi untuk penggunaan layanan *cloud*.

Panduan
Organisasi sebaiknya menetapkan dan mengomunikasikan kebijakan topik spesifik tentang penggunaan layanan *cloud* kepada semua pihak berkepentingan yang relevan.

Organisasi sebaiknya mendefinisikan dan mengomunikasikan cara yang dimaksud untuk memanajemeni risiko keamanan informasi yang terkait dengan penggunaan layanan *cloud*. Ini dapat berupa kelanjutan atau bagian dari pendekatan yang ada tentang bagaimana organisasi memanajemeni layanan yang disediakan oleh pihak eksternal (lihat 5.21 dan 5.22).

Penggunaan layanan *cloud* dapat melibatkan tanggung jawab bersama terhadap keamanan informasi dan upaya kolaboratif antara penyedia layanan *cloud* dan organisasi yang bertindak sebagai pengguna layanan *cloud*. Hal ini esensial bahwa tanggung jawab bagi penyedia layanan *cloud* dan organisasi yang bertindak sebagai pengguna layanan *cloud*, telah didefinisikan dan diimplementasikan dengan tepat.

Organisasi sebaiknya mendefinisikan:
a) semua persyaratan keamanan informasi yang relevan terkait dengan penggunaan layanan *cloud*;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) kriteria pemilihan layanan *cloud* dan ruang lingkup penggunaan layanan *cloud*;
c) peran dan tanggung jawab yang terkait dengan penggunaan dan manajemen layanan *cloud*;
d) kontrol keamanan informasi mana yang dimanajemeni oleh penyedia layanan *cloud* dan yang dimanajemeni oleh organisasi sebagai pengguna layanan *cloud*;
e) cara mendapatkan dan memanfaatkan kapabilitas keamanan informasi yang disediakan oleh penyedia layanan *cloud*;
f) cara mendapatkan keyakinan kontrol keamanan informasi yang diimplementasikan oleh penyedia layanan *cloud*;
g) cara memanajemeni kontrol, antarmuka, dan perubahan layanan ketika organisasi menggunakan beberapa layanan *cloud*, khususnya dari penyedia layanan *cloud* yang berbeda;
h) prosedur penanganan insiden keamanan informasi yang terjadi terkait penggunaan layanan *cloud*;
i) pendekatan untuk memonitor, mereviu, dan mengevaluasi penggunaan layanan *cloud* yang sedang berlangsung untuk memanajemeni risiko keamanan informasi;
j) cara untuk mengubah atau menghentikan penggunaan layanan *cloud* termasuk strategi keluar untuk layanan *cloud*.

Perjanjian layanan *cloud* sering kali sudah didefinisikan sebelumnya dan tidak terbuka untuk negosiasi. Untuk semua layanan *cloud*, organisasi sebaiknya mereviu perjanjian layanan *cloud* dengan penyedia layanan *cloud*. Perjanjian layanan *cloud* sebaiknya menangani persyaratan konfidensialitas, integritas, availabilitas, dan penanganan informasi organisasi, dengan sasaran level layanan *cloud* yang tepat dan sasaran kualitatif layanan *cloud*. Organisasi juga sebaiknya menjalankan asesmen risiko yang relevan untuk mengidentifikasi risiko yang terkait dengan penggunaan layanan *cloud*. Setiap risiko residual yang terkait dengan penggunaan layanan *cloud* sebaiknya diidentifikasi dengan jelas dan diterima oleh manajemen organisasi yang tepat.

Perjanjian antara penyedia layanan *cloud* dan organisasi, yang bertindak sebagai pengguna layanan *cloud*, sebaiknya termasuk ketentuan berikut untuk proteksi data dan availabilitas layanan organisasi:
a) menyediakan solusi berdasarkan standar yang diterima industri untuk arsitektur dan infrastruktur;
b) memanajemeni kontrol akses layanan *cloud* untuk memenuhi persyaratan organisasi;
c) mengimplementasikan solusi pemonitoran dan proteksi perangkat perusak;
d) memproses dan menyimpan informasi sensitif organisasi di lokasi yang disetujui (misalnya negara atau wilayah tertentu) atau di dalam atau tunduk pada yurisdiksi tertentu;
e) menyediakan dukungan khusus jika terjadi insiden keamanan informasi di lingkungan layanan *cloud*;
f) memastikan bahwa persyaratan keamanan informasi organisasi terpenuhi jika layanan *cloud* disubkontrakkan lebih lanjut ke pemasok eksternal (atau melarang layanan *cloud* disubkontrakkan);
g) mendukung organisasi dalam mengumpulkan bukti digital, dengan konsiderasi hukum dan regulasi tentang bukti digital di berbagai yurisdiksi;
h) menyediakan dukungan dan availabilitas layanan yang tepat untuk jangka waktu yang sesuai ketika organisasi ingin keluar dari layanan *cloud*;
i) menyediakan pencadangan data dan informasi konfigurasi yang dipersyaratkan dan memanajemeni pencadangan dengan aman sebagaimana berlaku, berdasarkan kapabilitas penyedia layanan *cloud* yang digunakan oleh organisasi, yang bertindak sebagai pengguna layanan *cloud*;
j) menyediakan dan mengembalikan informasi seperti fail konfigurasi, kode sumber, dan data yang dimiliki oleh organisasi, yang bertindak sebagai pengguna layanan *cloud*, ketika diminta selama penyediaan layanan atau pada saat penghentian layanan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Organisasi, yang bertindak sebagai pengguna layanan *cloud,* sebaiknya mempertimbangkan apakah perjanjian tersebut sebaiknya mensyaratkan penyedia layanan *cloud* untuk memberikan pemberitahuan awal sebelum perubahan pelanggan substantif yang berdampak pada cara penyediaan layanan kepada organisasi, termasuk:

a) perubahan infrastruktur teknis (misalnya relokasi, konfigurasi ulang, atau perubahan perangkat keras atau perangkat lunak) yang memengaruhi atau mengubah penawaran layanan *cloud*;
b) memproses atau menyimpan informasi dalam yurisdiksi geografis atau legal yang baru;
c) penggunaan sesama penyedia layanan *cloud* atau subkontraktor lainnya (termasuk mengubah yang ada atau menggunakan pihak baru).

Organisasi yang menggunakan layanan *cloud* sebaiknya menjalin kontak erat dengan penyedia layanan *cloud*. Kontak ini memungkinkan pertukaran informasi bersama tentang keamanan informasi untuk penggunaan layanan *cloud* termasuk mekanisme untuk penyedia layanan *cloud* dan organisasi, yang bertindak sebagai pengguna layanan *cloud*, untuk memonitor setiap karakteristik layanan dan melaporkan kegagalan terhadap komitmen yang terkandung dalam perjanjian.

Informasi lain
Kontrol ini mempertimbangkan keamanan *cloud* dari perspektif pengguna layanan *cloud*.

Informasi tambahan yang berhubungan dengan layanan *cloud* dapat ditemukan di ISO/IEC 17788, ISO/IEC 17789, dan ISO/IEC 22123-1. Hal-hal spesifik yang berhubungan dengan portabilitas *cloud* dalam mendukung strategi keluar dapat ditemukan di ISO/IEC 19941. Hal-hal spesifik yang berhubungan dengan keamanan informasi dan layanan *cloud* publik dijelaskan dalam ISO/IEC 27017. Hal-hal spesifik berhubungan dengan proteksi PII di *cloud* publik yang bertindak sebagai prosesor PII dijelaskan dalam ISO/IEC 27018.

Hubungan pemasok untuk layanan *cloud* dibahas dalam ISO/IEC 27036-4 dan perjanjian layanan *cloud* dan isinya dibahas dalam seri ISO/IEC 19086, dengan keamanan dan privasi secara spesifik dibahas dalam ISO/IEC 19086-4.

5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons #Memulihkan	#Tata_kelola #Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Organisasi sebaiknya merencanakan dan mempersiapkan untuk memanajemeni insiden keamanan informasi dengan mendefinisikan, menetapkan, dan mengomunikasikan proses, peran, dan tanggung jawab manajemen insiden keamanan informasi.

Tujuan
Untuk memastikan respons yang cepat, efektif, konsisten, dan tertib terhadap insiden keamanan informasi, termasuk komunikasi tentang peristiwa keamanan informasi.

Panduan
Peran dan tanggung jawab
Organisasi sebaiknya menetapkan proses manajemen insiden keamanan informasi yang tepat. Peran dan tanggung jawab untuk melaksanakan prosedur manajemen insiden

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

sebaiknya ditentukan dan dikomunikasikan secara efektif kepada pihak internal dan eksternal terkait yang relevan.

Hal-hal berikut sebaiknya dipertimbangkan:

a) menetapkan metode umum untuk melaporkan peristiwa keamanan informasi termasuk narahubung (lihat 6.8);
b) menetapkan proses manajemen insiden untuk memberikan kapabilitas kepada organisasi untuk memanajemeni insiden keamanan informasi termasuk administrasi, dokumentasi, deteksi, *triage*, prioritisasi, analisis, komunikasi, dan koordinasi dengan pihak yang berkepentingan;
c) menetapkan proses respons insiden untuk memberikan kapabilitas kepada organisasi untuk menilai, merespons, dan mempelajari dari insiden keamanan informasi;
d) hanya mengizinkan personel yang kompeten untuk menangani masalah yang berhubungan dengan insiden keamanan informasi dalam organisasi. Personel tersebut sebaiknya diberi dokumentasi prosedur dan pelatihan periodik;
e) menetapkan proses untuk mengidentifikasi pelatihan yang diperlukan, sertifikasi, dan pengembangan profesional yang sedang berlangsung untuk personel respons insiden.

Prosedur manajemen insiden

Sasaran untuk manajemen insiden keamanan informasi sebaiknya disepakati dengan manajemen dan sebaiknya dipastikan bahwa mereka yang bertanggung jawab atas manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi termasuk kerangka waktu penyelesaian berdasarkan kemungkinan konsekuensi dan keparahan. Prosedur manajemen insiden sebaiknya diimplementasikan untuk memenuhi sasaran dan prioritas ini.

Manajemen sebaiknya memastikan bahwa rencana manajemen insiden keamanan informasi dibuat dengan mempertimbangkan berbagai skenario dan prosedur yang dikembangkan dan diimplementasikan untuk aktivitas berikut:

a) evaluasi peristiwa keamanan informasi menurut kriteria apa yang dianggap insiden keamanan informasi;
b) pemonitoran (lihat 8.15 dan 8.16), deteksi (lihat 8.16), klasifikasi (lihat 5.25), analisis, dan pelaporan (lihat 6.8) peristiwa dan insiden keamanan informasi (oleh manusia atau secara otomatis);
c) memanajemeni insiden keamanan informasi hingga kesimpulan, termasuk respons dan eskalasi (lihat 5.26), sesuai dengan tipe dan kategori insiden, kemungkinan aktivasi manajemen krisis dan aktivasi rencana kontinuitas, pemulihan terkontrol dari insiden, dan komunikasi kepada pihak internal dan eksternal yang berkepentingan;
d) koordinasi dengan pihak internal dan eksternal yang berkepentingan seperti otoritas, grup dan forum kepentingan eksternal, pemasok dan klien (lihat 5.5 dan 5.6);
e) membuat log aktivitas manajemen insiden;
f) penanganan bukti (lihat 5.28);
g) analisis akar penyebab atau prosedur *post-mortem*;
h) identifikasi pembelajaran dan setiap perbaikan pada prosedur manajemen insiden atau kontrol keamanan informasi secara umum yang diperlukan.

Prosedur pelaporan

Prosedur pelaporan sebaiknya mencakup:

a) tindakan yang akan diambil jika terjadi peristiwa keamanan informasi (misalnya segera mencatat semua detail yang berkaitan seperti malafungsi yang terjadi dan pesan di layar, segera melaporkan ke narahubung dan hanya mengambil tindakan terkoordinasi);
b) formulir insiden untuk mendukung personel melakukan semua tindakan yang diperlukan saat melaporkan insiden keamanan informasi;
c) proses umpan balik yang cocok untuk memastikan bahwa orang-orang yang melaporkan peristiwa keamanan informasi dinotifikasi, sebanyak yang diperbolehkan, mengenai

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

hasil setelah masalah ditangani dan ditutup;
d) pembuatan laporan peristiwa.

Segala persyaratan eksternal tentang pelaporan insiden kepada pihak terkait yang relevan dalam jangka waktu yang didefinisikan (misalnya persyaratan pemberitahuan pelanggaran kepada regulator) sebaiknya dipertimbangkan saat mengimplementasikan prosedur manajemen insiden.

Informasi lain
Insiden keamanan informasi dapat melampaui batas organisasi dan nasional. Untuk merespons insiden semacam itu, sangat perlu untuk mengoordinasikan respons dan berbagi informasi tentang insiden ini dengan organisasi eksternal yang tepat.

Panduan detail tentang manajemen insiden keamanan informasi tersedia dalam seri ISO/IEC 27035.

5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeksi #Merespons	#Tata_kelola #Manajamen_peristiwa _keamanan_informasi	#Pertahanan

Kontrol
Organisasi sebaiknya melakukan asesmen peristiwa keamanan informasi dan memutuskan apakah peristiwa tersebut akan dikategorikan sebagai insiden keamanan informasi.

Tujuan
Untuk memastikan kategorisasi dan prioritisasi yang efektif dari peristiwa keamanan informasi.

Panduan
Skema kategorisasi dan prioritisasi insiden keamanan informasi sebaiknya disepakati untuk identifikasi konsekuensi dan prioritas insiden. Skema ini sebaiknya mencakup kriteria untuk mengategorikan peristiwa sebagai insiden keamanan informasi. Titik kontak sebaiknya menilai setiap peristiwa keamanan informasi menggunakan skema yang disepakati.

Personel yang bertanggung jawab untuk mengoordinasikan dan merespons insiden keamanan informasi sebaiknya melakukan asesmen dan membuat keputusan tentang peristiwa keamanan informasi.

Hasil asesmen dan keputusan sebaiknya direkam secara terperinci untuk tujuan referensi dan verifikasi di masa mendatang.

Informasi lain
Seri ISO/IEC 27035 memberikan panduan lebih lanjut tentang manajemen insiden.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.26 Respons terhadap insiden keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons #Memulihkan	#Manajamen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Insiden keamanan informasi sebaiknya direspons sesuai dengan prosedur yang terdokumentasi .

Tujuan
Untuk memastikan respons yang efisien dan efektif terhadap insiden keamanan informasi.

Panduan
Organisasi sebaiknya menetapkan dan mengomunikasikan prosedur tentang respons insiden keamanan informasi kepada semua pihak terkait yang relevan.

Insiden keamanan informasi sebaiknya direspons oleh tim yang ditunjuk dengan kompetensi yang dipersyaratkan (lihat 5.24).

Respons sebaiknya mencakup hal-hal berikut:
a) pengurungan (*containing*) sistem yang terdampak insiden, jika konsekuensi dari insiden dapat menyebar;
b) mengoleksi bukti (lihat 5.28) sesegera mungkin setelah peristiwa;
c) eskalasi, sebagaimana dipersyaratkan termasuk aktivitas manajemen krisis dan mungkin memerlukan rencana kontinuitas bisnis (lihat 5.29 dan 5.30);
d) memastikan bahwa semua aktivitas respons yang terlibat tercatat dengan benar untuk analisis di kemudian hari;
e) mengomunikasikan keberadaan insiden keamanan informasi atau detail terkait kepada semua pihak internal dan eksternal terkait yang relevan sesuai prinsip-perlu-mengetahui;
f) berkoordinasi dengan pihak internal dan eksternal seperti otoritas, grup dan forum kepentingan eksternal, pemasok, dan klien untuk meningkatkan efektivitas respons dan membantu meminimalkan konsekuensi bagi organisasi lain;
g) setelah insiden berhasil ditangani, secara resmi menutup dan merekamnya;
h) melakukan analisis forensik keamanan informasi, sebagaimana dipersyaratkan (lihat 5.28);
i) melakukan analisis pasca-insiden untuk mengidentifikasi akar penyebab. Pastikan akar penyebab tersebut didokumentasikan dan dikomunikasikan sesuai dengan prosedur yang didefinisikan (lihat 5.27);
j) mengidentifikasi dan memanajemeni kerentanan dan kelemahan keamanan informasi termasuk yang terkait dengan kontrol yang telah menyebabkan, berkontribusi pada, atau gagal mencegah insiden.

Informasi lain
Seri ISO/IEC 27035 memberikan panduan lebih lanjut tentang manajemen insiden.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.27 Belajar dari insiden keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Pengetahuan yang diperoleh dari insiden keamanan informasi sebaiknya digunakan untuk memperkuat dan meningkatkan kontrol keamanan informasi.

Tujuan
Untuk mengurangi kemungkinan atau konsekuensi insiden di masa depan.

Panduan
Organisasi sebaiknya menetapkan prosedur untuk menguantifikasi dan memonitor tipe, volume, dan biaya insiden keamanan informasi.
Informasi yang diperoleh dari evaluasi insiden keamanan informasi sebaiknya digunakan untuk:

a) meningkatkan rencana manajemen insiden termasuk skenario dan prosedur insiden (lihat 5.24);
b) mengidentifikasi insiden berulang atau serius dan penyebabnya untuk memperbarui asesmen risiko keamanan informasi organisasi serta menentukan dan mengimplementasikan kontrol tambahan yang diperlukan untuk mengurangi kemungkinan atau konsekuensi insiden serupa di masa depan. Mekanisme untuk memungkinkan pengumpulan, kuantifikasi, dan pemonitoran informasi tentang tipe, volume, dan biaya insiden;
c) meningkatkan kesadaran dan pelatihan pengguna (lihat 6.3) dengan menyediakan contoh apa yang dapat terjadi, bagaimana merespons insiden tersebut, dan bagaimana menghindarinya di masa depan.

Informasi lain
Seri ISO/IEC 27035 memberikan panduan lebih lanjut

5.28 Pengumpulan bukti

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendekteksi #Merespons	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Organisasi sebaiknya menetapkan dan mengimplementasikan prosedur untuk identifikasi, pengumpulan, akuisisi, dan preservasi bukti yang terkait dengan peristiwa keamanan informasi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Memastikan manajemen bukti yang konsisten dan efektif terkait insiden keamanan informasi untuk tujuan pendisiplinan dan tindakan legal.

Panduan
Prosedur internal sebaiknya dikembangkan dan diikuti ketika berurusan dengan bukti yang terkait dengan peristiwa keamanan informasi untuk tujuan pendisiplinan dan tindakan legal. Persyaratan yurisdiksi yang berbeda sebaiknya dipertimbangkan untuk memaksimalkan peluang penerimaan di seluruh yurisdiksi yang relevan.

Secara umum, prosedur untuk manajemen bukti ini sebaiknya memberikan instruksi untuk identifikasi, pengumpulan, akuisisi, dan penyimpanan bukti sesuai dengan berbagai tipe media penyimpanan, perangkat, dan status peranti (yaitu menyala atau mati). Bukti biasanya perlu dikumpulkan dengan cara yang akseptabel di pengadilan nasional yang tepat atau forum disiplin lainnya. Cara ini sebaiknya dapat menunjukkan bahwa:
a) rekamannya lengkap dan belum dirusak dengan cara apa pun;
b) salinan bukti elektronik mungkin sama persis dengan aslinya;
c) sistem informasi dari mana bukti dikumpulkan beroperasi dengan benar pada saat bukti direkam.

Jika tersedia, sertifikasi atau hal lain yang berkaitan dengan kualifikasi personel dan alat sebaiknya diperlihatkan, untuk memperkuat nilai bukti yang ada.

Bukti digital dapat melampaui batas-batas organisasi atau yurisdiksi. Dalam kasus seperti itu, sebaiknya dipastikan bahwa organisasi berhak untuk mengumpulkan informasi yang dipersyaratkan sebagai bukti digital.

Informasi lain
Ketika peristiwa keamanan informasi pertama kali terdeteksi, tidak selalu jelas apakah peristiwa tersebut akan menyebabkan tindakan pengadilan atau tidak. Oleh karena itu, terdapat kemungkinan bahaya bukti yang diperlukan dimusnahkan secara sengaja atau tidak sengaja sebelum level keseriusan insiden disadari. Keterlibatan penasihat legal atau penegak hukum lebih awal sangat dianjurkan dalam setiap tindakan legal yang dipertimbangkan dan menerima nasihat tentang bukti yang dipersyaratkan.

ISO/IEC 27037 memberikan definisi dan pedoman untuk identifikasi, pengumpulan, akuisisi, dan penyimpanan bukti digital.

Seri ISO/IEC 27050 membahas penemuan elektronik, yang melibatkan pemrosesan informasi yang disimpan secara elektronik sebagai bukti.

5.29 Keamanan informasi selama disrupsi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons	#Kontinuitas	#Proteksi #Resiliensi

Kontrol
Organisasi sebaiknya merencanakan bagaimana memelihara keamanan informasi pada level yang tepat selama disrupsi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk memproteksi informasi dan aset terkait lainnya selama disrupsi.

Panduan
Organisasi sebaiknya menentukan persyaratannya untuk mengadaptasi kontrol keamanan informasi selama disrupsi. Persyaratan keamanan informasi sebaiknya dimasukkan ke dalam proses manajemen kontinuitas bisnis.

Rencana sebaiknya dikembangkan, diimplementasikan, diuji, direviu, dan dievaluasi untuk memelihara atau memulihkan keamanan informasi proses bisnis kritis setelah gangguan atau kegagalan. Keamanan informasi sebaiknya dipulihkan pada level yang dipersyaratkan dan dalam rentang waktu yang dipersyaratkan.

Organisasi sebaiknya mengimplementasikan dan memelihara:
a) kontrol keamanan informasi, sistem pendukung, dan alat-alat dalam rencana kontinuitas usaha dan kontinuitas TIK;
b) proses untuk memelihara kontrol keamanan informasi yang ada selama disrupsi;
c) mengompensasi kontrol untuk kontrol keamanan informasi yang tidak dapat dipelihara selama disrupsi

Informasi lain
Dalam konteks perencanaan kontinuitas bisnis dan kontinuitas TIK, mungkin diperlukan pengadaptasian persyaratan keamanan informasi tergantung pada tipe disrupsi, dibandingkan dengan kondisi operasional normal. Sebagai bagian dari analisis dampak bisnis dan asesmen risiko yang dilakukan dalam manajemen kontinuitas bisnis, konsekuensi hilangnya konfidensialitas dan integritas informasi sebaiknya dipertimbangkan dan diprioritaskan sebagai tambahan atas kebutuhan untuk menjaga availabilitas.

Informasi tentang sistem manajemen kontinuitas bisnis dapat ditemukan di ISO 22301 dan ISO 22313. Panduan lebih lanjut tentang analisis dampak bisnis (BIA) dapat ditemukan di ISO/TS 22317.

5.30 Kesiapan TIK untuk kontinuitas bisnis

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Availabilitas	#Merespons	#Kontinuitas	#Resiliensi

Kontrol
Kesiapan TIK sebaiknya direncanakan, diimplementasikan, dipelihara, dan diuji berdasarkan sasaran kontinuitas bisnis dan persyaratan kontinuitas TIK.

Tujuan
Untuk memastikan availabilitas informasi organisasi dan aset terkait lainnya selama disrupsi.

Panduan
Kesiapan TIK untuk kontinuitas bisnis merupakan komponen penting dalam manajemen kontinuitas bisnis dan manajemen keamanan informasi untuk memastikan bahwa sasaran organisasi dapat terus terpenuhi selama disrupsi.

Persyaratan kontinuitas TIK merupakan hasil dari *business impact analysis* (BIA). Proses BIA sebaiknya menggunakan tipe dan kriteria dampak untuk menilai dampak dari waktu ke waktu yang diakibatkan oleh disrupsi aktivitas bisnis yang memberikan produk dan layanan. Besar dan durasi dampak yang dihasilkan sebaiknya digunakan untuk mengidentifikasi aktivitas

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

prioritas yang mana sebaiknya ditetapkan r*ecovery time objective* (RTO). Kemudian BIA sebaiknya menentukan sumber daya mana yang diperlukan untuk mendukung aktivitas yang diprioritaskan. RTO juga sebaiknya ditentukan untuk sumber daya ini. Subset dari sumber daya ini sebaiknya mencakup layanan TIK.

BIA yang melibatkan layanan TIK dapat diperluas untuk menentukan persyaratan kinerja dan kapasitas sistem TIK dan r*ecovery point objective* (RPO) atas informasi yang dipersyaratkan untuk mendukung aktivitas selama disrupsi.

Berdasarkan keluaran BIA dan asesmen risiko yang melibatkan layanan TIK, organisasi sebaiknya mengidentifikasi dan memilih strategi kontinuitas TIK yang mempertimbangkan opsi untuk sebelum, selama, dan setelah disrupsi. Strategi kontinuitas bisnis dapat terdiri dari satu solusi atau lebih. Berdasarkan strategi, rencana sebaiknya dikembangkan, diimplementasikan, dan diuji untuk memenuhi level availabilitas layanan TIK yang dipersyaratkan dan dalam rentang waktu yang dipersyaratkan setelah interupsi terhadap, atau kegagalan pada, proses kritis.

Organisasi sebaiknya memastikan bahwa:
a) struktur organisasi yang cukup disusun untuk mempersiapkan, memitigasi, dan merespons disrupsi yang didukung oleh personel dengan tanggung jawab, otoritas, dan kompetensi yang diperlukan;
b) rencana kontinuitas TIK, termasuk prosedur respons dan pemulihan yang mendetail bagaimana organisasi berencana untuk memanajemeni disrupsi layanan TIK:
    1) dievaluasi secara reguler melalui latihan dan pengujian;
    2) disetujui oleh manajemen;
c) rencana kontinuitas TIK meliputi informasi kontinuitas TIK berikut:
    1) spesifikasi kinerja dan kapasitas untuk memenuhi persyaratan dan sasaran kontinuitas bisnis sebagaimana ditentukan dalam BIA;
    2) RTO tiap-tiap layanan TIK yang diprioritaskan dan prosedur untuk pemulihan komponen tersebut;
    3) RPO sumber daya TIK yang diprioritaskan didefinisikan sebagai informasi dan prosedur untuk memulihkan informasi.

Informasi lain
Memanajemeni kontinuitas TIK merupakan kunci utama dari persyaratan kontinuitas bisnis mengenai availabilitas untuk dapat:
a) merespons dan memulihkan dari disrupsi layanan TIK terlepas dari penyebabnya;
b) memastikan kontinuitas aktivitas yang diprioritaskan didukung oleh layanan TIK yang dipersyaratkan;
c) merespons sebelum terjadinya disrupsi terhadap layanan TIK, dan setelah mendeteksi setidaknya satu insiden yang dapat mengakibatkan disrupsi terhadap layanan TIK.

Panduan lebih lanjut tentang kesiapan TIK untuk kontinuitas bisnis dapat ditemukan di ISO/IEC 27031.

Panduan lebih lanjut tentang sistem manajemen kontinuitas bisnis dapat ditemukan di ISO 22301 dan ISO 22313.

Panduan lebih lanjut tentang BIA dapat ditemukan di ISO/TS 22317.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.31 Persyaratan legal, statutori, regulatori, dan kontraktual

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Legal_dan_kepatuhan	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Persyaratan legal, statutori, regulatori, dan kontraktual yang relevan dengan keamanan informasi dan pendekatan organisasi untuk memenuhi persyaratan ini sebaiknya diidentifikasi, didokumentasikan, dan diperbarui.

Tujuan
Untuk memastikan kepatuhan terhadap persyaratan legal, statutori, regulatori, dan kontraktual yang terkait dengan keamanan informasi.

Panduan
Umum
Persyaratan eksternal termasuk persyaratan legal, statutori, regulatori, dan kontraktual sebaiknya dipertimbangkan ketika:
a) mengembangkan kebijakan dan prosedur keamanan informasi;
b) mendesain, mengimplementasikan, atau mengubah kontrol keamanan informasi;
c) mengklasifikasi informasi dan aset terkait lainnya sebagai bagian dari proses penetapan persyaratan keamanan informasi untuk kebutuhan internal atau untuk perjanjian pemasok;
d) melakukan asesmen risiko keamanan informasi dan menentukan aktivitas perawatan risiko keamanan informasi;
e) menentukan proses beserta peran dan tanggung jawab yang berkaitan dengan keamanan informasi;
f) menentukan persyaratan kontraktual pemasok yang relevan dengan organisasi dan ruang lingkup pasokan produk dan layanan.

Legislasi dan regulasi
Organisasi sebaiknya :
a) mengidentifikasi semua legislasi dan regulasi yang relevan dengan keamanan informasi organisasi agar menyadari persyaratan untuk tipe bisnisnya;
b) konsiderasi kepatuhan di semua negara yang terkait, jika organisasi:
   — menjalankan usaha di negara lain;
   — menggunakan produk dan layanan dari negara lain yang hukum dan regulasinya dapat memengaruhi organisasi;
   — mentransfer informasi lintas batas yurisdiksi yang hukum dan regulasinya dapat memengaruhi organisasi;
c) mereviu legislasi dan regulasi yang diidentifikasi secara reguler untuk mengikuti perubahan dan mengidentifikasi legislasi baru;
d) mendefinisikan dan mendokumentasikan proses spesifik dan tanggung jawab individual untuk memenuhi persyaratan ini.

Kriptografi
Kriptografi adalah bidang yang sering memiliki persyaratan legal spesifik. Kepatuhan terhadap perjanjian, hukum, dan regulasi yang berkaitan dengan hal-hal berikut sebaiknya menjadi konsiderasi:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) pembatasan impor atau ekspor perangkat keras dan perangkat lunak komputer untuk melakukan fungsi kriptografi;
b) pembatasan impor atau ekspor perangkat keras dan perangkat lunak komputer yang didesain untuk memiliki fungsi kriptografi yang ditambahkan ke dalamnya;
c) pembatasan penggunaan kriptografi;
d) metode akses wajib atau diskresi oleh otoritas negara untuk informasi terenkripsi;
e) validitas tanda tangan digital, cap, dan sertifikat.

Dianjurkan untuk meminta advis legal ketika memastikan kepatuhan terhadap legislasi dan regulasi yang relevan, terutama ketika informasi terenkripsi atau alat kriptografi dipindahkan lintas batas yurisdiksi.

Kontrak

Persyaratan kontraktual terkait keamanan informasi sebaiknya mencakup persyaratan yang tercantum dalam:

a) kontrak dengan klien;
b) kontrak dengan pemasok (lihat 5.20);
c) kontrak Asuransi.

Informasi lain

Tidak ada informasi lain.

5.32 Hak kekayaan intelektual

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Legal_dan_kepatuhan	#Tata_kelola_dan_ekosistem

Kontrol

Organisasi sebaiknya mengimplementasikan prosedur yang tepat untuk memproteksi hak kekayaan intelektual.

Tujuan

Untuk memastikan kepatuhan terhadap persyaratan legal, statutori, regalutori, dan kontraktual yang terkait dengan hak kekayaan intelektual dan penggunaan produk dengan hak milik

Panduan

Panduan berikut sebaiknya dipertimbangkan untuk memproteksi materi apa pun yang dapat dianggap sebagai kekayaan intelektual:

a) mendefinisikan dan mengomunikasikan kebijakan topik spesifik tentang proteksi hak kekayaan intelektual;
b) prosedur penerbitan untuk kepatuhan hak kekayaan intelektual yang mendefinisikan penggunaan perangkat lunak dan produk informasi yang sesuai;
c) memperoleh perangkat lunak hanya melalui sumber yang dikenal dan bereputasi baik, untuk memastikan bahwa hak cipta tidak dilanggar;
d) memelihara register aset yang tepat dan mengidentifikasi semua aset dengan persyaratan untuk memproteksi hak kekayaan intelektual;
e) memelihara bukti kepemilikan lisensi, manual dll;
f) memastikan bahwa jumlah maksimum pengguna atau sumber daya [misalnya *Central Processing Unit* (CPU)] yang diizinkan dalam lisensi tidak terlampaui;
g) melakukan reviu untuk memastikan bahwa hanya perangkat lunak resmi dan produk berlisensi yang terpasang;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

h) menyediakan prosedur untuk memelihara kondisi lisensi yang tepat;
i) menyediakan prosedur untuk menghapus atau mentransfer perangkat lunak kepada yang lain;
j) mematuhi syarat dan ketentuan untuk perangkat lunak dan informasi yang diperoleh dari jaringan publik dan sumber luar;
k) tidak menduplikasi, mengonversi ke format lain, atau mengekstrak dari rekaman komersial (video, audio) selain yang diizinkan oleh hukum hak cipta atau lisensi yang berlaku;
l) tidak menyalin, secara penuh atau sebagian, standar (misalnya Standar Internasional ISO/IEC), buku, artikel, laporan, atau dokumen lain, selain yang diizinkan oleh hukum hak cipta atau lisensi yang berlaku.

Informasi lain
Hak kekayaan intelektual mencakup hak cipta perangkat lunak atau dokumen, hak desain, merek dagang, paten, dan lisensi kode sumber.

Produk perangkat lunak dengan hak milik biasanya disediakan di bawah perjanjian lisensi yang menentukan syarat dan ketentuan lisensi, misalnya, membatasi penggunaan produk ke mesin tertentu atau membatasi penyalinan hanya untuk pembuatan salinan cadangan. Lihat seri ISO/IEC 19770 untuk detail tentang manajemen aset TI.
Data dapat diperoleh dari sumber luar. Umumnya data tersebut diperoleh berdasarkan ketentuan perjanjian berbagi data atau instrumen hukum serupa. Perjanjian berbagi data tersebut sebaiknya memperjelas pemrosesan yang diizinkan untuk data yang diperoleh. Pembuktian data juga disarankan untuk dinyatakan dengan jelas. Lihat ISO/IEC 23751untuk detail perjanjian berbagi data.

Persyaratan legal, statutori, regulatori dan kontraktual dapat membatasi penyalinan materi hak milik. Secara khusus, mereka dapat mensyaratkan hanya materi yang dikembangkan oleh organisasi atau yang dilisensikan atau disediakan oleh developer untuk organisasi, yang dapat digunakan. Pelanggaran hak cipta dapat menyebabkan tindakan legal, yang dapat melibatkan denda dan proses pidana.

Selain organisasi perlu mematuhi kewajibannya terhadap hak kekayaan intelektual pihak ketiga, risiko personel dan pihak ketiga yang gagal menegakkan hak kekayaan intelektual organisasi sendiri juga sebaiknya dimanajemeni.

5.33 Proteksi rekaman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Legal_dan_kepatuhan #Manajemen_aset #Proteksi_informasi	#Pertahanan

Kontrol
Rekaman sebaiknya diproteksi dari kehilangan, perusakan, pemalsuan, akses takterotorisasi, dan rilis takterotorisasi.

Tujuan
Untuk memastikan kepatuhan terhadap persyaratan legal, statutori, regalutori, dan kontraktual, serta harapan komunitas atau masyarakat yang terkait dengan proteksi dan availabilitas rekaman.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan

Organisasi sebaiknya mengambil langkah berikut untuk memproteksi keautentikan, reliabilitas, integritas, dan penggunaan rekaman, sebagai konteks bisnisnya dan persyaratan untuk perubahan manajemennya dari waktu ke waktu:

a) mengeluarkan pedoman tentang penyimpanan, penanganan rantai kustodi, dan pemusnahan rekaman, yang mencakup pencegahan manipulasi rekaman. Pedoman ini sebaiknya diselaraskan dengan kebijakan topik spesifik organisasi tentang manajemen rekaman dan persyaratan rekaman lainnya;
b) menyusun jadwal retensi yang mendefinisikan rekaman dan periode waktu yang sebaiknya dipertahankan.

Sistem penyimpanan dan penanganan sebaiknya memastikan identifikasi rekaman dan periode retensinya dengan konsiderasi legislasi atau regulasi nasional atau regional, serta harapan komunitas atau masyarakat, jika berlaku. Sistem sebaiknya mengizinkan pemusnahan rekaman yang tepat setelah periode tersebut jika tidak diperlukan oleh organisasi.

Ketika memutuskan proteksi untuk rekaman organisasi spesifik, klasifikasi keamanan informasi yang sesuai, berdasarkan skema klasifikasi organisasi, sebaiknya dipertimbangkan. Rekaman sebaiknya dikategorikan ke dalam tipe rekaman (misalnya rekaman akuntansi, rekaman transaksi bisnis, rekaman personel, rekaman legal), masing-masing dengan detail dari periode penyimpanan dan tipe media penyimpanan yang diizinkan dapat berupa fisik atau elektronik.

Sistem penyimpanan data sebaiknya dipilih sehingga rekaman yang diperlukan dapat diambil dalam kerangka waktu dan format yang akseptabel, tergantung pada persyaratan yang sebaiknya dipenuhi.

Jika media penyimpanan elektronik dipilih, prosedur untuk memastikan kemampuan mengakses rekaman (media penyimpanan dan keterbacaan format) selama periode retensi sebaiknya ditetapkan untuk memproteksi dari kehilangan akibat perubahan teknologi di masa depan. Setiap kunci kriptografi dan program yang terkait dengan arsip terenkripsi atau tanda tangan digital, juga sebaiknya disimpan untuk memungkinkan dekripsi data selama rekaman disimpan (lihat 8.24).

Prosedur penyimpanan dan penanganan sebaiknya diimplementasikan sesuai dengan rekomendasi yang disediakan oleh pabrikan media penyimpanan. Konsiderasi sebaiknya diberikan terhadap kemungkinan memburuknya media yang digunakan untuk penyimpanan rekaman.

Informasi lain

Rekaman mendokumentasikan peristiwa atau transaksi individual atau dapat membentuk agregasi yang telah didesain untuk mendokumentasikan proses kerja, aktivitas, atau fungsi. Keduanya merupakan bukti aktivitas bisnis dan aset informasi. Setiap rangkaian informasi, terlepas dari struktur atau bentuknya, dapat dimanajemeni sebagai rekaman. Hal ini termasuk informasi dalam bentuk dokumen, koleksi data, atau tipe informasi digital atau analog lainnya yang dibuat, diperoleh, dan dimanajemeni dalam bisnis.

Pada manajemen rekaman, metadata adalah data yang menjelaskan konteks, konten, dan struktur rekaman, serta manajemennya dari waktu ke waktu. Metadata adalah komponen penting dari setiap rekaman.

Metadata dapat diperlukan untuk menyimpan beberapa rekaman dengan aman agar memenuhi persyaratan legal, statutori, regulatori dan kontraktual serta untuk mendukung aktivitas bisnis penting. Hukum atau regulasi nasional dapat mengatur periode waktu dan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

konten data untuk penyimpanan informasi. Informasi lebih lanjut tentang manajemen rekaman dapat ditemukan di ISO 15489.

5.34 Privasi dan proteksi PII

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Proteksi_informasi #Legal_dan_kepatuhan	#Proteksi

Kontrol
Organisasi sebaiknya mengidentifikasi dan memenuhi persyaratan mengenai preservasi privasi dan proteksi PII sesuai dengan hukum dan regulasi yang berlaku dan persyaratan kontraktual.

Tujuan
Untuk memastikan kepatuhan terhadap persyaratan legal, statutori, regulatori, dan kontraktual yang terkait dengan aspek keamanan informasi proteksi PII.

Panduan
Organisasi sebaiknya menetapkan dan mengomunikasikan kebijakan topik spesifik tentang privasi dan proteksi PII kepada semua pihak terkait yang relevan.

Organisasi sebaiknya mengembangkan dan mengimplementasikan prosedur untuk preservasi privasi dan proteksi PII. Prosedur ini sebaiknya dikomunikasikan kepada semua pihak terkait yang relevan yang terlibat dalam pemrosesan informasi pengidentifikasi diri.

Kepatuhan terhadap prosedur ini dan semua legislasi serta regulasi yang relevan mengenai preservasi privasi dan proteksi PII mensyaratkan peran, tanggung jawab, dan kontrol yang tepat. Seringkali kepatuhan paling baik dicapai melalui penunjukan orang yang bertanggung jawab, seperti petugas privasi, yang sebaiknya menyediakan panduan kepada personel, penyedia layanan, dan pihak lain yang berkepentingan tentang tanggung jawabnya masing-masing dan prosedur spesifik yang sebaiknya diikuti.

Tanggung jawab penanganan PII sebaiknya ditangani dengan konsiderasi legislasi dan regulasi yang relevan.

Langkah-langkah teknis dan organisasi yang tepat untuk memproteksi PII sebaiknya diimplementasikan.

Informasi lain
Sejumlah negara telah memperkenalkan legislasi yang menempatkan kontrol terhadap pengumpulan, pemrosesan, transmisi, dan penghapusan PII. Tergantung pada legislasi nasional masing-masing, kontrol tersebut dapat memberikan tanggung jawab bagi mereka yang mengumpulkan, memproses, dan menyebarkan PII dan juga dapat membatasi otoritas untuk mentransfer PII ke negara lain.

ISO/IEC 29100 menyediakan kerangka kerja level tinggi untuk proteksi PII dalam sistem TIK. Informasi lebih lanjut tentang sistem manajemen informasi privasi dapat ditemukan di ISO/IEC 27701. Informasi spesifik mengenai manajemen informasi privasi untuk *cloud* publik yang bertindak sebagai pemroses PII dapat ditemukan di ISO/IEC 27018.

ISO/IEC 29134 menyediakan pedoman untuk *privacy impact assessment* (PIA) dan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

memberikan contoh struktur dan konten laporan PIA. Dibanding dengan ISO/IEC 27005, seri ini fokus pada pemrosesan PII dan relevan dengan organisasi yang memproses PII. Seri ini dapat membantu mengidentifikasi risiko privasi dan kemungkinan mitigasi untuk mengurangi risiko ini ke level yang akseptabel.

5.35 Reviu independen terhadap keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Keyakinan_keamanan_informasi	#Tata_kelola_dan_Ekosistem

Kontrol
Pendekatan organisasi untuk memanajemeni keamanan informasi dan implementasinya termasuk orang, proses, dan teknologi sebaiknya direviu secara independen pada interval yang direncanakan, atau ketika perubahan signifikan terjadi.

Tujuan
Untuk memastikan kesesuaian, kecukupan, dan efektivitas yang berkelanjutan terhadap pendekatan organisasi dalam memanajemeni keamanan informasi.

Panduan
Organisasi sebaiknya memiliki proses untuk melakukan reviu independen.

Manajemen sebaiknya merencanakan dan memulai reviu independen secara periodik. Reviu sebaiknya mencakup asesmen peluang untuk perbaikan dan perlunya perubahan pendekatan terhadap keamanan informasi, termasuk kebijakan keamanan informasi, kebijakan topik spesifik, dan kontrol lainnya.

Reviu tersebut sebaiknya dilakukan oleh individual independen dari area yang sedang direviu (misalnya fungsi audit internal, manajer independen, atau organisasi pihak eksternal yang spesialis di bidang reviu tersebut). Individu yang melakukan reviu ini sebaiknya memiliki kompetensi yang tepat. Orang yang melakukan reviu tidak boleh berada di garis otoritas untuk memastikan mereka memiliki independensi untuk membuat asesmen.

Hasil reviu independen sebaiknya dilaporkan kepada manajemen yang memulai reviu dan, jika perlu, kepada jajaran pimpinan. Rekaman reviu tersebut sebaiknya dipelihara.

Jika reviu independen mengidentifikasi bahwa pendekatan dan implementasi organisasi untuk memanajemeni keamanan informasi tidak memadai [misal sasaran dan persyaratan terdokumentasi tidak terpenuhi atau tidak sesuai dengan arah keamanan informasi yang dinyatakan dalam kebijakan keamanan informasi dan kebijakan topik spesifik (lihat 5.1), manajemen sebaiknya memulai tindakan korektif.

Selain tinjauan independen secara periodik, organisasi sebaiknya mempertimbangkan untuk melakukan reviu independen ketika:
a) ada perubahan pada hukum dan regulasi yang memengaruhi organisasi;
b) insiden signifikan terjadi;
c) organisasi memulai bisnis baru atau mengubah bisnis saat ini;
d) organisasi mulai menggunakan produk atau layanan baru, atau mengubah penggunaan produk atau layanan saat ini;
e) organisasi mengubah kontrol dan prosedur keamanan informasi secara signifikan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
ISO/IEC 27007 dan ISO/IEC TS 27008 menyediakan panduan untuk melakukan reviu independen.

5.36 Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Legal_dan_kepatuhan #Keyakinan_keamanan_informasi	#Tata_kelola_dan_Ekosistem

Kontrol
Kepatuhan terhadap kebijakan keamanan informasi organisasi, kebijakan topik spesifik, aturan, dan standar sebaiknya direviu secara reguler.

Tujuan
Untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan keamanan informasi organisasi, kebijakan topik spesifik, aturan, dan standar.

Panduan
Manajer, pemilik layanan, produk, atau pemilik informasi sebaiknya mengidentifikasi cara mereviu bahwa persyaratan keamanan informasi yang ditentukan dalam kebijakan keamanan informasi, kebijakan topik spesifik, aturan, standar, dan regulasi lain yang berlaku terpenuhi. Alat pengukuran dan pelaporan otomatis sebaiknya dipertimbangkan untuk reviu rutin yang efisien.

Jika ditemukan ketidakpatuhan sebagai hasil dari reviu, manajer sebaiknya:
a) mengidentifikasi penyebab ketidakpatuhan;
b) mengevaluasi perlunya tindakan korektif untuk mencapai kepatuhan;
c) mengimplementasikan tindakan perbaikan yang tepat;
d) mereviu tindakan perbaikan yang diambil untuk memverifikasi efektivitasnya dan mengidentifikasi defisiensi atau kelemahan.

Hasil reviu dan tindakan korektif yang dilakukan oleh manajer, layanan, produk, atau pemilik informasi sebaiknya direkam dan rekaman ini sebaiknya dipelihara. Manajer sebaiknya melaporkan hasilnya kepada person yang melakukan reviu independen (lihat 5.35) ketika reviu independen dilakukan di bidang yang menjadi tanggung jawabnya.

Tindakan korektif sebaiknya diselesaikan tepat waktu yang sesuai dengan risiko. Jika tidak diselesaikan hingga reviu berikutnya, progres sebaiknya setidaknya dibahas dalam reviu tersebut.

Informasi lain
Pemonitoran operasional penggunaan sistem tercakup dalam 8.15, 8.16, 8.17.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.37 Prosedur operasi terdokumentasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Memulihkan	#Manajemen_aset #Keamanan_fisik #Keamanan_Sistem_dan_jaringan #Keamanan_aplikasi #Konfigurasi_yang_aman #Manajemen_identitas_dan_akses #Kontinuitas #Manajemen_peristiwa_keamanan_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Pertahanan

Kontrol
Prosedur operasi untuk fasilitas pemrosesan informasi sebaiknya didokumentasikan dan tersedia untuk personel yang membutuhkannya.

Tujuan
Untuk memastikan pengoperasian fasilitas pengolahan informasi yang benar dan aman.

Panduan
Prosedur terdokumentasi sebaiknya disiapkan untuk aktivitas operasional organisasi yang terkait dengan keamanan informasi, misalnya:
a) ketika aktivitas perlu dilakukan dengan cara yang sama oleh banyak orang;
b) ketika aktivitas jarang dilakukan dan ketika berikutnya prosedur dilakukan kemungkinan telah dilupakan;
c) ketika aktivitas baru dan menimbulkan risiko jika tidak dilakukan dengan benar;
d) sebelum menyerahkan aktivitas kepada personel baru.

Prosedur operasi sebaiknya menentukan:
a) individual yang bertanggung jawab;
b) instalasi dan konfigurasi sistem yang aman;
c) pemrosesan dan penanganan informasi, otomatis maupun manual;
d) pencadangan (lihat 8.13) dan resiliensi;
e) persyaratan penjadwalan, termasuk saling ketergantungan dengan sistem lain;
f) instruksi untuk menangani kesalahan atau kondisi luar biasa lainnya [misal pembatasan pada penggunaan program utilitas (lihat 8.18), yang dapat timbul selama eksekusi pekerjaan;
g) dukungan dan kontak eskalasi termasuk kontak dukungan eksternal pada peristiwa kesulitan teknis atau operasional yang tidak terduga;
h) instruksi penanganan media penyimpanan (lihat 7.10 dan 7.14);
i) prosedur mulai ulang dan pemulihan sistem untuk digunakan pada peristiwa kegagalan sistem
j) manajemen jejak audit dan informasi log sistem (lihat 8.15 dan 8.17) dan sistem pemonitoran video (lihat 7.4);
k) prosedur pemonitoran seperti kapasitas, kinerja, dan keamanan (lihat 8.6 dan 8.16);
l) instruksi pemeliharaan.

Prosedur operasi yang terdokumentasi sebaiknya direviu dan diperbarui bila diperlukan. Perubahan pada prosedur operasi yang terdokumentasi sebaiknya diotorisasi. Jika memungkinkan secara teknis, sistem informasi sebaiknya dimanajemeni secara konsisten, menggunakan prosedur, alat, dan utilitas yang sama.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Tidak ada informasi lain.

6 Kontrol orang

6.1 Skrining

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem

Kontrol
Pemeriksaan verifikasi latar belakang pada semua kandidat untuk menjadi personel sebaiknya dilakukan sebelum bergabung dengan organisasi dan secara berkelanjutan dengan konsiderasi hukum, regulasi, dan etika serta proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses, dan risiko yang dipersepsikan.

Tujuan
Untuk memastikan semua personel memenuhi syarat dan cocok untuk peran yang mereka pertimbangkan dan tetap memenuhi syarat dan cocok selama mereka bekerja.

Panduan
Proses skrining sebaiknya dilakukan untuk semua personel termasuk staf penuh waktu, paruh waktu, dan sementara. Jika orang-orang ini dikontrak melalui pemasok layanan, persyaratan skrining sebaiknya dimasukkan dalam perjanjian kontraktual antara organisasi dan pemasok.

Informasi tentang semua kandidat yang dipertimbangkan untuk posisi dalam organisasi sebaiknya dikumpulkan dan ditangani dengan konsiderasi legislasi yang tepat yang ada di yurisdiksi yang relevan. Di beberapa yurisdiksi, organisasi dapat diwajibkan secara legal untuk menginformasikan kandidat sebelumnya tentang aktivitas skrining.

Verifikasi sebaiknya mempertimbangkan semua privasi relevan, proteksi PII, dan legislasi berbasis ketenagakerjaan dan sebaiknya, jika diizinkan, mencakup hal-hal berikut:
a) availabilitas referensi yang memuaskan (misalnya referensi bisnis dan pribadi);
b) verifikasi (untuk kelengkapan dan akurasi) daftar riwayat hidup pemohon;
c) konfirmasi kualifikasi akademik dan profesional sesuai pernyataan;
d) verifikasi identitas independen (misalnya paspor atau dokumen lain yang akseptabel yang dikeluarkan oleh otoritas yang tepat);
e) verifikasi yang lebih detail, seperti reviu kredit atau reviu rekaman kriminal jika kandidat mengambil peran kritis.

Ketika seorang individu dipekerjakan untuk peran keamanan informasi spesifik, organisasi sebaiknya memastikan kandidat:
a) memiliki kompetensi yang diperlukan untuk melakukan peran keamanan tersebut;
b) dapat dipercaya untuk melaksanakan peran tersebut, terutama jika perannya kritis bagi organisasi.

Ketika suatu pekerjaan, baik pada saat penunjukan awal atau promosi, melibatkan orang yang memiliki akses ke fasilitas pemrosesan informasi dan, khususnya, jika ini melibatkan penanganan informasi konfidensial (misalnya informasi finansial, informasi personal, atau informasi layanan kesehatan) organisasi juga sebaiknya mempertimbangkan verifikasi lebih

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

lanjut yang lebih detail.

Prosedur sebaiknya mendefinisikan kriteria dan batasan untuk reviu verifikasi (misalnya siapa yang memenuhi syarat untuk menyeleksi orang serta bagaimana, kapan dan mengapa reviu verifikasi dilakukan).

Dalam hal verifikasi tidak dapat dilengkapi tepat waktu, kontrol mitigasi sebaiknya diimplementasikan sampai reviu selesai, misalnya:
a) orientasi ditunda;
b) penyebaran aset korporasi ditunda;
c) orientasi dengan akses yang dikurangi;
d) Pemutusan hubungan kerja

Pengecekan verifikasi sebaiknya diulang secara periodik untuk mengonfirmasi kesesuaian personel yang sedang berlangsung, tergantung pada kekritisan peran seseorang.

Informasi lain
Tidak ada informasi lain.

6.2 Syarat dan ketentuan ketenagakerjaan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem

Kontrol
Perjanjian kontraktual kerja sebaiknya menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.

Tujuan
Untuk memastikan personel memahami tanggung jawab keamanan informasinya untuk peran yang akan ditempatinya.

Panduan
Kewajiban kontraktual untuk personel sebaiknya mengambil konsiderasi kebijakan keamanan informasi organisasi dan kebijakan topik spesifik yang relevan. Selain itu, poin berikut dapat diklarifikasi dan dinyatakan:
a) perjanjian konfidensialitas atau nirungkap yang sebaiknya ditandatangani oleh personel yang diberi akses ke informasi konfidensial sebelum diberi akses ke informasi dan aset terkait lainnya (lihat 6.6);
b) tanggung jawab dan hak legal [misalnya mengenai hukum hak cipta atau legislasi proteksi data (lihat 5.32 dan 5.34)];
c) tanggung jawab untuk klasifikasi informasi dan manajemen informasi organisasi dan aset terkait lainnya, fasilitas pemrosesan informasi, dan layanan informasi yang ditangani oleh personel (lihat 5.9 hingga 5.13);
d) tanggung jawab atas penanganan informasi yang diterima dari pihak yang berkepentingan;
e) tindakan yang sebaiknya diambil jika personel mengabaikan persyaratan keamanan organisasi (lihat 6.4).

Peran dan tanggung jawab keamanan informasi sebaiknya dikomunikasikan kepada kandidat selama proses prakerja.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Organisasi sebaiknya memastikan bahwa personel menyetujui syarat dan ketentuan mengenai keamanan informasi. Syarat dan ketentuan ini sebaiknya tepat untuk sifat dan level akses yang mereka miliki terhadap aset organisasi yang terkait dengan sistem dan layanan informasi. Syarat dan ketentuan mengenai keamanan informasi sebaiknya direviu ketika hukum, regulasi, kebijakan keamanan informasi, atau kebijakan topik spesifik berubah.

Jika tepat, tanggung jawab yang terkandung dalam syarat dan ketentuan kerja sebaiknya terus berlaku untuk periode yang ditentukan setelah hubungan kerja berakhir (lihat 6.5).

Informasi lain
Kode etik dapat digunakan untuk menyatakan tanggung jawab keamanan informasi personel mengenai konfidensialitas, proteksi PII, etika, penggunaan informasi organisasi dan aset terkait lainnya dengan tepat, serta praktik terhormat yang diharapkan oleh organisasi.

Pihak eksternal, yang terkait dengan personel pemasok, dapat dipersyaratkan untuk menandatangani perjanjian kontraktual atas nama individual yang dikontrak.

Jika organisasi bukan merupakan entitas legal dan tidak memiliki karyawan, dokumen yang setara dengan perjanjian kontraktual dan syarat dan ketentuan dapat dipertimbangkan sejalan dengan panduan kontrol ini.

6.3 Kesadaran, pendidikan, dan pelatihan keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem

Kontrol
Personel organisasi dan pihak terkait yang relevan sebaiknya menerima kesadaran keamanan informasi yang tepat, pendidikan dan pelatihan dan pembaruan reguler dari kebijakan keamanan informasi organisasi, kebijakan dan prosedur khusus topik, yang relevan untuk fungsi pekerjaannya.

Tujuan
Untuk memastikan personel dan pihak terkait yang relevan menyadari dan memenuhi tanggung jawab keamanan informasinya.

Panduan
Umum
Program kesadaran, pendidikan dan program pelatihan keamanan informasi sebaiknya ditetapkan sejalan dengan kebijakan keamanan informasi organisasi, kebijakan topik spesifik, dan prosedur yang relevan tentang keamanan informasi, dengan mengambil konsiderasi informasi organisasi untuk memproteksi dan kontrol keamanan informasi yang telah diimplementasikan untuk memproteksi informasi.

Kesadaran, pendidikan dan pelatihan keamanan informasi sebaiknya dilakukan secara periodik. Kesadaran, pendidikan, dan pelatihan awal dapat berlaku untuk personel baru dan bagi mereka yang transfer ke posisi atau peran baru dengan substansi persyaratan keamanan informasi yang sangat berbeda.

Pemahaman personel sebaiknya dinilai pada aktivitas kesadaran, pendidikan, atau pelatihan untuk menguji transfer pengetahuan dan efektivitas program kesadaran, pendidikan dan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

pelatihan.

Kesadaran
Program kesadaran keamanan informasi sebaiknya bertujuan untuk membuat personel menyadari tanggung jawabnya untuk keamanan informasi dan cara pelaksanaan tanggung jawab tersebut.

Program kesadaran sebaiknya direncanakan dengan mengambil konsiderasi peran personel dalam organisasi, termasuk personel internal dan eksternal (misalnya konsultan eksternal, personel pemasok). Aktivitas dalam program kesadaran sebaiknya dijadwalkan dari waktu ke waktu, sebaiknya secara reguler, sehingga aktivitas diulang dan mencakup personel baru. Program tersebut juga sebaiknya didasarkan pada pelajaran yang didapat dari insiden keamanan informasi.

Program kesadaran sebaiknya termasuk sejumlah aktivitas peningkatan kesadaran melalui saluran fisik atau virtual yang tepat seperti kampanye, buklet, poster, buletin, situs web, sesi informasi, pengarahan, modul pembelajaran daring, dan surel.

Kesadaran keamanan informasi sebaiknya mencakup aspek umum seperti:
a) komitmen manajemen terhadap keamanan informasi di seluruh organisasi;
b) kebutuhan pengetahuan dan kepatuhan mengenai aturan dan kewajiban keamanan informasi yang berlaku, dengan memperhitungkan kebijakan keamanan informasi dan kebijakan topik spesifik, standar, hukum, statuta, regulasi, kontrak, dan perjanjian;
c) akuntabilitas personal atas tindakan dan keputusan untuk tidak bertindak, dan tanggung jawab umum untuk mengamankan atau memproteksi informasi milik organisasi dan pihak yang terkait;
d) prosedur keamanan informasi dasar [misalnya pelaporan peristiwa keamanan informasi (6.8)] dan kontrol garis acuan [misalnya keamanan kata sandi (5.17)];
e) titik kontak dan sumber daya untuk informasi tambahan dan saran tentang masalah keamanan informasi, termasuk materi kesadaran keamanan informasi lebih lanjut.

Pendidikan dan pelatihan
Organisasi sebaiknya mengidentifikasi, mempersiapkan, dan mengimplementasikan rencana pelatihan yang tepat untuk tim teknis yang perannya mensyaratkan keterampilan dan keahlian spesifik. Tim teknis sebaiknya memiliki keterampilan untuk mengkonfigurasi dan memelihara level keamanan yang dipersyaratkan untuk perangkat, sistem, aplikasi, dan layanan. Jika ada keterampilan yang hilang, organisasi sebaiknya mengambil tindakan dan mendapatkannya.

Program pendidikan dan pelatihan sebaiknya mempertimbangkan bentuk yang berbeda [misalnya kuliah atau belajar mandiri, dibimbing oleh staf ahli atau konsultan (pelatihan di tempat kerja), merotasi anggota staf untuk mengikuti aktivitas yang berbeda, merekrut orang yang sudah terampil dan menyewa konsultan]. Program tersebut dapat disajikan dalam berbagai cara termasuk berbasis kelas, pembelajaran jarak jauh, berbasis web, pembelajaran mandiri, dan lain-lain. Personel teknis sebaiknya terus memperbarui pengetahuannya dengan berlangganan buletin dan majalah atau dengan menghadiri konferensi dan peristiwa yang ditujukan untuk pengembangan teknis dan profesional.

Informasi lain
Ketika menyusun program kesadaran, jika memungkinkan, penting untuk tidak hanya fokus pada 'apa' dan 'bagaimana', tetapi juga 'mengapa'. Penting bagi personel untuk memahami tujuan keamanan informasi dan efek potensial, positif dan negatif, pada organisasi dari perilaku mereka sendiri.

Kesadaran, pendidikan, dan pelatihan keamanan informasi dapat menjadi bagian dari, atau dilakukan bekerja sama dengan, aktivitas lain, misalnya pelatihan manajemen informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

umum, TIK, keamanan, privasi, atau pelatihan keselamatan.

6.4 Proses kedisiplinan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem

Kontrol
Proses kedisiplinan sebaiknya disusun dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan lain yang relevan yang telah melakukan pelanggaran kebijakan keamanan informasi.

Tujuan
Untuk memastikan personel dan pihak berkepentingan lain yang relevan memahami konsekuensi dari pelanggaran kebijakan keamanan informasi, untuk mencegah dan menangani personel dan pihak terkait lainnya yang berkepentingan lainnya yang melakukan pelanggaran dengan tepat.

Panduan
Proses disiplin tidak boleh dimulai tanpa verifikasi sebelumnya bahwa pelanggaran kebijakan keamanan informasi telah terjadi (lihat 5.28).
Proses disiplin formal sebaiknya memberikan respons bertahap yang mempertimbangkan faktor-faktor seperti:
a) sifat (siapa, apa, kapan, bagaimana) dan beratnya pelanggaran dan konsekuensinya;
b) apakah pelanggaran itu disengaja (dengan niat jahat) atau tidak disengaja (kebetulan);
c) apakah ini adalah pelanggaran pertama atau berulang atau tidak;
d) apakah pelanggar dilatih dengan benar atau tidak.

Respons sebaiknya mengambil konsiderasi legal, statutori, regulatori, kontraktual, dan persyaratan bisnis yang relevan serta faktor lain yang diperlukan. Proses disiplin juga sebaiknya digunakan untuk mencegah personel dan pihak terkait lain yang relevan melanggar kebijakan keamanan informasi, kebijakan topik spesifik, dan prosedur untuk keamanan informasi. Pelanggaran kebijakan keamanan informasi yang disengaja mungkin perlu tindakan segera.

Informasi lain
Jika memungkinkan, identitas individual yang menjadi subjek tindakan disiplin sebaiknya diproteksi sejalan dengan persyaratan yang berlaku.

Ketika individual menunjukkan perilaku yang sangat baik berkaitan dengan keamanan informasi, mereka dapat diapresiasi untuk mempromosikan keamanan informasi dan mendorong perilaku yang baik

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

6.5 Tanggung jawab setelah terminasi atau perubahan pekerjaan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_SDM #Manajemen_aset	#Tata_kelola_dan_Ekosistem

Kontrol
Tanggung jawab dan tugas keamanan informasi yang tetap berlaku setelah terminasi atau perubahan pekerjaan sebaiknya didefinisikan, ditegakkan, dan dikomunikasikan kepada personel terkait dan pihak lain yang berkepentingan.

Tujuan
Untuk memproteksi kepentingan organisasi sebagai bagian dari proses perubahan atau pemutusan hubungan kerja atau kontrak.

Panduan
Proses untuk memanajemeni terminasi atau perubahan pekerjaan sebaiknya mendefinisikan tanggung jawab dan tugas keamanan informasi mana yang sebaiknya tetap berlaku setelah terminasi atau perubahan. Ini dapat termasuk konfidensialitas informasi, kekayaan intelektual dan pengetahuan lain yang diperoleh, serta tanggung jawab yang terkandung dalam perjanjian konfidensialitas lainnya (lihat 6.6). Tanggung jawab dan kewajiban yang masih valid setelah terminasi hubungan kerja atau kontrak sebaiknya tertuang dalam syarat dan ketentuan kerja individu (lihat 6.2), kontrak, atau perjanjian. Kontrak atau perjanjian lain yang terus berlaku untuk periode yang didefinisikan setelah berakhirnya masa kerja individual juga dapat berisi tanggung jawab keamanan informasi.

Perubahan tanggung jawab atau pekerjaan sebaiknya dimanajemeni sebagai terminasi tanggung jawab saat ini atau pekerjaan dikombinasikan dengan inisiasi tanggung jawab baru atau pekerjaan.

Peran dan tanggung jawab keamanan informasi yang dipegang oleh setiap individual yang meninggalkan atau berganti peran pekerjaan sebaiknya diidentifikasi dan ditransfer ke individual lain.

Sebuah proses sebaiknya ditetapkan untuk komunikasi perubahan dan prosedur operasi kepada personel, pihak lain yang berkepentingan, dan narahubung yang relevan (misalnya kepada pelanggan dan pemasok).

Proses untuk terminasi atau perubahan pekerjaan juga sebaiknya diterapkan pada personel eksternal (yaitu pemasok) ketika terjadi terminasi personel, kontrak, atau pekerjaan dengan organisasi, atau ketika ada perubahan pekerjaan dalam organisasi.

Informasi lain
Di banyak organisasi, fungsi sumber daya manusia umumnya bertanggung jawab atas keseluruhan proses terminasi dan bekerja sama dengan manajer pengawas orang yang bertransisi untuk memanajemeni aspek keamanan informasi dari prosedur yang relevan. Dalam hal personel yang disediakan melalui pihak eksternal (misalnya melalui pemasok), proses penghentian ini dilakukan oleh pihak eksternal sesuai dengan kontrak antara organisasi dan pihak eksternal.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

6.6 Perjanjian konfidensialitas atau nirungkap

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Keamanan_SDM #Proteksi_informasi #Hubungan_pemasok	#Tata_kelola_dan_Ekosistem

Kontrol
Perjanjian konfidensialitas atau nirungkap yang merefleksikan kebutuhan organisasi untuk proteksi informasi sebaiknya diidentifikasi, didokumentasikan, direviu secara regular, dan ditandatangani oleh personel dan pihak terkait lainnya yang relevan.

Tujuan
Untuk memelihara konfidensialitas informasi yang dapat diakses oleh personel atau pihak eksternal.

Panduan
Perjanjian konfidensialitas atau nirungkap sebaiknya memenuhi persyaratan untuk memproteksi informasi konfidensial menggunakan persyaratan yang dapat ditegakkan secara legal. Perjanjian konfidensialitas atau nirungkap berlaku untuk pihak yang berkepentingan dan personel organisasi. Berdasarkan persyaratan keamanan informasi organisasi, persyaratan dalam perjanjian sebaiknya ditentukan dengan mengambil konsiderasi tipe informasi yang akan ditangani, level klasifikasinya, penggunaannya, dan akses yang diizinkan oleh pihak lain. Untuk mengidentifikasi persyaratan untuk perjanjian konfidensialitas atau nirungkap, elemen-elemen berikut sebaiknya dipertimbangkan:

a) definisi informasi yang diproteksi (misalnya informasi konfidensial);
b) durasi perjanjian yang diharapkan, termasuk kasus-kasus yang diharuskan untuk memelihara konfidensialitas tanpa batas waktu atau sampai informasi tersedia untuk umum;
c) tindakan yang dipersyaratkan ketika perjanjian diterminasi;
d) tanggung jawab dan tindakan penandatangan untuk menghindari pengungkapan informasi yang takterotorisasi;
e) kepemilikan informasi, konfidensial dagang dan kekayaan intelektual, dan bagaimana hal ini berkaitan dengan proteksi informasi konfidensial;
f) penggunaan informasi konfidensial dengan izin dan hak penandatangan untuk menggunakan informasi;
g) hak untuk mengaudit dan memonitor aktivitas yang melibatkan informasi konfidensial untuk keadaan yang sangat sensitif;
h) proses untuk notifikasi dan pelaporan pengungkapan yang takterotorisasi atau kebocoran informasi konfidensial;
i) ketentuan untuk informasi yang akan dikembalikan atau dihancurkan pada saat pengakhiran perjanjian;
j) tindakan yang diharapkan akan diambil dalam kasus ketidakpatuhan terhadap perjanjian.

Organisasi sebaiknya mengambil konsiderasi kepatuhan terhadap perjanjian konfidensialitas dan nirungkap untuk yurisdiksi yang berlaku (lihat 5.31, 5.32, 5.33, 5.34).

Persyaratan untuk perjanjian konfidensialitas dan nirungkap sebaiknya direviu secara periodik serta ketika perubahan terjadi yang memengaruhi persyaratan ini.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Perjanjian konfidensialitas dan nirungkap memproteksi informasi organisasi dan memberi tahu penandatangan akan tanggung jawab mereka untuk memproteksi, menggunakan, dan mengungkapkan informasi dengan cara yang bertanggung jawab dan dengan terotorisasi.

6.7 Telekarya (*Remote working*)

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_aset #Proteksi_informasi #Keamanan_fisik #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Langkah keamanan sebaiknya diimplementasikan ketika personel bekerja dari jarak jauh untuk memproteksi informasi yang diakses, diproses, atau disimpan di luar premis organisasi.

Tujuan
Untuk memastikan keamanan informasi ketika personel bekerja dari jarak jauh.

Panduan
Telekarya terjadi setiap kali personel organisasi bekerja dari lokasi di luar premis organisasi berada, mengakses informasi baik dalam salinan cetak (*hard copy*) atau secara elektronik melalui peralatan TIK. Lingkungan telekarya termasuk yang disebut sebagai "*teleworking*", "*telecommuting*", "*flexible workplace*", "*virtual work environments*", dan "*remote maintenance*".

CATATAN Ada kemungkinan bahwa tidak semua rekomendasi dalam panduan ini dapat diberlakukan karena legislasi dan regulasi setempat di yurisdiksi yang berbeda.

Organisasi yang mengizinkan aktivitas telekarya sebaiknya mengeluarkan kebijakan topik spesifik tentang kerja jarak jauh yang mendefinisikan kondisi dan batasan yang relevan. Jika dianggap berlaku, hal berikut sebaiknya dipertimbangkan:

a) keamanan fisik yang ada atau yang diajukan dari lokasi kerja telekarya, dengan memperhitungkan keamanan fisik lokasi dan lingkungan setempat, termasuk yurisdiksi yang berbeda tempat personel berada;
b) aturan dan mekanisme keamanan untuk lingkungan fisik jarak jauh seperti lemari arsip yang dapat dikunci, transportasi aman antar lokasi dan aturan untuk akses jarak jauh, meja bersih, pencetakan dan pembuangan informasi dan aset terkait lainnya, dan pelaporan peristiwa keamanan informasi (lihat 6.8);
c) lingkungan telekarya fisik yang diharapkan;
d) persyaratan keamanan komunikasi, dengan memperhitungkan perlunya akses jarak jauh ke sistem organisasi, sensitivitas informasi yang akan diakses dan dikirimkan melalui saluran komunikasi, serta sensitivitas sistem dan aplikasi;
e) penggunaan akses jarak jauh seperti akses *desktop* virtual yang mendukung pemrosesan dan penyimpanan informasi tentang peralatan milik pribadi;
f) ancaman akses takterotorisasi ke informasi atau sumber daya dari orang lain di lokasi kerja jarak jauh (misalnya keluarga dan teman);
g) ancaman akses takterotorisasi ke informasi atau sumber daya dari person lain di tempat umum;
h) penggunaan jaringan rumah dan jaringan publik, dan persyaratan atau pembatasan konfigurasi layanan jaringan nirkabel;
i) penggunaan langkah-langkah keamanan, seperti *firewall* dan proteksi terhadap

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

perangkat perusak;
j) mekanisme yang aman untuk menerapkan dan mengaktifkan sistem dari jarak jauh;
k) mekanisme aman untuk autentikasi dan pemberdayaan hak akses privilese dengan mengambil konsiderasi kerentanan mekanisme autentikasi faktor tunggal ketika akses jarak jauh ke jaringan organisasi diperbolehkan.

Pedoman dan langkah-langkah yang dipertimbangkan sebaiknya termasuk:
a) penyediaan peralatan dan furnitur penyimpanan yang sesuai untuk aktivitas kerja jarak jauh, ketika penggunaan peralatan milik pribadi yang tidak berada di bawah kontrol organisasi tidak diperbolehkan;
b) definisi pekerjaan yang diizinkan, klasifikasi informasi yang dapat diselenggarakan, dan sistem dan layanan internal yang terotorisasi untuk diakses oleh pekerja telekarya;
c) penyediaan pelatihan bagi mereka yang bekerja secara jarak jauh dan mereka yang memberikan dukungan. Ini sebaiknya termasuk bagaimana melakukan bisnis dengan cara yang aman saat bekerja dari jarak jauh;
d) penyediaan peralatan komunikasi yang sesuai, termasuk metode untuk mengamankan akses jarak jauh, seperti persyaratan pada kunci layar peranti dan penghitung waktu ketidakaktifan; pengaktifan pelacakan lokasi perangkat; instalasi kapabilitas penghapusan jarak jauh;
e) keamanan fisik
f) aturan dan panduan tentang akses keluarga dan pengunjung ke peralatan dan informasi;
g) penyediaan dukungan dan pemeliharaan perangkat keras dan perangkat lunak;
h) penyediaan asuransi;
i) prosedur untuk pencadangan dan kontinuitas bisnis;
j) audit dan pemonitoran keamanan;
k) pencabutan otoritas dan hak akses dan pengembalian peralatan ketika aktivitas telekarya diterminasi.

Informasi lain
Tidak ada informasi lain.

6.8 Pelaporan peristiwa keamanan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Organisasi sebaiknya menyediakan mekanisme bagi personel untuk melaporkan peristiwa keamanan informasi yang diamati atau dicurigai melalui saluran yang sesuai pada waktu yang tepat.

Tujuan
Untuk mendukung pelaporan peristiwa keamanan informasi yang tepat waktu, konsisten dan efektif yang dapat diidentifikasi oleh personel.

Panduan
Semua personel dan pengguna sebaiknya dipastikan sadar akan tanggung jawabnya untuk melaporkan peristiwa keamanan informasi secepat mungkin untuk mencegah atau meminimalkan efek insiden keamanan informasi.

Mereka juga sebaiknya sadar akan prosedur untuk melaporkan peristiwa keamanan informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dan titik kontak peristiwa sebaiknya dilaporkan. Mekanisme pelaporan sebaiknya mudah, dapat diakses, dan tersedia sebaik mungkin. Peristiwa keamanan informasi termasuk insiden, pelanggaran, dan kerentanan.

Situasi yang sebaiknya dipertimbangkan untuk pelaporan peristiwa keamanan informasi meliputi:

a) kontrol keamanan informasi yang tidak efektif;
b) pelanggaran konfidensialitas informasi, integritas, atau ekspektasi availabilitas;
c) kesalahan manusia;
d) ketidakpatuhan terhadap kebijakan keamanan informasi, kebijakan topik spesifik, atau standar yang berlaku;
e) pelanggaran langkah-langkah keamanan fisik;
f) perubahan sistem yang belum melalui proses manajemen perubahan;
g) malafungsi atau perilaku sistem anomali lainnya dari perangkat lunak atau perangkat keras;
h) pelanggaran akses;
i) kerentanan;
j) dugaan infeksi perangkat perusak.

Personel dan pengguna sebaiknya disarankan untuk tidak mencoba membuktikan dugaan kerentanan keamanan informasi. Pengujian kerentanan dapat diintepretasikan sebagai potensi penyalahgunaan sistem dan juga dapat menyebabkan kerusakan pada sistem informasi atau layanan, dan dapat merusak atau mengaburkan bukti digital. Pada akhirnya, ini dapat menghasilkan liabilitas legal bagi individual yang melakukan pengujian.

Informasi lain
Lihat seri ISO/IEC 27035 untuk informasi tambahan.

7 Kontrol fisik

7.1 Perimeter keamanan fisik

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi

Kontrol
Perimeter keamanan sebaiknya didefinisikan dan digunakan untuk memproteksi area yang berisi informasi dan aset terkait lainnya.

Tujuan
Untuk mencegah akses fisik yang takterotorisasi, kerusakan, dan interferensi terhadap informasi organisasi dan aset terkait lainnya.

Panduan
Pedoman berikut sebaiknya dipertimbangkan dan diimplementasikan di mana sesuai untuk perimeter keamanan fisik:

a) mendefinisikan perimeter keamanan dan penempatan dan kekuatan setiap perimeter sesuai dengan persyaratan keamanan informasi yang terkait dengan aset dalam perimeter;
b) memiliki perimeter yang baik secara fisik untuk suatu bangunan atau situs yang berisi fasilitas pemrosesan informasi (yaitu sebaiknya tidak ada celah di perimeter atau area

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

tempat pembobolan dapat dengan mudah terjadi). Atap bagian luar, dinding, langit-langit, dan lantai dari situs sebaiknya merupakan konstruksi yang solid dan semua pintu eksternal sebaiknya diproteksi dengan tepat terhadap akses yang takterotorisasi dengan mekanisme kontrol (misalnya jeruji, alarm, kunci). Pintu dan jendela sebaiknya dikunci ketika ditinggalkan dan proteksi eksternal sebaiknya dipertimbangkan untuk jendela, terutama di permukaan tanah; titik ventilasi juga sebaiknya dipertimbangkan;

c) memperingatkan, memonitor, dan menguji semua pintu api (*fire door*) di perimeter keamanan bersama dengan dinding untuk menetapkan level resiliensi berdasarkan pada standar yang sesuai. Mereka sebaiknya beroperasi dengan cara *failsafe*.

Informasi lain
Proteksi fisik dapat dicapai dengan menciptakan satu atau lebih pembatas fisik di sekitar lokasi organisasi dan fasilitas pemrosesan informasi.

Area aman dapat berupa kantor yang dapat dikunci atau beberapa ruangan yang dikelilingi oleh pembatas keamanan fisik internal yang berkelanjutan. Pembatas dan perimeter tambahan untuk mengontrol akses fisik dapat diperlukan antara area dengan persyaratan keamanan yang berbeda di dalam perimeter keamanan. Organisasi sebaiknya mempertimbangkan untuk memiliki ukuran keamanan fisik yang dapat diperkuat selama situasi ancaman yang meningkat.

7.2 Entri fisik

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_Identitas_dan_Akses	#Proteksi

Kontrol
Area aman sebaiknya diproteksi oleh kontrol entri dan titik akses yang tepat.

Tujuan
Untuk memastikan hanya akses fisik yang terotorisasi terhadap informasi organisasi dan aset terkait lainnya terjadi.

Panduan
Umum
Titik akses seperti area pengiriman dan pemuatan serta titik-titik lain tempat orang yang takterotorisasi dapat memasuki lokasi sebaiknya dikontrol dan, jika mungkin, diisolasi dari fasilitas pemrosesan informasi untuk menghindari akses yang takterotorisasi.
Panduan berikut sebaiknya dipertimbangkan:

a) membatasi akses ke situs dan bangunan hanya untuk personel yang terotorisasi. Proses untuk manajemen hak akses ke area fisik sebaiknya mencakup persediaan, reviu periodik, pembaruan, dan pencabutan otorisasi (lihat 5.18);
b) memelihara dan memonitor *logbook* fisik atau jejak audit elektronik dengan aman dari semua akses serta memproteksi semua log (lihat 5.33) dan informasi autentikasi sensitif;
c) menetapkan dan mengimplementasikan proses serta mekanisme teknis untuk manajemen akses ke area tempat informasi diproses atau disimpan. Mekanisme autentikasi termasuk penggunaan kartu akses, biometrik, atau autentikasi dua faktor seperti kartu akses dan PIN konfidensial. Pintu keamanan ganda sebaiknya dipertimbangkan untuk akses ke area sensitif;
d) menyiapkan area penerimaan yang dimonitor oleh personel, atau cara lain untuk mengontrol akses fisik ke situs atau bangunan;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

e) menginspeksi dan memeriksa barang pribadi personel dan pihak yang berkepentingan saat masuk dan keluar;
CATATAN Legislasi dan regulasi lokal bisa eksis mengenai kemungkinan inspeksi kepemilikan pribadi
f) mensyaratkan semua personel dan pihak yang berkepentingan untuk mengenakan beberapa bentuk identifikasi yang terlihat dan untuk segera menotifikasi petugas keamanan jika mereka menemukan pengunjung yang tidak mengenakan identifikasi yang terlihat. Tanda pengenal yang mudah dibedakan sebaiknya dipertimbangkan untuk mengidentifikasi karyawan, pemasok, dan pengunjung permanen dengan lebih baik;
g) memberikan personel pemasok akses terbatas ke area aman atau fasilitas pemrosesan informasi hanya ketika diperlukan. Akses ini sebaiknya diotorisasi dan dimonitor;
h) memberikan atensi spesial pada keamanan akses fisik dalam kasus bangunan yang di dalamnya terdapat aset untuk beberapa organisasi;
i) mendesain langkah keamanan fisik sehingga mereka dapat diperkuat ketika kemungkinan insiden fisik meningkat;
j) mengamankan titik masuk lainnya seperti pintu keluar darurat dari akses yang takterotorisasi;
k) menyiapkan proses manajemen kunci untuk memastikan manajemen kunci fisik atau informasi autentikasi (misalnya kode kunci, kunci kombinasi ke kantor, ruangan, dan fasilitas seperti lemari kunci) dan untuk memastikan buku log atau audit kunci tahunan dan akses ke kunci fisik atau informasi autentikasi terkontrol (lihat 5.17 untuk panduan lebih lanjut tentang informasi autentikasi).

Pengunjung
Hal-hal berikut sebaiknya dipertimbangkan:
a) mengautentikasi identitas pengunjung dengan cara yang tepat;
b) merekam tanggal dan jam masuk dan keluar pengunjung;
c) hanya memberikan akses bagi pengunjung untuk tujuan spesifik terotorisasi serta dengan instruksi tentang persyaratan keamanan area dan prosedur darurat;
d) menyupervisi semua pengunjung, kecuali terdapat eksepsi eksplisit.

Area pengiriman dan pemuatan dan bahan yang masuk
Pedoman berikut sebaiknya dipertimbangkan:
a) membatasi akses ke area pengiriman dan pemuatan dari luar gedung kepada personel yang diidentifikasi dan terotorisasi;
b) mendesain area pengiriman dan pemuatan sehingga pengiriman dapat dimuat dan dibongkar tanpa memungkinkan petugas pengiriman mendapatkan akses takterotorisasi ke bagian lain dari bangunan;
c) mengamankan pintu eksternal area pengiriman dan pemuatan ketika pintu ke area terbatas dibuka;
d) menginspeksi dan memeriksa pengiriman yang masuk untuk bahan peledak, bahan kimia atau bahan berbahaya lainnya sebelum dipindahkan dari area pengiriman dan pemuatan;
e) mendaftarkan pengiriman yang masuk sesuai dengan prosedur manajemen aset (lihat 5.9 dan 7.10) saat masuk ke situs;
f) memisahkan pengiriman masuk dan keluar secara fisik, jika memungkinkan;
g) menginspeksi pengiriman yang masuk untuk memperoleh bukti gangguan dalam perjalanan. Jika ditemukan gangguan, sebaiknya segera dilaporkan ke petugas keamanan.

Informasi lain
Tidak ada informasi lain.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7.3 Mengamankan kantor, ruangan, dan fasilitas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi

Kontrol
Keamanan fisik untuk kantor, ruangan, dan fasilitas sebaiknya didesain dan diimplementasikan.

Tujuan
Untuk mencegah akses fisik yang takterotorisasi, kerusakan dan interferensi terhadap informasi organisasi serta aset terkait lainnya di kantor, ruangan dan fasilitas.

Panduan
Panduan berikut sebaiknya dipertimbangkan untuk mengamankan kantor, ruangan, dan fasilitas:

a) menempatkan fasilitas kritis untuk menghindari akses oleh publik;
b) jika berlaku, memastikan bangunan tidak mengganggu dan memberikan indikasi minimum tentang tujuannya, tanpa tanda-tanda yang jelas, di luar atau di dalam gedung, yang mengidentifikasi keberadaan aktivitas pemrosesan informasi;
c) mengonfigurasi fasilitas untuk mencegah informasi atau aktivitas konfidensial terlihat dan terdengar dari luar. Pelindung elektromagnetik sebaiknya juga dipertimbangkan yang tepat;
d) tidak membuat direktori, buku telepon internal, dan peta daring yang dapat diakses mengidentifikasi lokasi fasilitas pemrosesan informasi konfidensial yang tersedia untuk person yang takterotorisasi.

Informasi lain
Tidak ada informasi lain.

7.4 Pemonitoran keamanan fisik

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_fisik	#Proteksi #Pertahanan

Kontrol
Premis sebaiknya terus dimonitor untuk menemukan akses fisik yang takterotorisasi.

Tujuan
Untuk mendeteksi dan mencegah akses fisik yang takterotorisasi.

Panduan
Premis fisik sebaiknya dimonitor dengan sistem surveilans, yang dapat mencakup penjaga, alarm penyusup, sistem pemonitoran video seperti televisi sirkuit tertutup dan perangkat lunak manajemen informasi keamanan fisik baik yang dimanajemeni secara internal atau oleh penyedia layanan pemonitoran.

Akses ke bangunan yang di dalamnya terdapat sistem kritis sebaiknya terus dimonitor untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

mendeteksi akses takterotorisasi atau perilaku mencurigakan dengan:

a) menginstal sistem pemonitoran video seperti televisi sirkuit tertutup untuk melihat dan merekam akses ke area sensitif di dalam dan di luar premis organisasi;
b) menginstal, sesuai dengan standar berlaku yang relevan, dan secara periodik menguji detektor kontak, suara, atau gerakan untuk memicu alarm penyusup seperti:
    1) menginstal detektor kontak yang memicu alarm ketika terdapat kontak atau kerusakan di tempat yang memungkinkan terjadinya kontak atau kerusakan (seperti jendela dan pintu dan di bawah objek) untuk digunakan sebagai alarm panik;
    2) detektor gerak berdasarkan teknologi inframerah yang memicu alarm ketika suatu objek melewati bidang pandangnya;
    3) memasang sensor yang sensitif terhadap suara pecahan kaca yang dapat digunakan untuk memicu alarm untuk memperingatkan petugas keamanan;
c) menggunakan alarm tersebut untuk menutupi semua pintu eksternal dan jendela yang dapat diakses. Area yang kosong sebaiknya diperhatikan setiap saat; penutup juga sebaiknya disediakan untuk area lain (misalnya komputer atau ruang komunikasi).

Desain sistem pemonitoran sebaiknya tetap konfidensial karena pengungkapan dapat memfasilitasi pembobolan yang tidak terdeteksi.

Sistem pemonitoran sebaiknya diproteksi dari akses takterotorisasi untuk mencegah informasi surveilans, seperti video, diakses oleh orang yang takterotorisasi atau sistem dinonaktifkan dari jarak jauh.

Panel kontrol sistem alarm sebaiknya ditempatkan di zona yang dipasangi alarm dan, untuk alarm keselamatan, di tempat yang memungkinkan orang yang mengatur alarm untuk keluar dengn mudah. Panel kontrol dan detektor sebaiknya memiliki mekanisme tahan kerusakan. Sistem sebaiknya diuji secara reguler untuk memastikannya bekerja sebagaimana mestinya, terutama jika komponennya bertenaga baterai.

Setiap mekanisme pemonitoran dan perekaman sebaiknya digunakan dengan mempertimbangkan hukum dan regulasi lokal termasuk legislasi proteksi data dan proteksi PII, terutama mengenai pemonitoran personel dan periode retensi video yang direkam.

Informasi lain
Tidak ada informasi lain.

7.5 Memproteksi dari ancaman fisik dan lingkungan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi

Kontrol
Proteksi terhadap ancaman fisik dan lingkungan, seperti bencana alam dan ancaman fisik yang disengaja atau tidak disengaja lainnya terhadap infrastruktur sebaiknya didesain dan diimplementasikan.

Tujuan
Untuk mencegah atau mengurangi konsekuensi dari peristiwa yang berasal dari ancaman fisik dan lingkungan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan

Asesmen risiko untuk mengidentifikasi potensi konsekuensi dari ancaman fisik dan lingkungan sebaiknya dilakukan sebelum memulai operasi kritis di lokasi fisik, dan secara berkala. Proteksi yang diperlukan sebaiknya dilaksanakan dan perubahan terhadap ancaman sebaiknya dimonitor. Diperlukan saran spesialis tentang cara memanajemeni risiko yang timbul dari ancaman fisik dan lingkungan seperti kebakaran, banjir, gempa bumi, ledakan, kerusuhan, limbah beracun, emisi lingkungan, dan bentuk bencana alam atau bencana lainnya yang disebabkan oleh manusia.

Premis dan konstruksi lokasi fisik sebaiknya memperhitungkan:

a) topografi lokal, seperti elevasi yang tepat, perairan, dan garis patahan tektonik;
b) ancaman perkotaan, seperti lokasi yang sangat berpotensi menarik kerusuhan politik, aktivitas kriminal, atau serangan teroris.

Berdasarkan hasil asesmen risiko, ancaman fisik dan lingkungan yang relevan sebaiknya diidentifikasi dan kontrol yang tepat dipertimbangkan dalam konteks berikut sebagai contoh:

a) kebakaran: menginstal dan melakukan konfigurasi sistem yang mampu mendeteksi kebakaran pada tahap awal untuk mengirim peringatan atau memicu sistem pencegah kebakaran untuk mencegah kerusakan kebakaran pada media penyimpanan dan sistem pemrosesan informasi terkait. Pemadaman kebakaran sebaiknya dilakukan dengan menggunakan zat yang paling tepat berkaitan dengan lingkungan sekitarnya (misalnya gas di ruang terbatas);
b) banjir: menginstal sistem yang mampu mendeteksi banjir pada tahap awal di bawah lantai area yang berisi media penyimpanan atau sistem pemrosesan informasi. Pompa air atau yang ekuivalen sebaiknya tersedia jika terjadi banjir;
c) lonjakan listrik mengadopsi sistem yang mampu memproteksi sistem informasi server dan klien terhadap lonjakan listrik atau peristiwa serupa untuk meminimalkan konsekuensi dari peristiwa tersebut;
d) bahan peledak dan senjata: melakukan inspeksi acak untuk menemukan keberadaan bahan peledak atau senjata pada personel, kendaraan, atau barang yang memasuki fasilitas pemrosesan informasi sensitif.

Informasi lain

Brankas atau bentuk lain dari fasilitas penyimpanan yang aman dapat memproteksi informasi yang tersimpan di dalamnya terhadap bencana seperti kebakaran, gempa bumi, banjir, atau ledakan.

Organisasi dapat mempertimbangkan konsep pencegahan kejahatan melalui desain lingkungan ketika mendesain kontrol untuk mengamankan lingkungannya dan mengurangi ancaman perkotaan. Misalnya, alih-alih menggunakan trotoar, patung atau air mancur dapat berfungsi sebagai fitur dan pembatas fisik.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7.6 Bekerja di area aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi

Kontrol
Langkah-langkah keamanan untuk bekerja di area aman sebaiknya didesain dan diimplementasikan.

Tujuan
Untuk memproteksi informasi dan aset terkait lainnya di area yang aman dari kerusakan dan interferensi yang takterotorisasi oleh personel yang bekerja di area tersebut.

Panduan
Langkah-langkah keamanan untuk bekerja di area aman sebaiknya berlaku untuk semua personel dan mencakup semua aktivitas yang terjadi di area aman.
Hal-hal berikut sebaiknya dipertimbangkan:

a) membuat personel hanya mengetahui keberadaan, atau aktivitas di dalam, area aman berdasarkan kebutuhan untuk mengetahui;
b) menghindari pekerjaan taktersupervisi di area aman baik untuk alasan keamanan maupun untuk mengurangi kemungkinan aktivitas berbahaya;
c) mengunci secara fisik dan secara periodik memeriksa area aman yang kosong;
d) tidak mengizinkan peralatan fotografi, video, audio, atau rekaman lainnya, seperti kamera di peranti titik akhir pengguna, kecuali terotorisasi;
e) mengontrol keberadaan dan penggunaan peranti titik akhir pengguna dengan tepat di area aman;
f) mengumumkan prosedur darurat dengan cara yang mudah terlihat atau dapat diakses.

Informasi lain
Tidak ada informasi lain.

7.7 Meja bersih dan layar bersih

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Keamanan_fisik	#Proteksi

Kontrol
Aturan meja bersih untuk kertas dan media penyimpanan yang dapat dipindahkan serta aturan layar bersih untuk fasilitas pemrosesan informasi sebaiknya didefinisikan dan ditegakkan dengan tepat.

Tujuan
Untuk mengurangi risiko akses takterotorisasi, kehilangan, dan kerusakan informasi di meja, layar, dan di lokasi lain yang dapat diakses selama dan di luar jam kerja normal.

Panduan
Organisasi sebaiknya menetapkan dan mengomunikasikan kebijakan topik spesifik tentang meja dan layar yang bersih kepada semua pihak berkepentingan yang relevan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Hal-hal berikut sebaiknya dipertimbangkan:

a) mengunci informasi bisnis yang sensitif atau kritis (misalnya pada kertas atau pada media penyimpanan elektronik) (idealnya dalam brankas, lemari atau bentuk furnitur keamanan lainnya) bila tidak diperlukan, terutama ketika kantor dikosongkan;
b) memproteksi peranti titik akhir pengguna dengan kunci atau sarana keamanan lainnya saat tidak digunakan atau takterawasi
c) meninggalkan peranti titik akhir pengguna dalam kondisi *log off* atau diproteksi dengan mekanisme penguncian layar dan *keyboard* yang dikontrol oleh mekanisme autentikasi pengguna saat tanpa pengawasan. Semua komputer dan sistem sebaiknya dikonfigurasi dengan batas waktu atau fitur keluar otomatis;
d) meminta pencetak (*originator*) mengumpulkan keluaran dari *printer* atau peranti multifungsi dengan segera. Penggunaan *printer* dengan fungsi autentikasi, sehingga pencetak (*originator*) adalah satu-satunya yang bisa mendapatkan hasil cetakannya dan hanya ketika ia berdiri di samping *printer*;
e) menyimpan dokumen dengan aman dan media penyimpanan yang dapat dipindahkan yang berisi informasi sensitif dan, bila tidak lagi diperlukan, membuangnya menggunakan mekanisme pembuangan yang aman;
f) menetapkan dan mengomunikasikan aturan dan panduan untuk konfigurasi *pop-up* di layar (misalnya mematikan *pop-up* surel dan pesan baru, jika mungkin, selama presentasi, berbagi layar, atau di area publik);
g) membersihkan informasi sensitif atau kritis pada papan tulis dan tipe tampilan lainnya bila tidak lagi diperlukan.

Organisasi sebaiknya memiliki prosedur ketika mengosongkan fasilitas termasuk melakukan penyisiran akhir sebelum pergi untuk memastikan aset organisasi tidak tertinggal di belakang (misalnya dokumen yang tertinggal di belakang laci atau furnitur).

Informasi lain
Tidak ada informasi lain.

7.8 Penempatan dan proteksi peralatan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi

Kontrol
Peralatan sebaiknya ditempatkan dengan aman dan diproteksi.

Tujuan
Untuk mengurangi risiko dari ancaman fisik dan lingkungan, serta dari akses yang takterotorisasi dan kerusakan.

Panduan
Pedoman berikut sebaiknya dipertimbangkan untuk memproteksi peralatan:

a) menempatkan peralatan untuk meminimalkan akses yang takperlu ke area kerja dan untuk menghindari akses yang takterotorisasi;
b) dengan hati-hati memosisikan fasilitas pemrosesan informasi yang menangani data sensitif untuk mengurangi risiko informasi dilihat oleh orang yang takterotorisasi selama penggunaannya;
c) mengadopsi kontrol untuk meminimalkan risiko potensi ancaman fisik dan lingkungan [misalnya pencurian, kebakaran, bahan peledak, asap, air (atau kegagalan pasokan air),

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetik, dan vandalisme];
d) menetapkan pedoman untuk makan, minum, dan merokok di dekat fasilitas pemrosesan informasi;
e) memonitor kondisi lingkungan, seperti suhu dan kelembapan, untuk kondisi yang dapat berdampak buruk pada pengoperasian fasilitas pemrosesan informasi;
f) menerapkan penangkal petir pada semua bangunan dan memasang filter penangkal petir pada semua saluran listrik dan komunikasi yang masuk;
g) mempertimbangkan penggunaan metode proteksi khusus, seperti membran *keyboard*, untuk peralatan di lingkungan industri;
h) memproteksi peralatan yang memproses informasi konfidensial untuk meminimalkan risiko kebocoran informasi karena pancaran elektromagnetik;
i) secara fisik memisahkan fasilitas pemrosesan informasi yang dimanajemeni oleh organisasi dari yang tidak dimanajemeni oleh organisasi.

Informasi lain
Tidak ada informasi lain.

7.9 Keamanan aset di luar premis

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik#Manajemen_aset	#Proteksi

Kontrol
Aset di luar lokasi sebaiknya diproteksi.

Tujuan
Untuk mencegah kehilangan, kerusakan, pencurian, atau pembobolan peranti di luar lokasi dan interupsi pada operasi organisasi.

Panduan
Setiap peranti yang digunakan di luar premis organisasi yang menyimpan atau memproses informasi (misalnya peranti seluler), termasuk peranti yang dimiliki oleh organisasi dan peranti yang dimiliki secara pribadi dan digunakan atas nama organisasi [bawa peranti Anda sendiri (*Bring Your Own Device*-BYOD)] memerlukan proteksi. Penggunaan peranti ini sebaiknya diotorisasi oleh manajemen.

Pedoman berikut sebaiknya dipertimbangkan untuk proteksi peranti yang menyimpan atau memproses informasi di luar tempat organisasi:
a) tidak meninggalkan peralatan dan media penyimpanan yang dibawa keluar lokasi takterawasi di tempat umum dan takaman;
b) mengamati instruksi pabrikan untuk memproteksi peralatan setiap saat (misalnya proteksi terhadap paparan medan elektromagnetik yang kuat, air, panas, kelembapan, debu);
c) ketika peralatan di luar premis ditransfer dari satu individu ke individu lain atau pihak yang berkepentingan, memelihara log yang mendefinisikan rantai kustodi untuk peralatan tersebut termasuk setidaknya nama dan organisasi orang yang bertanggung jawab atas peralatan tersebut. Informasi yang tidak perlu ditransfer dengan aset sebaiknya dihapus dengan aman sebelum transfer;
d) jika perlu dan dapat dilakukan, mensyaratkan otorisasi untuk peralatan dan media yang akan dipindahkan dari premis organisasi dan menyimpan rekaman pemindahan tersebut

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

untuk memelihara jejak audit (lihat 5.14);
e) memproteksi agar tidak ada yang melihat informasi pada peranti (misalnya ponsel atau laptop) di transportasi umum, dan risiko yang terkait dengan *shoulder surfing*;
f) mengimplementasikan pelacakan lokasi dan kemampuan untuk menghapus peranti dari jarak jauh.

Instalasi permanen di luar premis organisasi [seperti antena dan anjungan tunai mandiri (ATM)] dapat memiliki risiko kerusakan, pencurian, atau penyadapan yang lebih tinggi. Risiko ini dapat sangat beragam antar lokasi dan sebaiknya diperhitungkan dalam menentukan langkah yang paling tepat. Pedoman berikut sebaiknya dipertimbangkan saat menempatkan peralatan tersebut di luar premis organisasi:
a) pemonitoran keamanan fisik (lihat 7.4);
b) memproteksi dari ancaman fisik dan lingkungan (lihat 7.5);
c) kontrol akses fisik dan anti-perusakan;
d) kontrol akses *logical*.

Informasi lain
Informasi lebih lanjut tentang aspek lain untuk memproteksi peralatan penyimpanan dan pemrosesan informasi dan peranti titik akhir pengguna dapat ditemukan di 8.1 dan 6.7.

7.10 Media penyimpanan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi

Kontrol
Media penyimpanan sebaiknya dimanajemeni melalui siklus hidup akuisisi, penggunaan, transportasi, dan pembuangan sesuai dengan skema klasifikasi organisasi dan persyaratan penanganan.

Tujuan
Untuk memastikan hanya pengungkapan, modifikasi, penghapusan, atau penghancuran informasi yang terotorisasi pada media penyimpanan.

Panduan
Media penyimpanan yang dapat dipindahkan
Panduan berikut untuk manajemen media penyimpanan yang dapat dipindahkan sebaiknya mempertimbangkan:
a) menetapkan kebijakan khusus spesifik tentang manajemen media penyimpanan yang dapat dipindahkan dan mengomunikasikan kebijakan khusus spesifik tersebut kepada siapa saja yang menggunakan atau menangani media penyimpanan yang dapat dipindahkan;
b) jika perlu dan dapat dilakukan, mensyaratkan otorisasi untuk media penyimpanan dipindahkan dari organisasi dan menyimpan rekaman pemindahan tersebut untuk memelihara jejak audit;
c) menyimpan semua media penyimpanan di lingkungan yang aman dan terjamin sesuai dengan klasifikasi informasinya dan memproteksinya dari ancaman lingkungan (seperti panas, uap, kelembapan, medan elektronik, atau penuaan), sesuai dengan spesifikasi pabrikan;
d) jika konfidensialitas atau integritas informasi adalah konsiderasi penting, menggunakan teknik kriptografi untuk memproteksi informasi pada media penyimpanan yang dapat

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dipindahkan;
e) untuk memitigasi risiko kerusakan media penyimpanan saat informasi yang disimpan masih diperlukan, mentransfer informasi ke media penyimpanan baru sebelum informasi tersebut takterbaca;
f) menyimpan beberapa salinan informasi berharga pada media penyimpanan terpisah untuk lebih mengurangi risiko kerusakan atau kehilangan informasi yang tak disengaja;
g) mempertimbangkan registrasi media penyimpanan yang dapat dipindahkan untuk membatasi kemungkinan kehilangan informasi;
h) hanya mengaktifkan porta media penyimpanan yang dapat dipindahkan [misalnya *Secure Digital* (SD) dan slot *universal serial bus* (USB) jika ada alasan organisasi untuk penggunaannya;
i) jika ada kebutuhan untuk menggunakan media penyimpanan yang dapat dipindahkan, memonitor transfer informasi ke media penyimpanan tersebut;
j) informasi mungkin rentan terhadap akses yang takterotorisasi, penyalahgunaan, atau perusakan selama pengangkutan secara fisik, misalnya ketika mengirim media penyimpanan melalui pos atau kurir.

Dalam kontrol ini, media termasuk dokumen kertas. Saat mentransfer media penyimpanan fisik, terapkan langkah-langkah keamanan di 5.14.

Penggunaan kembali atau pemusnahan yang aman
Prosedur untuk penggunaan kembali atau pemusnahan media penyimpanan yang aman sebaiknya ditetapkan untuk meminimalkan risiko kebocoran informasi konfidensial kepada orang yang takterotorisasi. Prosedur untuk penggunaan kembali atau pemusnahan media penyimpanan yang aman yang berisi informasi konfidensial sebaiknya proporsional dengan sensitivitas informasi tersebut. Hal-hal berikut sebaiknya dipertimbangkan:
a) jika media penyimpanan yang berisi informasi konfidensial perlu digunakan kembali dalam organisasi, menghapus data dengan aman atau memformat media penyimpanan sebelum digunakan kembali (lihat 8.10);
b) memusnahkan media penyimpanan yang berisi informasi konfidensial dengan aman bila tidak diperlukan lagi (misalnya dengan menghancurkan, memotong kecil-kecil, atau menghapus konten dengan aman);
c) memiliki prosedur identifikasi barang-barang yang dapat mensyaratkan pemusnahan yang aman;
d) banyak organisasi menawarkan layanan pengumpulan dan pemusnahan media penyimpanan. Kehati-hatian diperlukan dalam memilih pemasok pihak eksternal yang sesuai dengan kontrol dan pengalaman yang cukup;
e) membuat log pembuangan barang-barang sensitif untuk memelihara jejak audit;
f) ketika mengumpulkan media penyimpanan untuk dimusnahkan, mempertimbangkan efek agregasi, yang dapat menyebabkan sejumlah besar informasi nonsensitif menjadi sensitif.

Asesmen risiko sebaiknya dilakukan pada peranti rusak yang berisi data sensitif untuk menentukan apakah peranti tersebut sebaiknya dihancurkan secara fisik daripada diperbaiki atau dibuang (lihat 7.14).

Informasi lain
Ketika informasi konfidensial pada media penyimpanan tidak dienkripsi, proteksi fisik tambahan terhadap media penyimpanan sebaiknya dipertimbangkan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7.11 Utilitas pendukung

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_fisik	#Proteksi

Kontrol
Fasilitas pemrosesan informasi sebaiknya diproteksi dari kegagalan daya dan disrupsi lain yang disebabkan oleh kegagalan dalam utilitas pendukung.

Tujuan
Untuk mencegah kehilangan, kerusakan, atau pembobolan informasi dan aset terkait lainnya, atau interupsi pada operasi organisasi karena kegagalan serta disrupsi utilitas pendukung.

Panduan
Organisasi bergantung pada utilitas (misalnya listrik, telekomunikasi, pasokan air, gas, limbah, ventilasi, dan AC) untuk mendukung fasilitas pemrosesan informasinya. Oleh karena itu, organisasi sebaiknya:

a) memastikan peralatan yang mendukung utilitas dikonfigurasi, dioperasikan, dan dipelihara sesuai dengan spesifikasi pabrikan yang relevan;
b) memastikan kapasitas utilitas dinilai secara reguler untuk memenuhi pertumbuhan bisnis dan interaksi dengan utilitas pendukung lainnya;
c) memastikan peralatan yang mendukung utilitas diinspeksi dan diuji secara reguler untuk memastikannya berfungsi dengan layak;
d) jika perlu, ingatkan untuk mendeteksi malafungsi utilitas;
e) jika perlu, pastikan utilitas memiliki beberapa sumber dengan perutean fisik yang beragam;
f) memastikan peralatan yang mendukung utilitas berada pada jaringan terpisah dari fasilitas pemrosesan informasi jika terhubung ke jaringan;
g) memastikan peralatan yang mendukung utilitas terkoneksi ke internet hanya bila diperlukan dan hanya dengan cara yang aman.

Pencahayaan dan komunikasi darurat sebaiknya disediakan. Sakelar dan katup darurat untuk memutus listrik, air, gas, atau utilitas lainnya sebaiknya terletak di dekat pintu keluar darurat atau ruang peralatan. Detail kontak darurat sebaiknya direkam dan tersedia untuk personel jika terjadi pemadaman.

Informasi lain
Redundansi tambahan untuk konektivitas jaringan dapat diperoleh melalui beberapa rute dari lebih dari satu penyedia utilitas.

7.12 Keamanan perkabelan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi

Kontrol
Kabel yang menyalurkan listrik, data, atau layanan informasi pendukung sebaiknya diproteksi dari intersepsi, interferensi, atau kerusakan.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk mencegah kehilangan, kerusakan, pencurian, atau pembobolan informasi dan aset terkait lainnya serta gangguan pada operasi organisasi yang terkait dengan kabel listrik dan komunikasi.

Panduan
Panduan untuk keamanan kabel berikut sebaiknya dipertimbangkan:
a) saluran listrik dan telekomunikasi ke dalam fasilitas pemrosesan informasi berada di bawah tanah jika memungkinkan, atau bergantung pada proteksi alternatif yang cukup, seperti pelindung kabel lantai dan tiang utilitas; jika kabel berada di bawah tanah, memproteksi agar tidak terpotong (misalnya dengan pipa lapis baja atau tanda keberadaan);
b) mensegregasi kabel listrik dari kabel komunikasi untuk mencegah interefrensi
c) untuk sistem sensitif atau kritis, kontrol lebih lanjut yang perlu dipertimbangkan meliputi:
    1) instalasi pipa lapis baja dan ruangan atau kotak terkunci serta alarm di titik inspeksi dan terminasi;
    2) penggunaan pelindung elektromagnetik untuk memproteksi kabel;
    3) pemeriksaan teknis berkala dan inspeksi fisik untuk mendeteksi peranti takterotorisasi terpasang pada kabel;
    4) akses terkontrol ke panel *patch* dan ruang kabel (misalnya dengan kunci mekanis atau PIN);
    5) penggunaan kabel serat optik;
d) melabeli kabel di setiap ujung dengan detail sumber dan tujuan yang cukup untuk memungkinkan identifikasi fisik dan inspeksi kabel.

Saran spesialis sebaiknya dicari tentang cara memanajemeni risiko yang timbul dari insiden atau malafungsi kabel.

Informasi lain
Terkadang kabel listrik dan telekomunikasi adalah sumber daya bersama untuk lebih dari satu organisasi yang menempati premis yang digunakan bersama.

7.13 Pemeliharaan peralatan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik#Manajemen_aset	#Proteksi #Resiliensi

Kontrol
Peralatan sebaiknya dipelihara dengan benar untuk memastikan availabilitas, integritas, dan konfidensialitas informasi.

Tujuan
Untuk mencegah kehilangan, kerusakan, pencurian, atau pembobolan informasi dan aset terkait lainnya dan interupsi pada operasi organisasi yang disebabkan oleh kurangnya pemeliharaan.

Panduan
Pedoman berikut sebaiknya dipertimbangkan untuk pemeliharaan peralatan:
a) memelihara peralatan sesuai dengan frekuensi dan spesifikasi layanan yang direkomendasikan pemasok;
b) mengimplementasikan dan memonitor program pemeliharaan oleh organisasi;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

c) hanya personel pemeliharaan terotorisasi yang melakukan perbaikan dan pemeliharaan peralatan;
d) menyimpan rekaman semua kesalahan suspek atau aktual, dan semua pemeliharaan preventif dan korektif;
e) mengimplementasikan kontrol yang tepat ketika peralatan dijadwalkan untuk pemeliharaan, dengan memperhitungkan apakah pemeliharaan ini dilakukan oleh personel di lokasi atau di luar organisasi; membuat personel pemeliharaan tunduk pada perjanjian konfidensialitas yang cocok;
f) menyupervisi personel pemeliharaan saat melakukan pemeliharaan di lokasi;
g) mengotorisasi dan mengontrol akses untuk pemeliharaan jarak jauh;
h) menerapkan langkah-langkah keamanan untuk aset di luar premis (lihat 7.9) jika peralatan yang berisi informasi dibawa keluar premis untuk pemeliharaan;
i) mematuhi semua persyaratan pemeliharaan yang ditentukan oleh asuransi;
j) sebelum mengoperasikan kembali peralatan setelah pemeliharaan, menginspeksinya untuk memastikan bahwa peralatan belum dirusak dan berfungsi dengan baik;
k) menerapkan langkah-langkah untuk pembuangan atau penggunaan kembali peralatan secara aman (lihat 7.14) jika ditentukan bahwa peralatan akan dibuang.

Informasi lain
Peralatan termasuk komponen teknis fasilitas pemrosesan informasi, *uninterruptable power supply* (UPS) dan baterai, generator listrik, alternator dan konverter listrik, sistem deteksi intrusi fisik dan alarm, detektor asap, alat pemadam kebakaran, AC, dan lift.

7.14 Pemusnahan atau penggunaan kembali peralatan dengan aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memprotek si	#Keamanan_fisik#Manajemen_aset	#Proteksi

Kontrol
Peralatan yang berisi media penyimpanan sebaiknya diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dipindahkan atau ditimpa dengan aman sebelum dimusnahkan atau digunakan kembali.

Tujuan
Untuk mencegah kebocoran informasi dari peralatan yang akan dimusnahkan atau digunakan kembali.

Panduan
Peralatan sebaiknya diverifikasi untuk memastikan apakah media penyimpanan telah ditampung (*contained*) sebelum dimusnahkan atau digunakan kembali.

Media penyimpanan yang berisi informasi konfidensial atau berhak cipta sebaiknya dihancurkan secara fisik atau informasi sebaiknya dihancurkan, dihapus, atau ditimpa menggunakan teknik untuk membuat informasi asli tidak dapat diambil dari pada menggunakan fungsi hapus standar. Lihat 7.10 untuk panduan detail tentang pemusnahan media penyimpanan yang aman dan 8.10 untuk panduan penghapusan informasi.

Label dan tanda yang mengidentifikasi organisasi atau mengindikasikan klasifikasi, pemilik, sistem atau jaringan, sebaiknya dipindahkan sebelum dimusnahkan, termasuk penjualan kembali atau sumbangan untuk amal.

Organisasi sebaiknya mempertimbangkan pemindahan kontrol keamanan seperti kontrol

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

akses atau peralatan surveilans pada akhir sewa atau ketika berpindah premis. Ini tergantung pada faktor-faktor seperti:
a) perjanjian sewa untuk mengembalikan fasilitas ke kondisi orisinal;
b) meminimalkan risiko meninggalkan informasi sensitif pada sistem untuk penyewa berikutnya (contohnya daftar akses pengguna, fail video atau gambar);
c) kemampuan untuk menggunakan kembali kontrol di fasilitas berikutnya.

Informasi lain
Peralatan rusak yang berisi media penyimpanan dapat mensyaratkan asesmen risiko untuk menentukan apakah peralatan tersebut sebaiknya dihancurkan secara fisik daripada diperbaiki atau dibuang. Informasi dapat dibobol melalui kecerobohan pemusnahan atau penggunaan kembali peralatan.

Selain penghapusan diska yang aman, enkripsi diska penuh mengurangi risiko pengungkapan informasi konfidensial ketika peralatan dimusnahkan atau dipindahkan, dengan ketentuan bahwa:
a) proses enkripsi cukup kuat dan mencakup seluruh diska (termasuk *slack space, swap files*);
b) kunci kriptografi cukup panjang untuk menahan serangan *brute force*;
c) kunci kriptografi itu sendiri tetap konfidensial (contohnya tidak pernah disimpan pada diska yang sama).

Untuk saran lebih lanjut tentang kriptografi, lihat 8.24.

Teknik untuk menimpa media penyimpanan dengan aman berbeda sesuai dengan teknologi media penyimpanan dan level klasifikasi informasi pada media penyimpanan. Alat penimpa sebaiknya direviu untuk memastikan bahwa alat tersebut dapat diterapkan pada teknologi media penyimpanan tersebut.

Lihat ISO/IEC 27040 untuk detail tentang metode pembersihan media penyimpanan.

8 Kontrol teknologi

8.1 Perangkat titik akhir pengguna

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_aset #Proteksi_informasi	#Proteksi

Kontrol
Informasi yang disimpan, diproses, atau dapat diakses melalu peranti titik akhir pengguna sebaiknya diproteksi.

Tujuan
Untuk memproteksi informasi terhadap risiko yang muncul dari penggunaan peranti titik akhir pengguna.

Panduan
Umum
Organisasi sebaiknya menetapkan kebijakan topik spesifik tentang konfigurasi yang aman dan penanganan peranti titik akhir pengguna. Kebijakan topik spesifik tersebut sebaiknya dikomunikasikan kepada semua personel yang relevan dan mempertimbangkan hal berikut:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) tipe informasi dan level klasifikasi yang dapat ditangani, diproses, disimpan, atau didukung oleh peranti titik akhir pengguna;
b) registrasi peranti titik akhir pengguna;
c) persyaratan untuk proteksi fisik;
d) pembatasan instalasi perangkat lunak (misalnya dikontrol dari jarak jauh oleh administrator sistem);
e) persyaratan untuk perangkat lunak pada peranti titik akhir pengguna (termasuk versi perangkat lunak) dan untuk menerapkan pembaruan (misalnya pembaruan otomatis aktif);
f) aturan untuk koneksi ke layanan informasi, jaringan publik, atau jaringan lain di luar premis (misalnya membutuhkan penggunaan *firewall* pribadi);
g) kontrol akses;
h) enkripsi peranti penyimpanan;
i) proteksi terhadap perangkat perusak;
j) penonaktifan, penghapusan, atau penguncian jarak jauh;
k) pencadangan;
l) penggunaan layanan web dan aplikasi web;
m) analisis perilaku pengguna akhir (lihat 8.16);
n) penggunaan peranti yang dapat dipindahkan, termasuk peranti memori yang dapat dipindahkan, dan kemungkinan menonaktifkan porta fisik (misalnya porta USB);
o) penggunaan kapabilitas mempartisi, jika didukung oleh peranti titik akhir pengguna, yang dapat memisahkan informasi organisasi dan aset terkait lainnya (contohnya perangkat lunak) dengan aman dari informasi lain dan aset terkait lainnya di perangkat.

Konsiderasi sebaiknya diberikan apakah informasi tertentu sangat sensitif sehingga hanya dapat diakses melalui peranti titik akhir pengguna, tetapi tidak disimpan di peranti tersebut. Dalam kasus seperti itu, proteksi teknis tambahan mungkin disyaratkan pada perangkat. Misalnya, memastikan bahwa mengunduh fail untuk kerja luring dinonaktifkan dan penyimpanan lokal seperti kartu SD dinonaktifkan.

Sedapat mungkin, rekomendasi tentang kontrol ini sebaiknya ditegakkan melalui manajemen konfigurasi (lihat 8.9) atau alat otomatisasi.

Tanggung jawab pengguna

Semua pengguna sebaiknya memahami persyaratan dan prosedur keamanan untuk memproteksi peranti titik akhir pengguna, serta tanggung jawab mereka untuk mengimplementasikan langkah-langkah keamanan tersebut. Pengguna sebaiknya disarankan untuk:

a) log keluar sesi aktif dan menterminasi layanan bila tidak lagi diperlukan;
b) memproteksi peranti titik akhir pengguna dari penggunaan yang takterotorisasi dengan kontrol fisik (contohnya kunci gembok, kunci khusus) dan kontrol logikal (misalnya akses kata sandi) saat tidak digunakan; tidak meninggalkan peranti yang berisi informasi bisnis penting, sensitif, atau kritis tanpa pengawasan;
c) menggunakan peranti dengan sangat hati-hati di tempat umum, kantor terbuka, tempat pertemuan, dan area tidak terlindungi lainnya (contohnya menghindari orang membaca informasi konfidensial dari belakang, gunakan filter layar privasi);
d) secara fisik memproteksi peranti titik akhir pengguna terhadap pencurian (contohnya di mobil dan bentuk transportasi lainnya, kamar hotel, pusat konferensi, dan tempat pertemuan).

Prosedur spesifik dengan memperhitungkan legal, statutori, regulatori, kontraktual (termasuk asuransi), dan persyaratan keamanan organisasi lainnya sebaiknya ditetapkan untuk kasus pencurian atau kehilangan peranti titik akhir pengguna.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Penggunaan peranti personal
Jika organisasi mengizinkan penggunaan peranti pribadi (kadang-kadang dikenal sebagai BYOD), selain panduan yang diberikan dalam kontrol ini, hal-hal berikut sebaiknya dipertimbangkan:

a) separasi penggunaan personal dan bisnis atas perangkat, termasuk menggunakan perangkat lunak untuk mendukung separasi tersebut dan memproteksi data bisnis pada peranti pribadi;
b) menyediakan akses ke informasi bisnis hanya setelah pengguna mengakui tugasnya (proteksi fisik, pembaruan perangkat lunak, dll.), melepaskan kepemilikan data bisnis, memungkinkan penghapusan data dari jarak jauh oleh organisasi jika terjadi pencurian atau kehilangan peranti atau ketika pengguna tidak lagi terotorisasi untuk menggunakan layanan. Dalam kasus seperti itu, legislasi proteksi PII sebaiknya dipertimbangkan;
c) kebijakan dan prosedur topik spesifik untuk mencegah perselisihan mengenai hak atas kekayaan intelektual yang dikembangkan pada peralatan yang dimiliki secara privat
d) akses ke peralatan yang dimiliki secara privat (untuk memverifikasi keamanan mesin atau selama investigasi), yang dapat dicegah dengan legislasi;
e) perjanjian lisensi perangkat lunak yang sedemikian rupa sehingga organisasi dapat bertanggung jawab atas lisensi untuk perangkat lunak klien pada peranti titik akhir pengguna yang dimiliki secara privat oleh personel atau pengguna pihak eksternal.

Koneksi nirkabel
Organisasi sebaiknya menetapkan prosedur untuk:

a) konfigurasi koneksi nirkabel pada peranti (contohnya menonaktifkan protokol yang rentan);
b) menggunakan koneksi nirkabel atau kabel dengan *bandwidth* yang tepat sesuai dengan kebijakan topik spesifik yang relevan (contohnya karena diperlukan pencadangan atau pembaruan perangkat lunak).

Informasi lain
Kontrol untuk memproteksi informasi pada peranti titik akhir pengguna bergantung pada apakah peranti titik akhir pengguna hanya digunakan di dalam premis dan koneksi jaringan aman organisasi, atau apakah peranti tersebut mengalami peningkatan ancaman fisik dan jaringan terkait di luar organisasi.

Koneksi nirkabel untuk peranti titik akhir pengguna mirip dengan tipe koneksi jaringan lainnya tetapi memiliki perbedaan penting yang sebaiknya dipertimbangkan saat mengidentifikasi kontrol. Secara khusus, pencadangan informasi yang disimpan pada peranti titik akhir pengguna terkadang gagal karena *bandwidth* jaringan yang terbatas atau karena peranti titik akhir pengguna tidak terhubung pada saat pencadangan dijadwalkan.

Untuk beberapa porta USB, seperti USB-C, menonaktifkan porta USB tidak dimungkinkan karena digunakan untuk tujuan lain (misalnya pengiriman daya dan keluaran tampilan).

8.2 Hak akses privilese

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Alokasi dan penggunaan hak akses privilese sebaiknya dibatasi dan dimanajemeni.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk memastikan hak akses privilese hanya diberikan pada pengguna, komponen, dan layanan perangkat lunak yang terotorisasi.

Panduan
Alokasi hak akses privilese sebaiknya dikontrol melalui proses otorisasi sesuai dengan kebijakan topik spesifik yang relevan pada kontrol akses (lihat 5.15). Hal-hal berikut sebaiknya dipertimbangkan:

a) mengidentifikasi pengguna yang membutuhkan hak akses privilese untuk setiap sistem atau proses (misalnya sistem operasi, sistem manajemen pangkalan data, dan aplikasi);
b) mengalokasikan hak akses privilese kepada pengguna sesuai kebutuhan dan berdasarkan peristiwa sesuai dengan kebijakan topik spesifik pada kontrol akses (lihat 5.15) (yaitu hanya untuk individual dengan kompetensi yang diperlukan untuk melakukan aktivitas yang memerlukan akses privilese dan berdasarkan persyaratan minimum untuk peran fungsionalnya
c) memelihara proses otorisasi (yaitu menentukan siapa yang dapat menyetujui hak akses privilese, atau tidak memberikan hak akses privilese sampai proses otorisasi selesai) dan rekaman semua hak privilese yang dialokasikan;
d) mendefinisikan dan mengimplementasikan persyaratan berakhirnya hak akses privilese;
e) mengambil langkah-langkah untuk memastikan bahwa pengguna mengetahui hak akses privilesenya dan ketika mereka berada dalam mode akses privilese. Langkah-langkah yang mungkin termasuk menggunakan identitas pengguna tertentu, pengaturan antarmuka pengguna, atau bahkan peralatan spesifik;
f) persyaratan autentikasi untuk hak akses privilese dapat lebih tinggi dari persyaratan untuk hak akses normal. Langkah autentikasi ulang atau autentikasi mungkin diperlukan sebelum melakukan pekerjaan dengan hak akses privilese;
g) secara reguler, dan setelah segala perubahan organisasi, mereviu pengguna yang bekerja dengan hak akses privilese untuk memverifikasi apakah tugas, peran, tanggung jawab, dan kompetensi mereka masih memenuhi syarat untuk bekerja dengan hak akses privilese (lihat 5.18);
h) menetapkan aturan spesifik untuk menghindari penggunaan identitas pengguna administrasi generik (seperti "*root*"), tergantung pada kapabilitas konfigurasi sistem. Memanajemeni dan memproteksi informasi autentikasi identitas tersebut (lihat 5.17);
i) memberikan akses privilese sementara hanya untuk jendela waktu yang diperlukan untuk mengimplementasikan perubahan atau aktivitas yang disetujui (misalnya untuk aktivitas pemeliharaan atau beberapa perubahan kritis), daripada secara permanen memberikan hak akses privilese. Ini sering disebut sebagai prosedur *break glass*, dan sering diotomatisasi oleh teknologi manajemen akses privilese;
j) membuat log semua akses privilese ke sistem untuk tujuan audit;
k) tidak berbagi atau menghubungkan identitas dengan hak akses privilese ke banyak orang, menetapkan identitas terpisah untuk setiap orang yang memungkinkan penetapan hak akses privilese spesifik. Identitas dapat dikelompokkan (misalnya dengan mendefinisikan grup administrator) untuk menyederhanakan manajemen hak akses privilese;
l) hanya menggunakan identitas dengan hak akses privilese untuk melakukan tugas administratif dan bukan untuk tugas umum sehari-hari [yaitu memeriksa surel, mengakses web (pengguna sebaiknya memiliki identitas jaringan normal yang terpisah untuk aktivitas ini)].

Informasi lain
Hak akses privilese adalah hak akses yang diberikan kepada identitas, peran, atau proses yang memungkinkan kinerja aktivitas yang tidak dapat dilakukan oleh pengguna atau proses tipikal. Peran administrator sistem biasanya memerlukan hak akses privilese.

Penggunaan hak privilese administrator sistem yang tidak tepat (fitur atau fasilitas apa pun

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

dari sistem informasi yang memungkinkan pengguna untuk mengesampingkan kontrol sistem atau aplikasi) merupakan faktor penyumbang utama kegagalan atau pelanggaran sistem.

Informasi lebih lanjut yang berkaitan dengan manajemen akses dan manajemen akses secara aman ke sumber daya informasi dan informasi dan teknologi komunikasi dapat ditemukan dalam ISO/IEC 29146.

8.3 Pembatasan akses informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Kontrol
Akses ke informasi dan aset terkait lainnya sebaiknya dibatasi sesuai dengan kebijakan topik spesifik yang ditetapkan pada kontrol akses.

Tujuan
Untuk memastikan hanya akses yang terotorisasi dan untuk mencegah akses yang takterotorisasi ke informasi dan aset terkait lainnya.

Panduan
Akses ke informasi dan aset terkait lainnya sebaiknya dibatasi sesuai dengan kebijakan topik spesifik yang ditetapkan. Berikut ini sebaiknya dipertimbangkan untuk mendukung persyaratan pembatasan akses:

a) tidak mengizinkan akses identitas pengguna yang tidak dikenal atau secara anonim ke informasi sensitif. Akses publik atau anonim hanya boleh diberikan ke lokasi penyimpanan yang tidak berisi informasi sensitif apa pun;
b) menyediakan mekanisme konfigurasi untuk mengontrol akses ke informasi dalam sistem, aplikasi, dan layanan;
c) mengontrol data mana yang dapat diakses oleh pengguna tertentu;
d) mengontrol identitas atau kelompok identitas mana yang memiliki akses tertentu, seperti membaca, menulis, menghapus, dan mengeksekusi;
e) menyediakan kontrol akses fisik atau logikal untuk isolasi aplikasi sensitif, data aplikasi, atau sistem.

Selanjutnya teknik dan proses manajemen akses dinamis untuk memproteksi informasi sensitif yang memiliki nilai tinggi bagi organisasi sebaiknya dipertimbangkan ketika organisasi:

a) membutuhkan kontrol granular atas siapa yang dapat mengakses informasi tersebut selama periode dan dengan cara tertentu;
b) ingin berbagi informasi tersebut dengan orang di luar organisasi dan memelihara kontrol atas siapa yang dapat mengaksesnya;
c) ingin memanajemeni, secara waktu-nyata, penggunaan dan distribusi informasi tersebut secara dinamis;
d) ingin memproteksi informasi tersebut terhadap perubahan, penyalinan, dan distribusi (termasuk pencetakan) yang takterotorisasi;
e) ingin memonitor penggunaan informasi;
f) ingin merekam setiap perubahan pada informasi tersebut yang terjadi jika diperlukan investigasi di masa depan.

Teknik manajemen akses dinamis sebaiknya memproteksi informasi sepanjang siklus hidupnya (yaitu pembuatan, pemrosesan, penyimpanan, transmisi, dan pemusnahan),

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

termasuk:
a) menetapkan aturan tentang manajemen akses dinamis berdasarkan kasus penggunaan spesifik dengan mempertimbangkan:
   1) memberikan izin akses berdasarkan identitas, perangkat, lokasi, atau aplikasi;
   2) memanfaatkan skema klasifikasi untuk menentukan informasi apa yang perlu diproteksi dengan teknik manajemen akses dinamis;
b) menyusun proses operasional, pemonitoran, dan pelaporan serta infrastruktur teknis pendukung

Sistem manajemen akses dinamis sebaiknya memproteksi informasi dengan:
a) mensyaratkan adanya autentikasi, kredensial yang tepat, atau sertifikat untuk mengakses informasi;
b) membatasi akses, misalnya ke jangka waktu tertentu (contohnya setelah tanggal tertentu atau sampai tanggal tertentu);
c) menggunakan enkripsi untuk memproteksi informasi;
d) mendefinisikan izin pencetakan informasi;
e) merekam siapa yang mengakses informasi dan bagaimana informasi tersebut digunakan;
f) memicu peringatan jika upaya penyalahgunaan informasi terdeteksi.

Informasi lain
Teknik manajemen akses dinamis dan teknologi proteksi informasi dinamis lainnya dapat mendukung proteksi informasi bahkan ketika data dibagikan di luar organisasi asal, tempat kontrol akses biasa tidak dapat ditegakkan. Ini dapat diterapkan pada dokumen, surel, atau fail lain yang berisi informasi untuk membatasi siapa yang dapat mengakses konten dan dengan cara apa. Ini bisa dilakukan pada level granular dan disesuaikan selama siklus hidup informasi.

Teknik manajemen akses dinamis tidak menggantikan manajemen akses klasik [contohnya menggunakan *access control list* (ACL)], tetapi dapat menambahkan lebih banyak faktor untuk persyaratan, evaluasi waktu-nyata, reduksi data tepat waktu, dan peningkatan lain yang dapat berguna untuk informasi yang paling sensitif. Teknik tersebut menawarkan cara untuk mengontrol akses di luar lingkungan organisasi. Respons insiden dapat didukung oleh teknik manajemen akses dinamis karena izin dapat dimodifikasi atau dicabut kapan saja.

Informasi tambahan tentang kerangka kerja untuk manajemen akses tersedia dalam ISO/IEC 29146.

8.4 Akses ke kode sumber

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses #Keamanan_aplikasi #Konfigurasi_yang_aman	#Proteksi

Kontrol
Akses untuk membaca dan menulis ke kode sumber, alat pengembangan, dan pustaka perangkat lunak sebaiknya dimanajemeni dengan tepat.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk mencegah munculnya fungsionalitas yang takterotorisasi, hindari perubahan yang takdisengaja atau berbahaya dan untuk memelihara konfidensialitas kekayaan intelektual yang berharga.

Panduan
Akses ke kode sumber dan hal-hal terkait (seperti desain, spesifikasi, rencana verifikasi, dan rencana validasi) dan alat pengembangan (misalnya kompilator, pembangun, alat integrasi, platform uji, dan lingkungan) sebaiknya dikontrol secara ketat.

Untuk kode sumber, hal ini dapat dicapai dengan mengontrol penyimpanan pusat kode tersebut, terutama dalam sistem manajemen kode sumber.

Akses untuk membaca dan menulis ke kode sumber dapat beragam berdasarkan peran personel. Misalnya, akses baca ke kode sumber dapat tersedia secara luas di dalam organisasi, tetapi akses menulis ke kode sumber hanya tersedia untuk personel privelese atau pemilik yang ditunjuk. Jika komponen kode digunakan oleh beberapa developer dalam suatu organisasi, sebaiknya diimplementasikan akses baca ke repositori kode terpusat. Selain itu, jika kode sumber terbuka atau komponen kode pihak ketiga digunakan di dalam organisasi, akses baca ke repositori kode eksternal tersebut dapat disediakan secara luas. Namun, akses untuk menulis masih sebaiknya dibatasi.

Pedoman berikut sebaiknya dipertimbangkan untuk mengontrol akses ke pustaka sumber program dalam rangka mengurangi potensi kerusakan program komputer:
a) memanajemeni akses ke kode sumber program dan pustaka sumber program sesuai dengan prosedur yang ditetapkan;
b) memberikan akses untuk membaca dan menulis ke kode sumber berdasarkan kebutuhan bisnis dan mengatasi risiko alterasi atau penyalahgunaan serta sesuai dengan prosedur yang ditetapkan;
c) memperbarui kode sumber dan hal-hal terkait serta pemberian akses ke kode sumber sesuai dengan prosedur kontrol perubahan (lihat 8.32) dan hanya melakukannya setelah memperoleh otorisasi yang tepat;
d) tidak memberikan akses langsung ke repositori kode sumber kepada developer, tetapi melalui alat developer yang mengontrol aktivitas dan otorisasi pada kode sumber;
e) memegang daftar program di lingkungan yang aman, tempat akses membaca dan menulis sebaiknya dimanajemeni dan ditetapkan dengan tepat;
f) memelihara log audit dari semua akses dan semua perubahan pada kode sumber.

Jika kode sumber program ingin dipublikasikan, sebaiknya dipertimbangkan kontrol tambahan untuk memberikan jaminan integritasnya (contohnya tanda tangan digital).

Informasi lain
Jika akses ke kode sumber tidak dikontrol dengan benar, kode sumber dapat dimodifikasi atau beberapa data di lingkungan pengembangan (misalnya salinan data produksi, detail konfigurasi) dapat diambil oleh orang yang takterotorisasi.

8.5 Autentikasi aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Manajemen_identitas_dan_akses	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Kontrol
Teknologi dan prosedur autentikasi yang aman sebaiknya diimplementasikan berdasarkan pembatasan akses informasi dan kebijakan topik spesifik pada kontrol akses.

Tujuan
Untuk memastikan pengguna atau entitas diautentikasi dengan aman, ketika akses ke sistem, aplikasi, dan layanan diberikan.

Panduan
Teknik autentikasi yang cocok sebaiknya dipilih untuk membuktikan identitas yang diklaim dari pengguna, perangkat lunak, pesan, dan entitas lainnya.

Kekuatan autentikasi sebaiknya tepat untuk klasifikasi informasi yang akan diakses. Jika autentikasi yang kuat dan verifikasi identitas diperlukan, alternatif metode autentikasi selain kata sandi, seperti sertifikat digital, kartu pintar, token, atau sarana biometrik, sebaiknya digunakan.

Informasi autentikasi sebaiknya disertai dengan faktor autentikasi tambahan untuk mengakses sistem informasi kritis (juga dikenal sebagai autentikasi multifaktor). Menggunakan kombinasi beberapa faktor autentikasi, seperti apa yang Anda ketahui, apa yang Anda miliki, dan siapa Anda, mengurangi kemungkinan untuk akses yang takterotorisasi. Autentikasi multifaktor dapat dikombinasikan dengan teknik lain untuk mensyaratkan faktor tambahan dalam keadaan tertentu, berdasarkan aturan dan pola yang telah ditentukan, seperti akses dari lokasi yang tidak biasa, dari peranti yang tidak biasa atau pada waktu yang tidak biasa.

Informasi autentikasi biometrik sebaiknya dibatalkan jika pernah dibobol. Autentikasi biometrik mungkin taktersedia tergantung pada kondisi penggunaan (misalnya kelembapan atau penuaan). Untuk mengantisipasi isu ini, autentikasi biometrik sebaiknya disertai dengan setidaknya satu teknik autentikasi alternatif.

Prosedur untuk membuat log ke sistem atau aplikasi sebaiknya didesain untuk meminimalkan risiko akses yang takterotorisasi. Prosedur dan teknologi log masuk sebaiknya diimplementasikan dengan mempertimbangkan hal-hal berikut:

a) tidak menampilkan sistem sensitif atau informasi aplikasi sampai proses *log-on* berhasil diselesaikan untuk menghindari pemberian bantuan yang takterotorisasi kepada pengguna yang takterotorisasi;
b) menampilkan peringatan pemberitahuan umum bahwa sistem atau aplikasi atau layanan hanya boleh diakses oleh pengguna yang terotorisasi;
c) tidak memberikan pesan bantuan selama prosedur log masuk yang akan membantu pengguna yang takterotorisasi (misalnya jika galat muncul, sistem tidak boleh menunjukkan bagian mana dari data yang benar atau salah);
d) memvalidasi informasi log masuk hanya setelah menyelesaikan semua data input;
e) memproteksi terhadap upaya *brute force* log masuk pada nama pengguna dan kata sandi [misalnya menggunakan tes Turing publik yang sepenuhnya otomatis untuk membedakan komputer dan manusia (CAPTCHA), dengan mensyaratkan pengaturan ulang kata sandi setelah sejumlah upaya gagal yang telah ditentukan sebelumnya atau memblokir pengguna setelah jumlah maksimum galat];
f) upaya membuat log yang takberhasil dan berhasil;
g) menindaklanjuti peristiwa keamanan jika potensi percobaan atau keberhasilan pelanggaran kontrol log masuk terdeteksi (misalnya mengirim peringatan kepada pengguna dan administrator sistem organisasi ketika sejumlah upaya kata sandi yang salah telah tercapai);
h) menampilkan atau mengirim informasi berikut pada saluran terpisah setelah berhasil masuk:
    1) tanggal dan waktu log masuk sukses sebelumnya;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

2) detail dari setiap upaya log masuk yang gagal sejak upaya log masuk terakhir yang berhasil;

i) tidak menampilkan kata sandi dalam teks yang jelas saat dimasukkan; dalam beberapa kasus, mungkin perlu untuk menonaktifkan fungsi ini untuk memfasilitasi log masuk pengguna (misalnya untuk alasan aksesibilitas atau untuk menghindari pemblokiran pengguna karena kesalahan berulang);

j) tidak mentransmisikan kata sandi dalam teks yang jelas melalui jaringan agar tidak tertangkap oleh program "*sniffer*" jaringan;

k) menterminasi sesi tidak aktif setelah periode takaktif yang ditentukan, terutama di lokasi berisiko tinggi seperti area publik atau eksternal di luar manajemen keamanan organisasi atau pada peranti titik akhir pengguna;

l) membatasi waktu durasi koneksi untuk memberikan keamanan tambahan untuk aplikasi berisiko tinggi dan mengurangi jendela peluang untuk akses yang takterotorisasi.

Informasi lain
Informasi tambahan tentang keyakinan autentikasi entitas dapat ditemukan dalam ISO/IEC 29115.

8.6 Manajemen kapasitas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Integritas #Availabilitas	#Mengidentifikasi #Memproteksi #Mendeteksi	#Kontinuitas	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Penggunaan sumber daya sebaiknya dimonitor dan disesuaikan sejalan dengan persyaratan kapasitas saat ini dan yang diharapkan.

Tujuan
Untuk memastikan kapasitas yang disyaratkan untuk fasilitas pengolahan informasi, sumber daya manusia, kantor, dan fasilitas lainnya.

Panduan
Persyaratan kapasitas untuk fasilitas pemrosesan informasi, sumber daya manusia, kantor, dan fasilitas lainnya sebaiknya diidentifikasi, dengan memperhitungkan kekritisan bisnis dari sistem dan proses yang bersangkutan.
Penyetelan dan pemonitoran sistem sebaiknya diterapkan untuk memastikan serta, jika perlu, meningkatkan availabilitas dan efisiensi sistem.

Organisasi sebaiknya melakukan uji tekanan sistem dan layanan untuk mengonfirmasi bahwa kapasitas sistem yang cukup tersedia untuk memenuhi persyaratan kinerja puncak.

Kontrol detektif sebaiknya dilakukan untuk menunjukkan problem pada waktunya.

Proyeksi persyaratan kapasitas masa depan sebaiknya memperhitungkan persyaratan bisnis dan sistem baru serta tren saat ini dan diproyeksikan dalam kapabilitas pemrosesan informasi organisasi.

Sebaik diberikan atensi khusus bagi sumber daya apa pun dengan waktu tunggu pengadaan yang lama atau biaya tinggi. Oleh karena itu, manajer, pemilik layanan, atau produk sebaiknya memonitor pemanfaatan sumber daya sistem utama.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Manajer sebaiknya menggunakan informasi kapasitas untuk mengidentifikasi dan menghindari potensi limitasi sumber daya dan ketergantungan pada personel kunci yang dapat menghadirkan ancaman terhadap keamanan atau layanan sistem dan merencanakan tindakan yang tepat.

Penyediaan kapasitas yang memadai dapat dicapai dengan meningkatkan kapasitas atau dengan mengurangi permintaan. Berikut ini sebaiknya dipertimbangkan untuk meningkatkan kapasitas:

a) mempekerjakan personel baru;
b) mendapatkan fasilitas atau ruang baru;
c) memperoleh sistem pemrosesan, memori, dan penyimpanan yang lebih kuat;
d) memanfaatkan komputasi awan, yang memiliki karakteristik melekat yang secara langsung mengatasi masalah kapasitas. Komputasi awan memiliki elastisitas dan skalabilitas yang memungkinkan ekspansi cepat sesuai permintaan dan reduksi sumber daya yang tersedia untuk aplikasi dan layanan tertentu.

Berikut ini sebaiknya dipertimbangkan untuk mereduksi permintaan pada sumber daya organisasi:

a) penghapusan data usang (ruang diska);
b) pemusnahan rekaman salinan cetak yang telah memenuhi periode retensinya (mengosongkan ruang rak);
c) penonaktifkan aplikasi, sistem, pangkalan data, atau lingkungan;
d) mengoptimalkan proses dan jadwal *batch*;
e) mengoptimalkan kode aplikasi atau kueri pangkalan data;
f) menolak atau membatasi *bandwidth* untuk layanan yang memakan sumber daya jika tidak kritis (misalnya *streaming* video).

Rencana manajemen kapasitas yang terdokumentasi sebaiknya dipertimbangkan untuk sistem kritis misi.

Informasi lain
Untuk detail lebih lanjut tentang elastisitas dan skalabilitas komputasi awan, lihat ISO/IEC TS 23167.

8.7 Proteksi terhadap perangkat perusak

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si #Mendeteksi	#Keamanan_sistem_dan_jaringan #Proteksi_informasi	#Proteksi #Pertahanan

Kontrol
Proteksi terhadap perangkat perusak sebaiknya diimplementasikan dan didukung oleh kesadaran pengguna yang tepat.

Tujuan
Untuk memastikan informasi dan aset terkait lainnya diproteksi dari perangkat perusak.

Panduan
Proteksi terhadap perangkat perusak sebaiknya berdasarkan pada perangkat lunak deteksi dan perbaikan dari perangkat perusak, kesadaran keamanan informasi, akses sistem yang tepat, dan kontrol manajemen perubahan. Penggunaan perangkat lunak deteksi dan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

perbaikan dari perangkat perusak saja biasanya tidak cukup. Panduan berikut sebaiknya dipertimbangkan:

a) mengimplementasikan aturan dan kontrol yang mencegah atau mendeteksi penggunaan perangkat lunak yang takterotorisasi [misalnya daftar izin aplikasi (yaitu menggunakan daftar yang berisi aplikasi yang diizinkan)] (lihat 8.19 dan 8.32);
b) mengimplementasikan kontrol yang mencegah atau mendeteksi penggunaan situs web berbahaya yang diketahui atau dicurigai (misalnya daftar blokir);
c) mengurangi kerentanan yang dapat dieksploitasi oleh perangkat perusak [misalnya melalui manajemen kerentanan teknis (lihat 8.8 dan 8.19)];
d) melakukan validasi otomatis reguler terhadap perangkat lunak dan konten data sistem, terutama untuk sistem yang mendukung proses bisnis penting; menginvestigasi adanya fail yang tidak disetujui atau perubahan yang takterotorisasi;
e) menetapkan langkah protektif terhadap risiko yang terkait dengan perolehan fail dan perangkat lunak baik dari atau melalui jaringan eksternal atau pada media lain;
f) menginstal dan secara reguler memperbarui perangkat lunak deteksi dan perbaikan dari perangkat perusak untuk memindai komputer dan media penyimpanan elektronik. Melakukan pemindaian rutin yang meliputi:
    1) memindai data apa pun yang diterima melalui jaringan atau melalui segala bentuk media penyimpanan elektronik, untuk menemukan perangkat perusak sebelum digunakan;
    2) memindai lampiran surel dan pesan instan dan unduhan untuk menemukan perangkat perusak sebelum digunakan. Melakukan pemindaian ini di tempat yang berbeda (misalnya di server surel, komputer desktop), dan saat memasuki jaringan organisasi;
    3) memindai halaman web untuk menemukan perangkat perusak saat diakses;
g) menentukan penempatan dan konfigurasi alat deteksi dan perbaikan dari perangkat perusak berdasarkan hasil asesmen risiko dan mempertimbangkan:
    1) prinsip pertahanan berlapis di lokasi yang paling efektif. Sebagai contoh, deteksi perangkat perusak di gerbang jaringan (dalam keberagaman protokol aplikasi seperti surel, transfer fail, dan web) serta peranti dan server titik akhir pengguna;
    2) teknik penghindaran oleh pihak penyerang (misalnya penggunaan fail terenkripsi) dalam pengantaran perangkat perusak atau penggunaan protokol enkripsi untuk mengirimkan perangkat perusak;
h) berhati-hati untuk memproteksi terhadap munculnya perangkat perusak selama masa pemeliharaan dan prosedur darurat, yang dapat melewati kontrol normal terhadap perangkat perusak;
i) mengimplementasikan proses untuk mengotorisasi sementara atau secara permanen menonaktifkan sebagian atau semua tindakan terhadap perangkat perusak, termasuk otoritas persetujuan eksepsi, justifikasi yang terdokumentasi, dan tanggal reviu. Ini mungkin diperlukan ketika proteksi terhadap perangkat perusak menyebabkan disrupsi pada operasi normal;
j) menyiapkan rencana kontinuitas bisnis yang tepat untuk pemulihan dari serangan perangkat perusak, termasuk semua cadangan data dan perangkat lunak yang diperlukan (termasuk pencadangan daring dan luring) serta langkah-langkah pemulihan (lihat 8.13);
k) mengisolasi lingkungan dimana konsekuensi bencana dapat terjadi;
l) mendefinisikan prosedur dan tanggung jawab untuk menangani proteksi terhadap perangkat perusak pada sistem, termasuk pelatihan dalam penggunaan, pelaporan, dan pemulihan dari serangan perangkat perusak;
m) memberikan kesadaran atau pelatihan (lihat 6.3) kepada semua pengguna tentang bagaimana mengidentifikasi dan memitigasi kemungkinan penerimaan, pengiriman, atau instalasi surel, fail, atau program yang terinfeksi perangkat perusak [informasi yang dikumpulkan dalam n) dan o) dapat digunakan untuk memastikan kesadaran serta pelatihan tetap mutakhir];
n) mengimplementasikan prosedur untuk secara reguler mengumpulkan informasi tentang

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

perangkat perusak baru, seperti berlangganan milis atau mereviu situs web yang relevan;

o) memverifikasi bahwa informasi yang berkaitan dengan perangkat perusak, seperti buletin peringatan, berasal dari sumber yang berkualitas dan bereputasi (misalnya situs web yang dapat diandalkan atau pemasok perangkat lunak deteksi perangkat perusak) serta akurat dan informatif.

Informasi lain

Terkadang tidak selalu mungkin untuk menginstal perangkat lunak yang memberi proteksi terhadap perangkat perusak pada beberapa sistem (misalnya pada beberapa sistem kontrol industri). Beberapa bentuk perangkat perusak menginfeksi sistem operasi komputer dan *firmware* komputer sedemikian sehingga kontrol perangkat perusak umum tidak dapat membersihkan sistem, dalam hal ini, pemulihan sistem berupa pencitraan ulang penuh sistem operasi dan terkadang *firmware* komputer diperlukan untuk kembali ke keadaan aman.

8.8 Manajemen kerentanan teknis

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Manajemen_ancaman_dan_kerentanan	#Tata_kelola_dan_Ekosistem #Proteksi #Pertahanan

Kontrol

Informasi kerentanan teknis dari sistem informasi yang sedang digunakan sebaiknya diperoleh, eksposur organisasi terhadap kerentanan tersebut sebaiknya dievaluasi, dan langkah-langkah yang tepat sebaiknya diambil.

Tujuan

Untuk mencegah eksploitasi terhadap kerentanan teknis.

Panduan

Mengidentifikasi kerentanan teknis

Organisasi sebaiknya memiliki inventaris aset yang akurat (lihat 5.9 hingga 5.14) sebagai prasyarat untuk manajemen kerentanan teknis yang efektif; inventaris sebaiknya mencakup vendor perangkat lunak, nama perangkat lunak, nomor versi, penyebaran saat ini (misalnya perangkat lunak apa yang diinstal pada sistem apa), dan orang dalam organisasi yang bertanggung jawab atas perangkat lunak.

Untuk mengidentifikasi kerentanan teknis, organisasi sebaiknya mempertimbangkan:

a) mendefinisikan dan menetapkan peran dan tanggung jawab yang terkait dengan manajemen kerentanan teknis, termasuk pemonitoran kerentanan, asesmen risiko kerentanan, pembaruan, pelacakan aset, dan tanggung jawab koordinasi apa pun yang dipersyaratkan;

b) untuk perangkat lunak dan teknologi lainnya (berdasarkan daftar inventaris aset, lihat 5.9), sebaiknya dapat mengidentifikasi sumber daya informasi yang akan digunakan untuk mengidentifikasi kerentanan teknis dan memelihara kesadaran tentang kerentanan tersebut. Memperbarui daftar sumber daya informasi berdasarkan perubahan dalam inventaris aset atau ketika diketahuinya sumber daya baru atau sumber daya lainnya yang berguna;

c) mensyaratkan pemasok sistem informasi (termasuk komponennya) untuk memastikan pelaporan, penanganan, dan pengungkapan kerentanan, termasuk persyaratan dalam kontrak yang berlaku (lihat 5.20);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) menggunakan alat pemindaian kerentanan yang tepat bagi teknologi yang digunakan untuk mengidentifikasi kerentanan dan untuk memverifikasi apakah penambalan kerentanan berhasil;
e) melakukan uji penetrasi atau asesmen kerentanan yang terencana, terdokumentasikan, dan dilakukan secara berulang oleh orang yang kompeten dan terotorisasi untuk mendukung identifikasi kerentanan. Organisasi perlu berhati-hati karena aktivitas tersebut dapat menyebabkan pembobolan keamanan sistem;
f) melacak penggunaan pustaka dan kode sumber pihak ketiga untuk kerentanan. Tindakan ini sebaiknya dimasukkan dalam pengodean yang aman (lihat 8.28).

Organisasi sebaiknya mengembangkan prosedur dan kapabilitas untuk:
a) mendeteksi eksistensi kerentanan dalam produk dan layanannya termasuk komponen eksternal apa pun yang digunakan;
b) menerima laporan kerentanan dari sumber internal atau eksternal.

Organisasi sebaiknya memberikan titik kontak publik sebagai bagian dari kebijakan topik spesifik tentang pengungkapan kerentanan sehingga peneliti dan orang lain dapat melaporkan isu. Organisasi sebaiknya menetapkan prosedur pelaporan kerentanan, formulir pelaporan daring, dan memanfaatkan intelijen ancaman yang sesuai atau forum berbagi informasi. Organisasi juga sebaiknya mempertimbangkan program *bug bounty* yang menawarkan hadiah sebagai insentif untuk membantu organisasi dalam mengidentifikasi kerentanan agar dapat memulihkannya dengan tepat. Organisasi juga sebaiknya berbagi informasi dengan badan industri yang kompeten atau pihak lain yang berkepentingan.

Mengevaluasi kerentanan teknis
Untuk mengevaluasi kerentanan teknis yang teridentifikasi, panduan berikut sebaiknya dipertimbangkan:
a) menganalisis dan memverifikasi laporan untuk menentukan aktivitas respons dan remediasi apa yang diperlukan;
b) setelah potensi kerentanan teknis telah diidentifikasi, organisasi sebaiknya mengidentifikasi risiko terkait dan tindakan yang diambil. Tindakan tersebut dapat melibatkan pembaruan sistem atau menerapkan kontrol lain.

Mengambil langkah-langkah yang tepat untuk mengatasi kerentanan teknis
Proses manajemen pembaruan perangkat lunak sebaiknya diimplementasikan untuk memastikan tambalan dan pembaruan aplikasi yang paling mutakhir diinstal untuk semua perangkat lunak terotorisasi. Jika perubahan diperlukan, perangkat lunak asli sebaiknya dipertahankan dan perubahan diterapkan pada salinan yang ditentukan. Semua perubahan sebaiknya sepenuhnya diuji dan didokumentasikan, sehingga dapat diterapkan kembali, jika perlu, untuk peningkatan perangkat lunak di masa depan. Jika diperlukan, modifikasi sebaiknya diuji dan divalidasi oleh organisasi evaluasi independen.

Untuk mengatasi kerentanan teknis, panduan berikut sebaiknya dipertimbangkan:
a) mengambil tindakan yang sesuai dan tepat waktu dalam merespons identifikasi potensi kerentanan teknis; mendefinisikan garis waktu untuk merespons notifikasi kerentanan teknis yang berpotensi relevan;
b) tergantung pada seberapa mendesak kerentanan teknis perlu ditangani, perlu dilakukan tindakan sesuai dengan kontrol yang terkait dengan manajemen perubahan (lihat 8.32) atau dengan mengikuti prosedur respons insiden keamanan informasi (lihat 5.26);
c) hanya menggunakan pembaruan dari sumber yang terlegitimasi (baik dari internal maupun eksternal organisasi);
d) menguji dan mengevaluasi pembaruan sebelum diinstal untuk memastikannya efektif dan tidak menghasilkan efek samping yang tidak dapat ditoleransi [yaitu jika pembaruan tersedia, menilai risiko yang terkait dengan menginstal pembaruan (risiko yang ditimbulkan oleh kerentanan sebaiknya dibandingkan dengan risiko dari menginstal

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

pembaruan)];
e) menangani sistem yang berisiko tinggi terlebih dahulu;
f) mengembangkan remediasi (biasanya pembaruan perangkat lunak atau tambalan);
g) menguji untuk mengkonfirmasi apakah remediasi atau mitigasi berjalan efektif;
h) menyediakan mekanisme untuk memverifikasi autentisitas remediasi;
i) jika tidak ada pembaruan yang tersedia atau pembaruan tidak dapat diinstal, maka sebaiknya mempertimbangkan kontrol lain, seperti:
   1) menerapkan solusi apa pun yang disarankan oleh vendor perangkat lunak atau sumber lain yang relevan;
   2) mematikan layanan atau kapabilitas yang terkait dengan kerentanan;
   3) mengadaptasi atau menambahkan kontrol akses (misalnya *firewall*) pada perbatasan jaringan (lihat 8.20 hingga 8.22);
   4) memproteksi sistem, perangkat, atau aplikasi yang rentan dari serangan dengan penggelaran filter lalu lintas yang sesuai (kadang-kadang disebut penambalan virtual);
   5) meningkatkan pemonitoran jaringan untuk mendeteksi serangan yang sebenarnya;
   6) meningkatkan kesadaran akan kerentanan.

Untuk perangkat lunak yang telah diperoleh, jika vendor penyedia secara reguler merilis informasi tentang pembaruan keamanan untuk perangkat lunaknya dan menyediakan fasilitas untuk menginstal pembaruan tersebut secara otomatis, maka organisasi sebaiknya memutuskan apakah akan menggunakan pembaruan otomatis atau tidak.

Konsiderasi lain
Log audit sebaiknya disimpan untuk semua langkah yang dilakukan dalam manajemen kerentanan teknis.

Proses manajemen kerentanan teknis sebaiknya dimonitor dan dievaluasi secara reguler untuk memastikan efektivitas dan efisiensinya.
Proses manajemen kerentanan teknis yang efektif sebaiknya diselaraskan dengan aktivitas manajemen insiden, untuk mengomunikasikan data tentang kerentanan terhadap fungsi respons insiden dan memberikan prosedur teknis yang sebaiknya dilakukan jika terjadi insiden.

Jika organisasi menggunakan layanan *cloud* yang disediakan oleh penyedia layanan *cloud* pihak ketiga, manajemen kerentanan teknis dari sumber daya penyedia layanan *cloud* sebaiknya dipastikan oleh penyedia layanan *cloud*. Tanggung jawab penyedia layanan *cloud* untuk manajemen kerentanan teknis sebaiknya menjadi bagian dari perjanjian layanan *cloud* dan sebaiknya mencakup proses untuk melaporkan tindakan penyedia layanan *cloud* yang berkaitan dengan kerentanan teknis (lihat 5.23). Untuk beberapa layanan *cloud*, ada tanggung jawab terpisah untuk penyedia layanan *cloud* dan pelanggan layanan *cloud*. Misalnya, pelanggan layanan *cloud* bertanggung jawab atas manajemen kerentanan asetnya sendiri yang digunakan untuk layanan *cloud*.

Informasi lain
Manajemen kerentanan teknis dapat dilihat sebagai subfungsi manajemen perubahan sehingga dapat memanfaatkan proses dan prosedur manajemen perubahan (lihat 8.32).

Ada kemungkinan bahwa pembaruan tidak mengatasi masalah secara cukup dan memiliki efek samping negatif. Selain itu, dalam beberapa kasus, penghapusan pembaruan tidak dapat dengan mudah dicapai setelah pembaruan diterapkan.

Jika pengujian pembaruan yang cukup tidak dimungkinkan (misalnya karena biaya atau kekurangan sumber daya), penundaan pembaruan dapat dipertimbangkan untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

mengevaluasi risiko terkait, berdasarkan pengalaman yang dilaporkan oleh pengguna lain. Penggunaan ISO/IEC 27031 dapat bermanfaat dalam hal ini.

Ketika terdapat tambalan perangkat lunak atau pembaruan dihasilkan, organisasi dapat mempertimbangkan pemberian proses pembaruan secara otomatis ketika pembaruan tersebut diinstal pada sistem atau produk yang terdampak tanpa perlu intervensi dari pelanggan atau pengguna. Jika proses pembaruan otomatis ditawarkan sebagai opsi, hal tersebut memungkinkan pelanggan atau pengguna untuk memilih opsi untuk mematikan pembaruan otomatis atau mengontrol waktu instalasi pembaruan.

Jika vendor menyediakan proses pembaruan otomatis dan pembaruan dapat diinstal pada sistem atau produk yang terdampak tanpa perlu intervensi, organisasi menentukan apakah akan menerapkan proses otomatis atau tidak. Salah satu alasan untuk tidak memilih pembaruan otomatis adalah untuk mempertahankan kontrol atas kapan pembaruan dilakukan. Misalnya, perangkat lunak yang digunakan untuk operasi bisnis tidak dapat diperbarui sampai operasi selesai.

Kelemahan pemindaian kerentanan yaitu kemungkinan bahwa pemindaian tersebut tidak sepenuhnya memperhitungkan pertahanan berlapis (*in depth*): dua tindakan penanggulangan yang selalu digunakan secara berurutan dapat memiliki kerentanan yang seolah-olah terlihat seperti kekuatan di sisi lain. Tindakan Penanggulangan komposit tidak rentan, sedangkan pemindai kerentanan dapat melaporkan bahwa kedua komponen rentan. Oleh karena itu, organisasi sebaiknya berhati-hati dalam mereviu dan bertindak berdasarkan laporan kerentanan.

Banyak organisasi menyuplai perangkat lunak, sistem, produk, dan layanan tidak hanya dalam organisasi tetapi juga untuk pihak yang berkepentingan seperti pelanggan, mitra, atau pengguna lain. Perangkat lunak, sistem, produk, dan layanan ini mungkin memiliki kerentanan keamanan informasi yang memengaruhi keamanan pengguna.

Organisasi dapat merilis remediasi dan mengungkapkan informasi tentang kerentanan kepada pengguna (biasanya melalui advis publik) dan memberikan informasi yang tepat untuk layanan pangkalan data kerentanan perangkat lunak.

Untuk informasi lebih lanjut yang berkaitan dengan manajemen kerentanan teknis saat menggunakan komputasi awan, lihat seri ISO/IEC 19086 dan ISO/IEC 27017.

ISO/IEC 29147 memberikan informasi detail tentang menerima laporan kerentanan dan menerbitkan solusi kerentanan. ISO/IEC 30111 memberikan informasi detail tentang penanganan dan penyelesaian kerentanan yang dilaporkan.

8.9 Manajemen konfigurasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Konfigurasi_yang_aman	#Proteksi

Kontrol
Konfigurasi, termasuk konfigurasi keamanan, perangkat keras, perangkat lunak, layanan, dan jaringan sebaiknya ditetapkan, didokumentasikan, diimplementasikan, dimonitor, dan direviu.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk memastikan perangkat keras, perangkat lunak, layanan, dan jaringan berfungsi dengan benar sesuai dengan pengaturan keamanan yang dipersyaratkan, dan konfigurasi tidak diubah secara takterotorisasi atau salah.

Panduan
Umum
Organisasi sebaiknya mendefinisikan dan mengimplementasikan proses dan alat untuk menegakkan konfigurasi yang telah didefinisikan (termasuk konfigurasi keamanan) untuk perangkat keras, perangkat lunak, layanan (misalnya layanan *cloud*), dan jaringan, baik untuk sistem yang baru diinstal maupun untuk sistem yang sedang operasional selama masa pakainya.

sebaiknya ada peran, tanggung jawab, dan prosedur untuk memastikan kontrol yang memuaskan dari semua perubahan konfigurasi.

Templat standar
Templat standar untuk konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang aman sebaiknya didefinisikan:
a) menggunakan panduan yang tersedia untuk umum (misalnya templat yang telah didefinisikan sebelumnya dari vendor dan dari organisasi keamanan independen);
b) mempertimbangkan level proteksi yang dibutuhkan untuk menentukan level keamanan yang memadai;
c) mendukung kebijakan keamanan informasi organisasi, kebijakan topik spesifik standar, dan persyaratan keamanan lainnya;
d) mempertimbangkan kelayakan dan kemungkinan penerapan konfigurasi keamanan dalam konteks organisasi.

Templat sebaiknya direviu secara periodik dan diperbarui ketika muncul ancaman atau kerentanan baru perlu ditangani, atau ketika perangkat lunak atau versi perangkat keras baru diperkenalkan.
Hal-hal berikut sebaiknya dipertimbangkan dalam menetapkan templat standar untuk konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang aman:
a) meminimalkan jumlah identitas dengan hak akses level privileses atau administrator;
b) menonaktifkan identitas yang tidak perlu, tidak digunakan, atau tidak aman;
c) menonaktifkan atau membatasi fungsi dan layanan yang tidak perlu;
d) membatasi akses ke program utilitas yang kuat dan pengaturan parameter hos;
e) menyinkronkan jam;
f) mengubah informasi autentikasi bawaan vendor seperti kata sandi bawaan segera setelah instalasi dan mereviu parameter terkait keamanan bawaan penting lainnya;
g) memohon fasilitas *time-out* yang secara otomatis membuat log keluar peranti komputasi setelah periode yang telah ditentukan tidak aktif;
h) memverifikasi bahwa persyaratan lisensi telah dipenuhi (lihat 5.32).

Memanajemeni konfigurasi
Konfigurasi perangkat keras, perangkat lunak, layanan, dan jaringan yang telah ditetapkan, sebaiknya direkam dan log sebaiknya dipelihara dari semua perubahan konfigurasi. Rekaman ini sebaiknya disimpan dengan aman. Ini dapat dicapai dengan beragam cara, seperti pangkalan data konfigurasi atau templat konfigurasi.

Perubahan pada konfigurasi sebaiknya mengikuti proses manajemen perubahan (lihat 8.32).
Catatan konfigurasi dapat berisi:
a) pemilik terbaru atau kontak informasi tentang aset;
b) tanggal perubahan konfigurasi terakhir;
c) versi templat konfigurasi;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) terkait dengan konfigurasi aset lainnya.

Konfigurasi pemonitoran
Konfigurasi sebaiknya dimonitor dengan seperangkat alat manajemen sistem yang komprehensif (misalnya utilitas pemeliharaan, dukungan akses jarak jauh, alat manajemen perusahaan, perangkat lunak cadangan dan pemulihan), dan sebaiknya direviu secara reguler untuk memverifikasi pengaturan konfigurasi, mengevaluasi kekuatan kata sandi serta menilai aktivitas yang dilakukan. Konfigurasi aktual dapat dibandingkan dengan templat target yang didefinisikan. Setiap deviasi sebaiknya ditangani, baik dengan penerapan otomatis target konfigurasi yang didefinisikan atau dengan analisis manual dari deviasi diikuti dengan tindakan korektif.

Informasi lain
Dokumentasi untuk sistem seringkali merekam detail tentang konfigurasi perangkat keras dan perangkat lunak.

Penguatan (*hardening*) sistem adalah bagian tipikal dari manajemen konfigurasi.

Manajemen konfigurasi dapat diintegrasikan dengan proses manajemen aset dan peralatan terkait.

Otomatisasi biasanya lebih efektif untuk memanajemeni konfigurasi keamanan (misalnya menggunakan infrastruktur sebagai kode)

Templat dan target konfigurasi dapat menjadi informasi konfidensial dan sebaiknya diproteksi dari akses yang takterotorisasi.

8.10 Penghapusan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Proteksi_informasi #Legal_dan_kepatuhan	#Proteksi

Kontrol
Informasi yang disimpan dalam sistem informasi, peranti atau di media penyimpanan lainnya sebaiknya dihapus bila tidak lagi diperlukan.

Tujuan
Untuk mencegah eksposur informasi sensitif yang tidak perlu dan untuk mematuhi persyaratan legal, statutori, regalutori, dan kontraktual dalam rangka penghapusan informasi.

Panduan
Umum
Informasi sensitif tidak boleh disimpan lebih lama dari yang diperlukan untuk mengurangi risiko pengungkapan yang takdiinginkan.
Saat menghapus informasi pada sistem, aplikasi, dan layanan, hal-hal berikut sebaiknya dipertimbangkan:
a) memilih metode penghapusan (misalnya menimpa secara elektronik atau menghapus secara kriptografi) yang sesuai dengan persyaratan bisnis dan dengan kondsiderasi hukum dan regulasi yang relevan;
b) menrekam hasil penghapusan sebagai bukti;
c) saat menggunakan penyedia layanan penghapusan informasi, memperoleh bukti penghapusan informasi dari mereka.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Jika pihak ketiga menyimpan informasi organisasi atas namanya, organisasi tersebut sebaiknya mempertimbangkan agar dimasukkan persyaratan tentang penghapusan informasi ke dalam perjanjian agar pihak ketiga menerapkannya selama dan setelah terminasi layanan tersebut.

Metode penghapusan

Sesuai dengan kebijakan topik spesifik organisasi tentang retensi data dan dengan konsiderasi legislasi dan regulasi yang relevan, informasi sensitif sebaiknya dihapus bila tidak lagi diperlukan, dengan :

a) mengonfigurasi sistem untuk menghancurkan informasi dengan aman bila tidak lagi diperlukan (misalnya setelah periode yang definisikan sesuai dengan kebijakan topik spesifik tentang retensi data atau dengan permintaan akses subjek);
b) menghapus versi usang, salinan dan fail temporer di mana pun fail tersebut berada;
c) menggunakan perangkat lunak penghapusan yang disetujui dan aman untuk menghapus informasi secara permanen untuk membantu memastikan informasi tidak dapat dipulihkan dengan menggunakan pemulihan spesialis atau alat forensik;
d) menggunakan penyedia layanan pembuangan yang aman, bersertifikat, dan disetujui;
e) menggunakan mekanisme pembuangan yang sesuai untuk tipe media penyimpanan yang dibuang (misalnya melakukan *degaussing hard disk drive* dan media penyimpanan magnetik lainnya).

Jika layanan *cloud* digunakan, organisasi sebaiknya memverifikasi apakah metode penghapusan yang disediakan oleh penyedia layanan *cloud* akseptabel, dan jika demikian, organisasi sebaiknya menggunakannya, atau meminta penyedia layanan *cloud* menghapus informasi tersebut. Proses penghapusan ini sebaiknya diotomatisasi sesuai dengan kebijakan topik spesifik, jika tersedia dan berlaku. Bergantung pada sensitivitas informasi yang dihapus, log dapat melacak atau memverifikasi bahwa proses penghapusan tersebut telah terjadi.

Untuk menghindari pemajanan informasi sensitif yang takdisengaja ketika peralatan dikirim kembali ke vendor, informasi sensitif sebaiknya diproteksi dengan memindahkan peranti penyimpanan tambahan (misalnya *hard disk drive*) dan memori sebelum peralatan meninggalkan premis organisasi.

Dengan mempertimbangkan bahwa penghapusan yang aman dari beberapa peranti (misalnya ponsel pintar) hanya dapat dicapai melalui destruksi atau menggunakan fungsi yang tertanam dalam peranti ini (misalnya "mengembalikan pengaturan pabrik"), organisasi sebaiknya memilih metode yang tepat sesuai dengan klasifikasi informasi yang ditangani oleh peranti tersebut.

Langkah-langkah kontrol yang dijelaskan dalam 7.14 sebaiknya diterapkan untuk menghancurkan peranti penyimpanan secara fisik dan secara simultan menghapus informasi yang terdapat didalamnya.

Catatan resmi penghapusan informasi akan berguna ketika menganalisis kemungkinan penyebab peristiwa kebocoran informasi.

Informasi lain

Informasi tentang penghapusan data pengguna dalam layanan *cloud* dapat ditemukan di ISO/IEC 27017.

Informasi tentang penghapusan PII dapat ditemukan dalam ISO/IEC 27555.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.11 Penyamaran (*masking*) data

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas	#Memproteksi	#Proteksi_informasi	#Proteksi

Kontrol
Penyamaran data sebaiknya digunakan sesuai dengan kebijakan topik spesifik organisasi tentang kontrol akses dan kebijakan topik spesifik terkait lainnya, serta persyaratan bisnis, konsiderasi legislasi yang berlaku.

Tujuan
Untuk membatasi pemajanan data sensitif, termasuk PII, dan untuk mematuhi persyaratan legal, statutori, regulatori, dan kontraktual.

Panduan
Ketika proteksi data sensitif (misalnya PII) menjadi perhatian, organisasi sebaiknya mempertimbangkan untuk menyembunyikan data tersebut dengan menggunakan teknik seperti penyamaran data, pseudonimisasi, atau anonimisasi.

Teknik pseudonimisasi atau anonimisasi dapat menyembunyikan PII, menyamarkan identitas sebenarnya dari PII *principal* atau informasi sensitif lainnya, dan memutuskan hubungan antara PII dan identitas PII *principal* atau hubungan antara informasi sensitif lainnya.

Saat menggunakan teknik pseudonimisasi atau anonimisasi, sebaiknya diverifikasi bahwa data telah cukup terpseudonimkan atau teranonimkan. Anonimisasi data sebaiknya mempertimbangkan semua elemen informasi sensitif agar efektif. Sebagai contoh, jika tidak dipertimbangkan dengan benar, seseorang dapat diidentifikasi bahkan jika data yang dapat secara langsung mengidentifikasi orang tersebut dianonimkan, dengan adanya data lebih lanjut yang memungkinkan orang tersebut diidentifikasi secara tidak langsung.

Teknik tambahan untuk penyamaran data meliputi:
a) enkripsi (mensyaratkan pengguna yang terotorisasasi untuk memiliki kunci);
b) membatalkan atau menghapus karakter (mencegah pengguna yang takterotorisasi dapat melihat pesan lengkap);
c) meragamkan angka dan tanggal;
d) substitusi (mengganti satu nilai dengan yang lain untuk menyembunyikan data sensitif);
e) mengganti nilai dengan *hash*-nya.

Hal berikut ini sebaiknya dipertimbangkan saat mengimplementasikan teknik penyamaran data:
a) tidak memberikan semua pengguna akses ke semua data, oleh karena itu perlu mendesain kueri dan samaran untuk hanya menampilkan data minimum yang diperlukan kepada pengguna;
b) ada kasus ketika beberapa data tidak boleh terlihat oleh pengguna untuk beberapa rekaman dari satu set data; dalam hal ini, mendesain dan mengimplementasikan mekanisme untuk mengaburkan data (misalnya jika pasien tidak ingin staf rumah sakit dapat melihat semua catatannya bahkan dalam keadaan darurat, maka staf rumah sakit diberi data yang sebagian dikaburkan dan data hanya dapat diakses oleh staf dengan peran spesifik jika berisi informasi yang berguna untuk perawatan medis yang sesuai);
c) ketika data dikaburkan, PII *principal* diberi kemungkinan untuk mensyaratkan pengguna tidak dapat melihat apakah data dikaburkan (mengaburkan pengaburan; ini digunakan di fasilitas kesehatan, sebagai contoh jika pasien tidak ingin staf rumah sakit melihat informasi sensitif seperti kehamilan atau hasil pemeriksaan darah telah dikaburkan);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) persyaratan legal atau regulatori apa pun (misalnya mensyaratkan penyamaran informasi kartu pembayaran selama pemrosesan atau penyimpanan).

Berikut ini sebaiknya dipertimbangkan saat menggunakan penyamaran data, pseudonimisasi, atau anonimisasi:
a) level kekuatan penyamaran data, pseudonimisasi, atau anonimisasi sesuai dengan penggunaan data yang diproses;
b) kontrol akses ke data yang diproses;
c) perjanjian atau pembatasan penggunaan data yang diproses;
d) melarang penyusunan data yang diproses dengan informasi lain sehingga dapat mengidentifikasi PII *principal*;
e) melacak penyediaan dan penerimaan data yang diproses.

Informasi lain
Anonimisasi secara takreversibel mengubah PII sedemikian rupa sehingga PII *principal* tidak dapat lagi diidentifikasi secara langsung atau tidak langsung.

Pseudonimisasi menggantikan informasi identifikasi dengan alias. Pengetahuan tentang algoritme (kadang-kadang disebut sebagai "informasi tambahan") yang digunakan untuk melakukan pseudonimisasi memungkinkan setidaknya beberapa bentuk identifikasi PII *principal*. Oleh karena itu, "informasi tambahan" semacam itu sebaiknya dipisahkan dan diproteksi.

Walaupun pseudonimisasi lebih lemah daripada anonimisasi, *dataset* terpseudonimkan dapat lebih berguna dalam penelitian statistik.

Penyamaran data adalah seperangkat teknik untuk menyembunyikan, mengganti, atau mengaburkan item data yang sensitif. Penyamaran data dapat bersifat statis (ketika item data disamarkan dalam pangkalan data asli), dinamis (menggunakan otomatisasi dan aturan untuk mengamankan data secara waktu-nyata), atau *on-the-fly* (dengan data tersamarkan dalam memori aplikasi).

Fungsi *hash* dapat digunakan untuk menganonimkan PII. Untuk mencegah serangan enumerasi, fungsi *hash* sebaiknya selalu dikombinasikan dengan *salt*.

PII dalam pengidentifikasi sumber daya dan atributnya [misalnya nama fail, *uniform resource locator* (URL)] sebaiknya dihindari atau dianonimkan dengan tepat.

Kontrol tambahan mengenai proteksi PII di *cloud* publik tersedia dalam ISO/IEC 27018.

Informasi tambahan tentang teknik *de-identification* tersedia dalam ISO / IEC 20889.

8.12 Pencegahan kebocoran data

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas	#Memproteksi #Mendeteksi	#Proteksi_informasi	#Proteksi #Pertahanan

Kontrol
Langkah-langkah pencegahan kebocoran data sebaiknya diterapkan pada sistem, jaringan, dan peranti lain yang memproses, menyimpan, atau mentransmisikan informasi sensitif.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tujuan
Untuk mendeteksi dan mencegah pengungkapan dan ekstraksi informasi yang takterotorisasi oleh individu atau sistem.

Panduan
Organisasi sebaiknya mempertimbangkan hal-hal berikut untuk mengurangi risiko kebocoran data:
a) mengidentifikasi dan mengklasifikasi informasi untuk memproteksi kebocoran (misalnya informasi personal, model penetapan harga, dan desain produk);
b) memonitor saluran kebocoran data (misalnya surel, transfer fail, peranti mobil (*mobile*), dan peranti penyimpanan portabel);
c) bertindak untuk mencegah informasi bocor (misalnya mengarantina surel yang berisi informasi sensitif).

Alat pencegahan kebocoran data sebaiknya digunakan untuk:
a) mengidentifikasi dan memonitor informasi sensitif yang memiliki risiko pengungkapan yang takterotorisasi (misalnya dalam data tidak terstruktur pada sistem pengguna);
b) mendeteksi pengungkapan informasi sensitif (misalnya ketika informasi diunggah ke layanan *cloud* pihak ketiga yang taktepercaya atau dikirim melalui surel);
c) memblokir tindakan pengguna atau transmisi jaringan yang mengekspos informasi sensitif (misalnya mencegah penyalinan entri pangkalan data ke dalam *spreadsheet*).

Organisasi sebaiknya menentukan apakah perlu untuk membatasi kemampuan pengguna untuk menyalin dan menempelkan atau mengunggah data ke layanan, perangkat, dan media penyimpanan di luar organisasi. Jika demikian, organisasi sebaiknya mengimplementasikan teknologi seperti alat pencegahan kebocoran data atau konfigurasi alat yang ada yang memungkinkan pengguna untuk melihat dan memanipulasi data yang disimpan secara jarak jauh tetapi mencegah menyalin dan menempelkan di luar kontrol organisasi.

Jika diperlukan ekspor data, pemilik data sebaiknya diizinkan untuk menyetujui pengiriman dan meminta akuntabel pengguna atas tindakannya.

Pengambilan tangkapan layar atau foto layar sebaiknya ditangani melalui syarat dan ketentuan penggunaan, pelatihan, dan audit.

Jika data dicadangkan, organisasi sebaiknya berhati-hati untuk memastikan informasi sensitif diproteksi menggunakan langkah-langkah seperti enkripsi, kontrol akses, dan proteksi fisik media penyimpanan yang menyimpan cadangan.

Pencegahan kebocoran data juga sebaiknya dipertimbangkan untuk memproteksi terhadap tindakan intelijen musuh dari memperoleh informasi konfidensial atau rahasia (geopolitik, manusia, finansial, komersial, saintifik, atau lainnya) yang dapat menarik bagi spionase atau dapat menjadi kritis bagi masyarakat

Tindakan pencegahan kebocoran data sebaiknya berorientasi untuk membingungkan keputusan musuh sebagai contoh dengan mengganti informasi autentik dengan informasi palsu, baik sebagai tindakan yang independen maupun sebagai respons terhadap tindakan intelijen musuh. Contoh dari tindakan semacam ini adalah rekayasa sosial terbalik atau penggunaan *honeypot* untuk menarik penyerang.

Informasi lain
Alat pencegahan kebocoran data didesain untuk mengidentifikasi data, memonitor penggunaan dan pergerakan data, dan mengambil tindakan untuk mencegah kebocoran data (misalnya memperingatkan pengguna tentang perilakunya yang berisiko dan memblokir transfer data ke peranti penyimpanan portabel).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pencegahan kebocoran data secara inheren melibatkan pemonitoran komunikasi dan aktivitas daring personel, dan dengan ekstensi pesan pihak eksternal, yang menimbulkan masalah legal yang sebaiknya dipertimbangkan sebelum memasang alat pencegahan kebocoran data. Ada berbagai legalisasi yang berkaitan dengan privasi, proteksi data, ketenagakerjaan, intersepsi data, dan telekomunikasi yang berlaku untuk pemonitoran dan pemrosesan data dalam konteks pencegahan kebocoran data.

Pencegahan kebocoran data dapat didukung oleh kontrol keamanan standar, seperti kebijakan topik spesifik tentang kontrol akses dan manajemen dokumen yang aman (lihat 5.12 dan 5.15).

8.13 Pencadangan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Korektif	#Integritas #Availabilitas	#Memulihkan	#Kontinuitas	#Proteksi

Kontrol
Salinan cadangan informasi, perangkat lunak, dan sistem sebaiknya dipelihara dan diuji secara reguler sesuai dengan kebijakan topik spesifik yang disepakati tentang pencadangan.

Tujuan
Untuk memungkinkan pemulihan dari kehilangan data atau sistem.

Panduan
Kebijakan topik spesifik tentang pencadangan sebaiknya ditetapkan untuk mengatasi persyaratan penyimpanan data dan keamanan informasi organisasi.

Fasilitas pencadangan yang cukup sebaiknya disediakan untuk memastikan bahwa semua informasi dan perangkat lunak esensial dapat dipulihkan setelah insiden atau kegagalan atau hilangnya media penyimpanan.

Rencana sebaiknya dikembangkan dan diimplementasikan tentang cara organisasi akan mencadangkan informasi, perangkat lunak, dan sistem, dalam rangka memenuhi kebijakan topik spesifik tentang pencadangan.

Saat mendesain rencana pencadangan, hal berikut sebaiknya menjadi konsiderasi:

a) menghasilkan rekaman yang akurat dan lengkap dari salinan cadangan dan prosedur restorasi terdokumentasi;
b) merefleksikan persyaratan bisnis organisasi (misalnya sasaran titik pemulihan, lihat 5.30), persyaratan keamanan informasi yang terlibat dan kekritisan informasi terhadap keberlanjutan operasi organisasi (misalnya pencadangan penuh atau diferensial) dan frekuensi pencadangan;
c) menyimpan cadangan di lokasi yang aman dan terjamin, dengan jarak yang cukup untuk menghindari kerusakan dari bencana di lokasi utama;
d) memberikan level proteksi fisik dan lingkungan yang tepat untuk informasi cadangan (lihat Pasal 7 dan 8.1) sesuai dengan standar yang diterapkan di lokasi utama;
e) Secara reguler menguji media cadangan untuk memastikan bahwa media tersebut dapat diandalkan untuk penggunaan darurat bila diperlukan. Menguji kemampuan untuk mengembalikan data yang dicadangkan ke sistem pengujian, bukan dengan menimpa media penyimpanan asli jika proses pencadangan atau restorasi gagal dan menyebabkan kerusakan atau kehilangan data yang tidak dapat diperbaiki;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

f) memproteksi cadangan melalui enkripsi sesuai dengan risiko yang teridentifikasi (misalnya dalam situasi ketika konfidensialitas sangat penting);
g) berhati-hati untuk memastikan bahwa kehilangan data yang tidak disengaja terdeteksi sebelum dilakukan pencadangan.

Prosedur operasional sebaiknya memonitor eksekusi pencadangan dan mengatasi kegagalan pencadangan terjadwal, untuk memastikan kelengkapan cadangan sesuai dengan kebijakan topik spesifik tentang pencadangan.

Langkah-langkah pencadangan untuk sistem dan layanan individual sebaiknya diuji secara reguler untuk memastikan bahwa langkah-langkah tersebut memenuhi sasaran respons insiden dan rencana kontinuitas bisnis (lihat 5.30). Langkah-langkah Ini sebaiknya dikombinasikan dengan uji prosedur restorasi dan diperiksa terhadap waktu restorasi yang dipersyaratkan oleh rencana kontinuitas bisnis. Dalam hal sistem dan layanan kritis, langkah-langkah pencadangan sebaiknya mencakup semua informasi sistem, aplikasi, dan data yang diperlukan untuk memulihkan sistem lengkap jika terjadi bencana.

Ketika organisasi menggunakan layanan *cloud*, salinan cadangan informasi, aplikasi, dan sistem organisasi di lingkungan layanan *cloud* sebaiknya diambil. Organisasi sebaiknya menentukan kapan dan bagaimana persyaratan untuk pencadangan terpenuhi saat menggunakan layanan cadangan informasi yang disediakan sebagai bagian dari layanan *cloud*.

Periode retensi untuk informasi bisnis esesnsial sebaiknya ditentukan dengan memperhitungkan persyaratan untuk retensi salinan arsip. Organisasi sebaiknya mempertimbangkan penghapusan informasi (lihat 8.10) di media penyimpanan yang digunakan untuk pencadangan setelah periode retensi informasi berakhir dan sebaiknya mengambil konsiderasi legislasi dan regulasi.

Informasi lain
Untuk informasi lebih lanjut tentang keamanan penyimpanan termasuk konsiderasi retensi, lihat ISO/IEC 27040.

8.14 Redundansi fasilitas pemrosesan informasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Availabilitas	#Memproteksi	#Kontinuitas #Manajemen_aset	#Proteksi #Resiliensi

Kontrol
Fasilitas pemrosesan informasi sebaiknya diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan availabilitas.

Tujuan
Untuk memastikan pengoperasian fasilitas pengolahan informasi yang berkelanjutan.

Panduan
Organisasi sebaiknya mengidentifikasi persyaratan untuk availabilitas layanan bisnis dan sistem informasi. Organisasi sebaiknya mendesain dan mengimplementasikan arsitektur sistem dengan redundansi yang sesuai untuk memenuhi persyaratan ini.

Redundansi dapat dilakukan dengan menduplikasi fasilitas pemrosesan informasi sebagian atau secara keseluruhan (yaitu komponen cadangan atau memiliki semua komponen

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

sebanyak 2 rangkap). Organisasi sebaiknya merencanakan dan mengimplementasikan prosedur untuk aktivasi komponen dan fasilitas pemrosesan redundan. Prosedur tersebut sebaiknya menentukan apakah komponen dan aktivitas redundan selalu diaktifkan, atau dalam keadaan darurat, diaktifkan secara otomatis atau manual. Komponen dan fasilitas pemrosesan informasi redundan sebaiknya dipastikan memiliki level keamanan yang sama dengan yang utama.

Sebaiknya ada mekanisme untuk mengingatkan organisasi tentang kegagalan dalam fasilitas pemrosesan informasi, memungkinkan pengeksekusian prosedur terencana, dan memungkinkan availabilitas berkelanjutan sementara fasilitas pemrosesan informasi diperbaiki atau diganti.

Organisasi sebaiknya mempertimbangkan hal-hal berikut ketika mengimplementasikan sistem redundan:

a) kontrak dengan dua atau lebih pemasok jaringan dan fasilitas pemrosesan informasi kritis seperti penyedia layanan internet;
b) menggunakan jaringan redundan;
c) menggunakan dua pusat data yang terpisah secara geografis dengan sistem pencadangan data *mirrored*;
d) menggunakan catu daya atau sumber daya redundan secara fisik;
e) menggunakan beberapa bagian paralel komponen perangkat lunak, dengan penyeimbangan beban otomatis di antaranya (antara bagian di pusat data yang sama atau di pusat data yang berbeda);
f) memiliki komponen terduplikat dalam sistem (misalnya CPU, *hard disk*, memori) atau dalam jaringan (misalnya *firewall,* ruter*, switch*).

Jika dapat diterapkan, lebih disukai dalam mode produksi, sistem informasi redundan sebaiknya diuji untuk memastikan *failover* dari satu komponen ke komponen lain berfungsi sesuai tujuan.

Informasi lain

Ada hubungan yang kuat antara redundansi dan kesiapan TIK untuk kontinuitas bisnis (lihat 5.30) terutama jika waktu pemulihan yang singkat diperlukan. Banyak langkah redundansi dapat menjadi bagian dari strategi dan solusi kontinuitas TIK.

Implementasi redundansi dapat menimbulkan risiko terhadap integritas (misalnya proses menyalin data ke komponen duplikat dapat menimbulkan galat) atau konfidensialitas (misalnya kontrol keamanan yang lemah terhadap komponen duplikat dapat menyebabkan pembobolan) informasi dan sistem informasi, yang perlu dipertimbangkan ketika mendesain sistem informasi.

Redundansi dalam fasilitas pemrosesan informasi biasanya tidak mengatasi ketidaktersediaan aplikasi karena kesalahan dalam aplikasi.

Dengan menggunakan komputasi awan publik, dimungkinkan untuk memiliki beberapa versi langsung dari fasilitas pemrosesan informasi, yang ada di beberapa lokasi fisik terpisah dengan *failover* otomatis dan penyeimbangan beban di antaranya.

Beberapa teknologi dan teknik untuk menyediakan redundansi dan *fail-over* otomatis dalam konteks layanan *cloud* dibahas dalam ISO/IEC TS 23167.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.15 Membuat log

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi	#Manajemen_peristiwa_keamanan_informasi	#Proteksi #Pertahanan

Kontrol
Log yang merekam aktivitas, eksepsi, kesalahan, dan peristiwa relevan lainnya sebaiknya diproduksi, disimpan, diproteksi, dan dianalisis.

Tujuan
Untuk merekam peristiwa, menghasilkan bukti, memastikan integritas dari informasi log, mencegah akses yang takterotorisasi, mengidentifikasi peristiwa keamanan informasi yang dapat menyebabkan insiden keamanan informasi, dan untuk mendukung investigasi.

Panduan
Umum
Organisasi sebaiknya menentukan tujuan pembuatan log tertentu, data apa yang dikumpulkan dan dilakukan log, dan persyaratan log spesifik lainnya untuk memproteksi dan menangani data log. Ini sebaiknya didokumentasikan dalam kebijakan topik spesifik tentang log.

Log peristiwa sebaiknya disertakan untuk setiap peristiwa, sebagaimana dapat berlaku:
a) *ID* pengguna;
b) aktivitas sistem
c) tanggal, waktu, dan detail peristiwa yang relevan (misalnya masuk dan keluar);
d) identitas perangkat, pengenal sistem, dan lokasi;
e) alamat jaringan dan protokol yang digunakan.

Peristiwa berikut sebaiknya dipertimbangkan untuk membuat log:
a) upaya mengakses sistem, baik yang berhasil maupun yang ditolak;
b) data serta upaya mengakses sumber daya lainnya, baik yang berhasil maupun yang ditolak;
c) perubahan pada konfigurasi sistem;
d) penggunaan privilese;
e) penggunaan program utilitas dan aplikasi;
f) fail yang diakses dan tipe akses, termasuk penghapusan fail data penting;
g) alarm yang dipicu oleh sistem kontrol akses;
h) aktivasi dan deaktivasi sistem keamanan, seperti sistem antivirus dan sistem deteksi intrusi;
i) pembuatan, modifikasi, atau penghapusan identitas;
j) transaksi yang dieksekusi oleh pengguna dalam aplikasi. Dalam beberapa kasus, aplikasi merupakan layanan atau produk yang disediakan atau dijalankan oleh pihak ketiga.

Penting bagi semua sistem untuk memiliki sumber waktu yang disinkronkan (lihat 8.17) karena ini memungkinkan korelasi log antarsistem untuk analisis, peringatan, dan investigasi suatu insiden.

Proteksi log
Pengguna, termasuk mereka yang memiliki hak akses privilese, sebaiknya tidak memiliki izin untuk menghapus atau mendeaktivasi log aktivitasnya sendiri. Mereka berpotensi memanipulasi log pada fasilitas pemrosesan informasi di bawah kontrolnya langsung. Oleh

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

karena itu, perlu untuk memproteksi dan mereviu log untuk memelihara akuntabilitas bagi pengguna privilese.

Kontrol sebaiknya bertujuan untuk memproteksi informasi log terhadap perubahan yang takterotorisasi dan problem operasional dengan fasilitas pembuatan log termasuk antara lain:
a) alterasi pada tipe pesan yang direkam
b) fail log yang diedit atau dihapus;
c) kegagalan untuk merekam peristiwa atau menimpa peristiwa yang direkam sebelumnya jika media penyimpanan yang terdapat fail log di dalamnya telah penuh.

Untuk proteksi log, penggunaan teknik berikut sebaiknya dipertimbangkan: *hashing* kriptografis, perekaman dalam fail yang hanya dapat dilampirkan dan dibaca (*read-only*), merekam dalam fail transparansi publik.

Beberapa log audit dapat dipersyaratkan untuk diarsipkan karena persyaratan tentang retensi data atau persyaratan untuk mengumpulkan dan menyimpan bukti (lihat 5.28).

Jika organisasi perlu mengirim log sistem atau aplikasi ke vendor untuk membantu dalam hal kesalahan *debugging* atau *troubleshooting*, log sebaiknya dihilangkan identitasnya jika memungkinkan menggunakan teknik penyamaran data (lihat 8.11) untuk informasi seperti nama pengguna, alamat *internet protocol* (IP), nama hos, atau nama organisasi, sebelum dikirim ke vendor.

Log peristiwa dapat berisi data sensitif dan informasi pengidentifikasi diri. Langkah-langkah proteksi privasi yang tepat sebaiknya diambil (lihat 5.34).

Analisis log

Analisis log sebaiknya mencakup analisis dan interpretasi peristiwa keamanan informasi, untuk membantu mengidentifikasi aktivitas yang tidak biasa atau perilaku anomali, yang dapat menunjukkan indikator pembobolan.

Analisis peristiwa sebaiknya dilakukan dengan memperhitungkan:
a) keterampilan yang diperlukan bagi para ahli yang melakukan analisis;
b) menentukan prosedur analisis log;
c) atribut yang diperlukan untuk setiap peristiwa terkait keamanan;
d) eksepsi yang diidentifikasi melalui penggunaan aturan yang telah ditentukan [misalnya konfigurasi pada *Security Information and Event Management* SIEM) atau aturan *firewall* dan *intrusion detection system* (IDS) atau tanda tangan perangkat perusak];
e) pola perilaku yang diketahui dan lalu lintas jaringan standar dibandingkan dengan aktivitas dan perilaku anomali [*user and entity behaviour analytics* (UEBA)];
f) hasil analisis tren atau pola (misalnya sebagai akibat dari penggunaan analisis data, teknik *big data*, dan alat analisis khusus);
g) intelijen ancaman yang tersedia.

Analisis log sebaiknya didukung oleh aktivitas pemonitoran khusus untuk membantu mengidentifikasi dan menganalisis perilaku anomali, yang meliputi:
a) mereviu upaya yang berhasil dan gagal untuk mengakses sumber daya yang diproteksi [misalnya server *domain name system* (DNS), portal web, dan berbagi fail];
b) memeriksa log DNS untuk mengidentifikasi koneksi jaringan keluar ke server berbahaya, seperti yang terkait dengan server pengontrol *(command & control) botnet*;
c) memeriksa laporan penggunaan dari penyedia layanan (misalnya faktur atau laporan layanan) untuk menemukan aktivitas yang tidak biasa dalam sistem dan jaringan (misalnya dengan mereviu pola aktivitas);
d) termasuk log peristiwa pemonitoran fisik seperti masuk dan keluar untuk memastikan deteksi dan analisis insiden yang lebih akurat;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

e) mengorelasikan log untuk memungkinkan analisis yang lebih efisien dan sangat akurat.

Insiden keamanan informasi yang dicurigai dan aktual sebaiknya diidentifikasi (misalnya infeksi perangkat perusak atau pemerikasaan *firewall*) dan pada investigasi lebih lanjut (misalnya sebagai bagian dari proses manajemen insiden keamanan informasi, lihat 5.25).

Informasi lain
Log sistem sering kali berisi sejumlah besar informasi, yang sebagian besar asing bagi pemonitoran keamanan informasi. Untuk membantu mengidentifikasi peristiwa signifikan untuk tujuan pemonitoran keamanan informasi, penggunaan program utilitas atau alat audit yang sesuai untuk melakukan interogasi fail dapat dipertimbangkan.

Pemberlakuan log peristiwa *(event logging)* menetapkan fondasi bagi sistem pemonitoran otomatis (lihat 8.16) yang mampu menghasilkan laporan dan peringatan terkonsolidasi tentang keamanan sistem.

Alat SIEM atau layanan serupa dapat digunakan untuk menyimpan, menghubungkan, menormalkan, dan menganalisis informasi log**,** dan menghasilkan peringatan. SIEM cenderung membutuhkan konfigurasi yang cermat untuk mengoptimalkan manfaatnya. Konfigurasi yang perlu dipertimbangkan termasuk identifikasi dan seleksi sumber log yang sesuai, penyetelan dan pengujian aturan dan pengembangan kasus penggunaan.

Fail transparansi publik untuk perekaman log digunakan, sebagai contoh, dalam sistem transparansi sertifikat. Fail semacam itu dapat memberikan mekanisme deteksi tambahan yang berguna untuk menjaga dari gangguan log.

Pada lingkungan *cloud*, tanggung jawab manajemen log dapat dibagi antara pelanggan layanan *cloud* dan penyedia layanan *cloud*. Tanggung jawab tersebut akan beragam tergantung pada tipe layanan *cloud* yang digunakan. Panduan lebih lanjut dapat ditemukan di ISO/TS 22317.

8.16 Pemonitoran aktivitas

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi #Merespons	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Kontrol
Jaringan, sistem, dan aplikasi sebaiknya dimonitor untuk menemukan perilaku anomali dan mengambil tindakan yang tepat untuk mengevaluasi potensi insiden keamanan informasi.

Tujuan
Untuk mendeteksi perilaku anomali dan potensi insiden keamanan informasi.

Panduan
Ruang lingkup dan level pemonitoran sebaiknya ditentukan sesuai dengan persyaratan keamanan informasi dan bisnis serta dengan mengambil konsiderasi hukum dan regulasi yang relevan. Rekaman pemonitoran sebaiknya dipelihara untuk periode retensi yang telah didefinisikan.

Hal-hal berikut ini sebaiknya dipertimbangkan untuk dimasukkan dalam sistem pemonitoran:
a) jaringan keluar dan masuk, lalu lintas sistem dan aplikasi;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) akses ke sistem, server, peralatan jaringan, sistem pemonitoran, aplikasi kritis, dll.;
c) sistem level kritis atau admin dan fail konfigurasi jaringan;
d) log dari alat keamanan [misalnya antivirus, IDS, *intrusion prevention system* (IPS), filter web, *firewall*, pencegahan kebocoran data];
e) log peristiwa yang berkaitan dengan aktivitas sistem dan jaringan;
f) memeriksa bahwa kode yang dieksekusi telah terotorisasi untuk berjalan dalam sistem dan bahwa kode tersebut tidak dirusak (misalnya dengan kompilasi ulang untuk menambahkan kode tambahan yang tidak diinginkan);
g) penggunaan sumber daya (misalnya CPU, *hard disk*, memori, *bandwidth*) dan kinerjanya.

Organisasi sebaiknya menetapkan suatu garis acuan perilaku normal dan memonitor garis acuan ini untuk anomali. Saat menetapkan garis acuan, hal-hal berikut sebaiknya dipertimbangkan:
a) mereviu pemanfaatan sistem pada periode normal dan puncak;
b) waktu akses, lokasi akses, frekuensi akses untuk setiap pengguna atau kelompok pengguna.

Sistem pemonitoran sebaiknya dikonfigurasi terhadap garis acuan yang ditetapkan untuk mengidentifikasi perilaku anomali, seperti:
a) terminasi proses atau aplikasi yang tidak direncanakan;
b) aktivitas yang biasanya terkait dengan perangkat perusak atau lalu lintas yang berasal dari alamat IP atau domain berbahaya yang diketahui (misalnya yang terkait dengan server kontrol dan *command botnet*);
c) karakteristik serangan yang diketahui (misalnya *denial of service* dan *buffer overflows*);
d) perilaku sistem yang tidak biasa (misalnya pemerlakuan log *keystroke*, injeksi proses, dan deviasi dalam penggunaan protokol standar);
e) kemacetan dan kelebihan beban (misalnya antrean jaringan, level latensi, dan *jitter* jaringan);
f) akses takterotorisasi (aktual atau percobaan) ke sistem atau informasi;
g) pemindaian aplikasi bisnis, sistem, dan jaringan yang takterotorisasi;
h) upaya yang berhasil dan tidak berhasil untuk mengakses sumber daya yang diproteksi (misalnya server DNS, portal web, dan sistem fail];
g) perilaku pengguna dan sistem yang tidak biasa dalam kaitannya dengan perilaku yang diharapkan.

Pemonitoran berkelanjutan melalui alat pemonitoran sebaiknya digunakan. Pemonitoran sebaiknya dilakukan secara waktu nyata atau interval periodik, tergantung pada kebutuhan dan kemampuan organisasi. Alat pemonitoran sebaiknya mencakup kemampuan untuk menangani sejumlah besar data, beradaptasi dengan lanskap ancaman yang terus berubah, dan memungkinkan notifikasi waktu nyata. Alat ini juga sebaiknya dapat mengenali tanda tangan spesifik dan data atau pola perilaku jaringan atau aplikasi.

Perangkat lunak pemonitoran otomatis sebaiknya dikonfigurasi untuk menghasilkan peringatan (misalnya melalui konsol manajemen, pesan surel, atau sistem pesan instan) berdasarkan ambang batas yang telah didefinisikan. Sistem peringatan sebaiknya disetel dan dilatih pada garis acuan organisasi untuk meminimalkan *false-positive*. Personel sebaiknya didedikasikan untuk merespons peringatan dan sebaiknya dilatih dengan tepat agar dapat secara akurat menafsirkan potensi insiden. Sebaiknya ada sistem dan proses redundan untuk menerima dan merespons notifikasi.

Peristiwa abnormal sebaiknya dikomunikasikan kepada pihak yang relevan untuk meningkatkan aktivitas berikut: audit, evaluasi keamanan, pemindaian, dan pemonitoran kerentanan (lihat 5.25). Prosedur sebaiknya dilakukan untuk merespons indikator positif dari sistem pemonitoran secara tepat waktu, untuk meminimalkan efek samping peristiwa (lihat

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.26) pada keamanan informasi. Prosedur juga sebaiknya ditetapkan untuk mengidentifikasi dan mengatasi *false-positive* termasuk menyetel perangkat lunak pemonitoran untuk mengurangi jumlah *false-positive* di masa depan.

Informasi lain
Pemonitoran keamanan dapat ditingkatkan dengan:
a) memanfaatkan sistem intelijen ancaman (lihat 5.7);
b) memanfaatkan *machine learning* dan kemampuan kecerdasan artifisial;
c) menggunakan *blacklist* atau *allowlist*;
d) melakukan berbagai asesmen keamanan teknis (misalnya asesmen kerentanan, uji penetrasi, simulasi serangan siber, dan latihan respons siber), serta menggunakan hasil asesmen ini untuk membantu menentukan garis acuan atau perilaku yang akseptabel;
e) menggunakan sistem pemonitoran kinerja untuk membantu membangun dan mendeteksi perilaku anomali;
f) memanfaatkan log yang dikombinasikan dengan sistem pemonitoran.

Aktivitas pemonitoran sering dilakukan dengan menggunakan perangkat lunak khusus, seperti *intrusion detection systems.* Perangkat lunak Ini dapat dikonfigurasi sesuai dengan garis acuan aktivitas sistem dan jaringan yang normal, akseptabel, dan diharapkan.

Pemonitoran untuk komunikasi anomali membantu dalam identifikasi *botnet* (yaitu set peranti di bawah kontrol jahat dari pemilik *botnet*, biasanya digunakan untuk memasang serangan *denial of service* terdistribusi pada komputer organisasi lain). Jika komputer dikontrol oleh peranti eksternal, ada komunikasi antara peranti yang terinfeksi dan pengontrol. Oleh karena itu organisasi sebaiknya menggunakan teknologi untuk memonitor komunikasi anomali dan mengambil tindakan yang diperlukan.

8.17 Sinkronisasi jam

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Detektif	#Integritas	#Memproteksi #Mendeteksi	#Manajemen_peristiwa_keamanan_informasi	#Proteksi #Pertahanan

Kontrol
Jam sistem pemrosesan informasi yang digunakan oleh organisasi sebaiknya disinkronkan ke sumber waktu yang disetujui.

Tujuan
Untuk memungkinkan korelasi dan analisis peristiwa terkait keamanan dan data lain yang direkam, dan untuk mendukung investigasi insiden keamanan informasi.

Panduan
Persyaratan eksternal dan internal untuk representasi, sinkronisasi dan akurasi waktu yang andal sebaiknya didokumentasikan dan diimplementasikan. Persyaratan tersebut dapat berasal dari kebutuhan legal, statutori, regalutori, kontraktual, standar, dan pemonitoran internal. Waktu referensi standar untuk digunakan dalam organisasi sebaiknya didefinisikan dan dipertimbangkan untuk semua sistem, termasuk sistem manajemen bangunan, sistem masuk dan keluar, dan lain-lain yang dapat digunakan untuk membantu investigasi.

Jam yang terhubung ke siaran waktu radio dari jam atom nasional atau *global positioning system* (GPS) sebaiknya digunakan sebagai jam referensi untuk sistem pembuatan log (*logging*); sumber tanggal dan waktu yang konsisten dan tepercaya untuk memastikan penanda waktu (*time-stamp*) yang akurat. Protokol seperti *Network Time Protocol* (NTP) atau

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Precision Time Protocol (PTP) sebaiknya digunakan untuk menjaga semua sistem jaringan tersinkronisasi dengan jam referensi.

Organisasi dapat menggunakan dua sumber waktu eksternal pada saat yang sama untuk meningkatkan reliabilitas jam eksternal, dan memanajemeni varians apa pun dengan tepat.

Sinkronisasi jam mungkin sulit saat menggunakan beberapa layanan *cloud* atau saat menggunakan layanan *cloud* dan layanan *on-premise*. Dalam hal ini, jam setiap layanan sebaiknya dimonitor dan perbedaan direkam untuk memitigasi risiko yang timbul dari perbedaan.

Informasi lain
Pengaturan jam komputer yang benar penting untuk memastikan keakuratan log peristiwa, yang mungkin dipersyaratkan untuk investigasi atau sebagai bukti dalam kasus legal dan disiplin. Log audit yang takakurat dapat menghambat investigasi dan merusak kredibilitas bukti elektronik.

8.18 Penggunaan program utilitas privilese

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan #Konfigurasi_yang_aman #Keamanan_aplikasi	#Proteksi

Kontrol
Penggunaan program utilitas yang mampu membatalkan sistem dan kontrol aplikasi sebaiknya dibatasi dan dikontrol dengan ketat.

Tujuan
Untuk memastikan penggunaan program utilitas tidak membahayakan kontrol sistem dan aplikasi untuk keamanan informasi.

Panduan
Pedoman berikut ini untuk penggunaan program utilitas yang dapat membatalkan sistem dan kontrol aplikasi yang sebaiknya dijadikan konsiderasi:

a) limitasi penggunaan program utilitas hingga jumlah minimum pengguna resmi yang terotorisasi (lihat 8.2);
b) penggunaan prosedur identifikasi, autentikasi, dan otorisasi untuk program utilitas, termasuk identifikasi unik dari orang yang menggunakan program utilitas;
c) mendefinisikan dan mendokumentasikan level otorisasi untuk program utilitas;
d) otorisasi untuk penggunaan program utilitas secara ad hoc;
e) tidak menyediakan program utilitas bagi pengguna yang memiliki akses ke aplikasi pada sistem yang mensyaratkan segregasi tugas;
f) memindahkan atau menonaktifkan semua program utilitas yang tidak diperlukan;
g) minimal, terdapat pemisahan logis program utilitas dari perangkat lunak aplikasi. Jika memungkinkan, memisahkan komunikasi jaringan untuk program tersebut dari lalu lintas aplikasi;
h) limitasi availabilitas program utilitas (misalnya untuk durasi perubahan terotorisasi);
i) membuat log semua penggunaan program utilitas.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Sebagian besar sistem informasi memiliki satu atau lebih program utilitas yang mampu mengesampingkan sistem dan kontrol aplikasi, misalnya diagnostik, penambalan perangkat lunak, antivirus, pengurai diska, *debugger*, cadangan, dan alat jaringan.

8.19 Instalasi perangkat lunak pada sistem operasional

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Konfigurasi_yang_aman #Keamanan_aplikasi	#Proteksi

Kontrol
Prosedur dan langkah-langkah sebaiknya diimplementasikan untuk memanajemeni instalasi perangkat lunak dengan aman pada sistem operasional.

Tujuan
Untuk memastikan integritas sistem operasi dan mencegah eksploitasi kerentanan teknis.

Panduan
Pedoman berikut sebaiknya dipertimbangkan dalam rangka memanajemeni perubahan dan instalasi perangkat lunak secara aman pada sistem operasional:

a) melakukan pembaruan perangkat lunak operasional hanya oleh administrator terlatih atas otorisasi manajemen yang sesuai (lihat 8.5);
b) memastikan bahwa hanya kode yang telah disetujui yang dapat dieksekusi dan tidak ada kode pengembangan atau kompilator yang diinstal pada sistem operasional;
c) hanya menginstal dan memperbarui perangkat lunak setelah pengujian ekstensif yang sukses (lihat 8.29 dan 8.31);
d) memperbaharui semua pustaka sumber program yang sesuai;
e) menggunakan sistem kontrol konfigurasi untuk mengontrol semua perangkat lunak operasi serta dokumentasi sistem;
f) menentukan strategi *rollback* sebelum perubahan diterapkan;
g) memelihara log audit dari semua pembaruan perangkat lunak operasional);
h) mengarsipkan versi lama perangkat lunak, bersama dengan semua informasi dan parameter, prosedur, detail konfigurasi dan perangkat lunak pendukung yang diperlukan sebagai tindakan kontingensi, dan selama perangkat lunak diperlukan untuk membaca atau memproses data yang diarsipkan.

Setiap keputusan untuk meningkatkan ke versi rilis yang baru sebaiknya memperhitungkan persyaratan bisnis untuk perubahan dan keamanan terkait rilis (misalnya introduksi fungsionalitas keamanan informasi baru atau jumlah dan level keparahan kerentanan keamanan informasi yang memengaruhi versi saat ini). Tambalan perangkat lunak sebaiknya diterapkan ketika dapat membantu memindahkan atau mengurangi kerentanan keamanan informasi (lihat 8.8 dan 8.19).

Perangkat lunak komputer dapat mengandalkan perangkat lunak dan paket yang disediakan secara eksternal (misalnya program perangkat lunak menggunakan modul yang di-hos di situs eksternal), yang sebaiknya dimonitor dan dikontrol untuk menghindari perubahan yang takterotorisasi, karena dapat memunculkan kerentanan keamanan informasi.

Perangkat lunak yang disediakan pemasok yang digunakan dalam sistem operasional sebaiknya dipelihara pada level yang didukung oleh pemasok. Seiring waktu, pemasok perangkat lunak akan berhenti mendukung versi perangkat lunak yang lebih lama. Organisasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

sebaiknya mempertimbangkan risiko dari mengandalkan perangkat lunak yang tak terdukung. Perangkat lunak sumber terbuka yang digunakan dalam sistem operasional sebaiknya dipelihara hingga rilis perangkat lunak terbaru yang sesuai. Seiring waktu, kode sumber terbuka dapat berhenti digunakan tetapi masih tersedia dalam repositori perangkat lunak sumber terbuka. Organisasi juga sebaiknya mempertimbangkan risiko dari mengandalkan perangkat lunak sumber terbuka yang tidak berkelanjutan ketika digunakan dalam sistem operasional.

Ketika pemasok terlibat dalam instalasi atau pembaruan perangkat lunak, akses fisik atau logis hanya boleh diberikan bila diperlukan dan dengan otorisasi yang sesuai. Aktivitas pemasok sebaiknya dimonitor (lihat 5.22).

Organisasi sebaiknya mendefinisikan dan menegakkan aturan ketat tentang tipe perangkat lunak yang dapat diinstal pengguna.

Prinsip privilese terendah sebaiknya diterapkan pada instalasi perangkat lunak pada sistem operasional. Organisasi sebaiknya mengidentifikasi tipe instalasi perangkat lunak apa yang diizinkan (misalnya pembaruan dan tambalan keamanan) dan tipe instalasi apa yang dilarang (misalnya perangkat lunak yang hanya untuk penggunaan personal dan perangkat lunak yang patut diduga berkaitan berpotensi berbahaya atau tidak diketahui). Privilese ini sebaiknya diberikan berdasarkan peran pengguna yang bersangkutan.

Informasi lain
Tidak ada informasi lain.

8.20 Keamanan jaringan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Jaringan dan peranti jaringan sebaiknya diamankan, dimanajemeni, dan dikontrolkan untuk memproteksi informasi dalam sistem dan aplikasi.

Tujuan
Untuk memproteksi informasi dalam jaringan dan fasilitas pemrosesan informasi pendukungnya dari pemobobolan melalui jaringan.

Panduan
Kontrol sebaiknya diimplementasikan untuk memastikan keamanan informasi dalam jaringan dan untuk memproteksi layanan dari akses yang takterotorisasi. Hal-hal berikut sebaiknya dipertimbangkan:

a) tipe dan level klasifikasi informasi yang dapat didukung jaringan;
b) menetapkan tanggung jawab dan prosedur untuk manajemen peralatan dan peranti jaringan;
c) memelihara dokumentasi terbaru termasuk diagram jaringan dan fail konfigurasi peranti (misalnya perute, sakelar);
d) memisahkan tanggung jawab operasional untuk jaringan dari operasi sistem TIK yang sesuai (lihat 5.3);
e) menetapkan kontrol untuk menjaga konfidensialitas dan integritas data yang melewati jaringan publik, jaringan pihak ketiga, atau melalui jaringan nirkabel serta untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

memproteksi sistem dan aplikasi yang terhubung (lihat 5.22 , 8.24 , 5.14 dan 6.6). kontrol tambahan juga mungkin diperlukan untuk memelihara availabilitas dari layanan jaringan dan komputer yang terhubung ke jaringan;

f) membuat log dan memonitor dengan tepat untuk memungkinkan perekaman dan deteksi tindakan yang dapat memengaruhi, atau relevan dengan, keamanan informasi (lihat 8.16 dan 8.15);

g) mengoordinasikan aktivitas manajemen jaringan baik untuk mengoptimalkan layanan kepada organisasi maupun untuk memastikan bahwa kontrol secara konsisten diterapkan di seluruh infrastruktur pemrosesan informasi;

h) mengautentikasi sistem pada jaringan;

i) membatasi dan memfilter koneksi sistem ke jaringan (misalnya menggunakan *firewall*);

j) mendeteksi, membatasi, dan mengautentikasi koneksi peralatan dan peranti ke jaringan;

k) penguatan (*hardening*) peranti jaringan;

l) memisahkan saluran administrasi jaringan dari lalu lintas jaringan lainnya;

m) mengisolasi sementara subjaringan kritis (misalnya dengan *drawbridge*) jika jaringan diserang;

n) menonaktifkan protokol jaringan yang rentan.

Organisasi sebaiknya memastikan bahwa kontrol keamanan yang sesuai telah diterapkan pada penggunaan jaringan virtual. Jaringan virtual juga mencakup *software-defined networking* (SDN, SD-WAN). Jaringan virtual mungkin menarik dari sudut pandang keamanan karena memungkinkan pemisahan logis komunikasi yang terjadi melalui jaringan fisik, terutama untuk sistem dan aplikasi yang diimplementasikan menggunakan komputasi terdistribusi.

Informasi lain
Informasi tambahan tentang keamanan jaringan dapat ditemukan di seri ISO/IEC 27033. Informasi lebih lanjut mengenai jaringan virtual dapat ditemukan di ISO/IEC TS 23167.

8.21 Keamanan layanan jaringan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Mekanisme keamanan, level layanan, dan persyaratan layanan jaringan sebaiknya diidentifikasi, diimplementasikan, dan dimonitor.

Tujuan
Untuk memastikan keamanan dalam penggunaan layanan jaringan.

Panduan
Langkah-langkah keamanan yang diperlukan untuk layanan tertentu, seperti fitur keamanan, level layanan, dan persyaratan layanan, sebaiknya diidentifikasi dan diimplementasikan (oleh penyedia layanan jaringan internal atau eksternal). Organisasi sebaiknya memastikan bahwa penyedia layanan jaringan mengimplementasikanlangkah-langkah ini.

Kemampuan penyedia layanan jaringan untuk memanajemeni layanan yang disepakati dengan cara yang aman sebaiknya ditentukan dan dimonitor secara reguler. Hak untuk audit sebaiknya disepakati antara organisasi dan penyedia. Organisasi juga sebaiknya mempertimbangkan pengesahan pihak ketiga yang disediakan oleh penyedia layanan untuk

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

menunjukkan bahwa mereka mendemostrasikan langkah-langkah keamanan yang tepat.

Aturan tentang penggunaan jaringan dan layanan jaringan sebaiknya diformulasikan dan diimplementasikan mencakup:
a) jaringan dan layanan jaringan yang diizinkan untuk diakses;
b) persyaratan autentikasi untuk mengakses berbagai layanan jaringan;
c) prosedur otorisasi untuk menentukan siapa yang diizinkan untuk mengakses jaringan dan layanan jaringan
d) manajemen jaringan serta kontrol dan prosedur teknologi untuk memproteksi akses ke koneksi jaringan dan layanan jaringan;
e) sarana yang digunakan untuk mengakses jaringan dan layanan jaringan [misalnya penggunaan *Virtual Private Network*-VPN atau jaringan nirkabel];
f) waktu, lokasi, dan atribut pengguna lainnya pada saat akses;
g) pemonitoran penggunaan layanan jaringan.

Fitur-fitur keamanan layanan jaringan berikut sebaiknya dipertimbangkan:
a) teknologi yang diterapkan untuk keamanan layanan jaringan, seperti autentikasi, enkripsi, dan kontrol koneksi jaringan;
b) parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan aturan keamanan dan koneksi jaringan;
c) *caching* (misalnya dalam jaringan pengiriman konten) dan parameternya yang memungkinkan pengguna untuk memilih penggunaan *caching* sesuai dengan persyaratan kinerja, availabilitas, dan konfidensialitas;
d) prosedur untuk penggunaan layanan jaringan untuk membatasi akses ke layanan jaringan atau aplikasi, jika perlu.

Informasi lain
Layanan jaringan meliputi penyediaan koneksi, layanan jaringan privat, dan solusi keamanan jaringan terkelola seperti *firewall* dan sistem deteksi intrusi. Layanan ini dapat berkisar dari *bandwidth* sederhana yang tidak dimanajemeni hingga penawaran nilai tambah yang kompleks.

Panduan lebih lanjut tentang kerangka kerja untuk manajemen akses tersedia dalam ISO/IEC 29146.

8.22 Segregasi jaringan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Kelompok layanan informasi, pengguna, dan sistem informasi sebaiknya disegregasi dalam jaringan organisasi.

Tujuan
Untuk membagi jaringan dalam batas-batas keamanan dan untuk mengontrol lalu lintas di antaranya berdasarkan kebutuhan bisnis.

Panduan
Organisasi sebaiknya mempertimbangkan untuk memanajemeni keamanan jaringan besar dengan membaginya menjadi domain-domain jaringan terpisah dan memisahkannya dari

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

jaringan publik (yaitu internet). Domain dapat dipilih berdasarkan level kepercayaan, kekritisan, dan sensitivitas (misalnya domain akses publik, domain desktop, domain server, sistem berisiko rendah dan tinggi), di sepanjang unit organisasi (misalnya sumber daya manusia, finansial, pemasaran) atau beberapa kombinasi (misalnya domain server yang terhubung ke beberapa unit organisasi). Segregasi dapat dilakukan dengan menggunakan jaringan yang berbeda secara fisik atau dengan menggunakan jaringan logis yang berbeda.

Perimeter setiap domain sebaiknya ditentukan dengan baik. Jika akses antardomain jaringan diizinkan, akses tersebut sebaiknya dikontrol di perimeter menggunakan gerbang (misalnya *firewall*, ruter penyaring).

Kriteria untuk segregasi jaringan ke dalam domain, dan akses yang diizinkan melalui gerbang, sebaiknya didasarkan pada asesmen persyaratan keamanan setiap domain. Asesmen sebaiknya sesuai dengan kebijakan topik spesifik tentang kontrol akses (lihat 5.15), persyaratan akses, nilai, dan klasifikasi informasi yang diproses dan memperhitungkan biaya relatif dan dampak kinerja dari penggabungan teknologi gerbang yang sesuai.

Jaringan nirkabel memerlukan perlakuan khusus karena perimeter jaringan yang tidak didefinisikan dengan baik. Penyesuaian cakupan radio sebaiknya dipertimbangkan untuk segregasi jaringan nirkabel. Untuk lingkungan yang sensitif, sebaiknya dilakukan konsiderasi untuk memperlakukan semua akses nirkabel sebagai koneksi eksternal dan untuk memisahkan akses ini dari jaringan internal sampai akses telah melewati gerbang sesuai dengan kontrol jaringan (lihat 8.20) sebelum memberikan akses ke sistem internal. Jaringan akses nirkabel untuk tamu sebaiknya dipisahkan dari jaringan untuk personel jika personel hanya menggunakan peranti titik akhir pengguna terkontrol yang sesuai dengan kebijakan topik spesifik organisasi. WiFi untuk tamu sebaiknya memiliki setidaknya pembatasan yang sama dengan WiFi untuk personel, untuk mencegah penggunaan WiFi tamu oleh personel.

Informasi lain
Jaringan seringkali melampaui batas-batas organisasi, sebagaimana kemitraan bisnis terbentuk yang mensyaratkan interkoneksi atau berbagi fasilitas pemrosesan informasi dan jaringan. Ektensi tersebut dapat meningkatkan risiko akses takterotorisasi ke sistem informasi organisasi yang menggunakan jaringan, beberapa diantaranya memerlukan proteksi dari pengguna jaringan lain karena sensitivitas atau kritikalitasnya.

8.23 Pemfilteran web

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Akses ke situs web eksternal sebaiknya dimanajemeni untuk mengurangi eksposur konten berbahaya.

Tujuan
Untuk memproteksi sistem agar tidak dibobol oleh perangkat perusak dan untuk mencegah akses ke sumber daya web yang takterotorisasi.

Panduan
Organisasi sebaiknya mengurangi risiko personelnya mengakses situs web yang berisi informasi ilegal atau diketahui mengandung virus atau materi *phishing*. Salah satu tekniknya

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

yaitu dengan memblokir alamat IP atau domain situs web yang bersangkutan. Beberapa peramban dan teknologi anti-perangkat perusak melakukan ini secara otomatis atau dapat dikonfigurasi untuk melakukannya.

Organisasi sebaiknya mengidentifikasi tipe situs web yang boleh atau tidak boleh diakses oleh personelnya. Organisasi sebaiknya mempertimbangkan pemblokiran akses ke tipe situs web berikut:

a) situs web yang memiliki fungsi unggah informasi kecuali diizinkan untuk alasan bisnis yang valid;
b) situs web berbahaya yang diketahui atau dicurigai (misalnya yang mendistribusikan konten perangkat perusak atau *phishing*);
c) server perintah dan kontrol;
d) situs web berbahaya yang diperoleh dari intelijen ancaman (lihat 5.7);
e) situs web yang membagikan konten ilegal.

Sebelum mengimplementasikankontrol ini, organisasi sebaiknya menetapkan aturan untuk penggunaan sumber daya daring yang aman dan tepat, termasuk pembatasan untuk situs web dan aplikasi berbasis web yang takdiinginkan atau takpantas. Aturan sebaiknya dijaga tetap mutakhir.

Pelatihan sebaiknya diberikan kepada personel tentang penggunaan sumber daya daring yang aman dan tepat termasuk akses ke web. Pelatihan sebaiknya mencakup aturan organisasi, titik kontak untuk meningkatkan masalah keamanan, dan proses eksepsi ketika sumber daya web terbatas perlu diakses karena alasan bisnis yang sah. Pelatihan juga sebaiknya diberikan kepada personel untuk memastikan bahwa mereka tidak menolak advis peramban yang melaporkan bahwa suatu situs web tidak aman tetapi memungkinkan pengguna untuk melanjutkan.

Informasi lain

Pemfilteran web dapat mencakup berbagai teknik termasuk tanda tangan, heuristik, daftar situs web atau domain yang akseptabel, daftar situs web atau domain terlarang, dan konfigurasi yang sudah ada untuk membantu mencegah perangkat lunak berbahaya dan aktivitas berbahaya lainnya menyerang jaringan dan sistem organisasi.

8.24 Penggunaan kriptografi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Konfigurasi_yang_aman	#Proteksi

Kontrol

Aturan untuk penggunaan kriptografi yang efektif, termasuk manajemen kunci kriptografi, sebaiknya didefinisikan dan diimplementasikan.

Tujuan

Untuk memastikan penggunaan kriptografi yang tepat dan efektif untuk memproteksi konfidensialitas, autentisitas, atau integritas informasi berdasarkan persyaratan keamanan bisnis dan informasi, dan dengan konsiderasi persyaratan legal, statutori, regulatori dan kontraktual yang terkait dengan kriptografi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan

Umum

Saat menggunakan kriptografi, hal-hal berikut sebaiknya dipertimbangkan:

a) kebijakan topik spesifik tentang kriptografi yang didefinisikan oleh organisasi, termasuk prinsip umum untuk proteksi informasi. Kebijakan topik spesifik tentang penggunaan kriptografi diperlukan untuk memaksimalkan manfaat dan meminimalkan risiko penggunaan teknik kriptografi dan untuk menghindari penggunaan yang taktepat atau takbenar;
b) mengidentifikasi level proteksi yang dipersyaratkan dan klasifikasi informasi serta menetapkan tipe, kekuatan, dan kualitas dari algoritma kriptografi yang dipersyaratkan;
c) penggunaan kriptografi untuk proteksi informasi yang berada pada peranti mobil titik akhir pengguna atau media penyimpanan dan ditransmisikan melalui jaringan ke peranti atau media penyimpanan tersebut;
d) pendekatan manajemen kunci, termasuk metode untuk menangani pembangkitan dan proteksi kunci kriptografi dan pemulihan informasi terenkripsi jika kunci hilang, dibobol, atau rusak;
e) Peran dan tanggung jawab untuk:
   1) implementasi aturan untuk penggunaan kriptografi yang efektif
   2) manajemen kunci, termasuk pembangkitan kunci (lihat 8.24);
f) standar yang akan diadopsi, serta algoritma kriptografi, kekuatan penyandian, solusi kriptografi dan praktik penggunaan yang disetujui atau dipersyaratkan untuk digunakan di organisasi;
g) dampak penggunaan informasi terenkripsi terhadap kontrol yang bergantung pada inspeksi konten (misalnya deteksi perangkat perusak atau pemfilteran konten).

Saat mengimplementasikan aturan organisasi untuk penggunaan kriptografi yang efektif, regulasi, dan pembatasan nasional yang dapat diterapkan pada penggunaan teknik kriptografi di berbagai belahan dunia serta isu aliran lintas-batas dari informasi terenkripsi sebaiknya dijadikan konsiderasi (lihat 5.31).

Konten perjanjian level layanan atau kontrak dengan pemasok eksternal dari layanan kriptografi (misalnya dengan otoritas sertifikasi) sebaiknya mencakup isu liabilitas, reliabilitas layanan, dan waktu respons untuk penyediaan layanan (lihat 5.22).

Manajemen kunci

Manajemen kunci yang tepat mensyaratkan proses yang aman untuk membangkitkan, menyimpan, mengarsipkan, mengambil, mendistribusikan, menghentikan, dan menghancurkan kunci kriptografi.

Sistem manajemen kunci sebaiknya didasarkan pada seperangkat standar, prosedur, dan metode keamanan yang disepakati untuk:

a) membangkitkan kunci untuk sistem kriptografi yang berbeda dan aplikasi yang berbeda;
b) menerbitkan dan memperoleh sertifikat kunci publik;
c) mendistribusikan kunci ke entitas yang dituju, termasuk cara mengaktifkan kunci saat diterima;
d) menyimpan kunci, termasuk bagaimana pengguna yang terotorisasi mendapatkan akses ke kunci;
e) mengubah atau memperbarui kunci termasuk aturan tentang kapan mengubah kunci dan bagaimana melakukannya;
f) mengurusi kunci yang dibobol;
g) mencabut kunci termasuk cara menarik atau menonaktifkan kunci [misalnya ketika kunci telah dibobol atau ketika pengguna meninggalkan organisasi (dalam hal ini kunci juga sebaiknya diarsipkan)];
h) memulihkan kunci yang hilang atau rusak;
i) mencadangkan atau mengarsipkan kunci;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

j) menghancurkan kunci;
k) membuat log atau mengaudit aktivitas terkait manajemen kunci;
l) mengatur tanggal aktivasi dan penonaktifan untuk kunci sehingga kunci hanya dapat digunakan untuk periode waktu sesuai dengan aturan organisasi tentang manajemen kunci;
m) menangani permintaan legal untuk akses ke kunci kriptografi (misalnya informasi terenkripsi dapat dipersyaratkan untuk disediakan dalam bentuk yang takterenkripsi sebagai bukti dalam kasus pengadilan).

Semua kunci kriptografi sebaiknya diproteksi dari modifikasi dan kehilangan. Sebagai tambahan, kunci konfidensial dan privat membutuhkan proteksi terhadap penggunaan takterotorisasi serta pengungkapan. Peralatan yang digunakan untuk membangkitkan, menyimpan, dan mengarsipkan kunci sebaiknya diproteksi secara fisik.

Sebagai tambahan untuk integritas, bagi banyak kasus penggunaan, autentisitas kunci publik juga sebaiknya dipertimbangkan.

Informasi lain
Autentisitas kunci publik biasanya diurus dengan proses manajemen kunci publik menggunakan otoritas sertifikat dan sertifikat kunci publik, tetapi juga dimungkinkan untuk mengurusnya dengan menggunakan teknologi seperti mengimplementasikanproses manual untuk kunci bilangan kecil.

Kriptografi dapat digunakan untuk mencapai sasaran keamanan informasi yang berbeda, misalnya:
a) konfidensialitas: menggunakan enkripsi informasi untuk memproteksi informasi sensitif atau kritis, baik yang disimpan atau ditransmisikan;
b) integritas atau autentisitas: menggunakan tanda tangan digital atau kode autentikasi pesan untuk memverifikasi autentisitas atau integritas dari informasi sensitif atau kritis yang disimpan atau ditransmisikan. Menggunakan algoritma untuk tujuan pemeriksaan integritas fail;
c) nirsangkal: menggunakan teknik kriptografi untuk menyediakan bukti terjadinya atau tidak terjadinya suatu peristiwa atau tindakan;
d) autentikasi: menggunakan teknik kriptografi untuk mengautentikasi pengguna dan entitas sistem lainnya yang meminta akses ke atau bertransaksi dengan pengguna, entitas, dan sumber daya sistem.

Seri ISO/IEC 11770 menyediakan informasi lebih lanjut tentang manajemen kunci.

8.25 Siklus hidup pengembangan yang aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Aturan untuk pengembangan perangkat lunak dan sistem yang aman sebaiknya ditetapkan dan diterapkan.

Tujuan
Untuk memastikan keamanan informasi didesain dan diimplementasikan dalam pengembangan siklus hidup yang aman dari perangkat lunak dan sistem.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan
Pengembangan yang aman adalah persyaratan untuk membangun layanan, arsitektur, perangkat lunak, dan sistem yang aman. Untuk mencapai hal ini, aspek berikut sebaiknya dipertimbangkan:

a) separasi lingkungan pengembangan, uji dan produksi (lihat 8.31);
b) panduan tentang keamanan dalam siklus hidup pengembangan perangkat lunak:
   1) keamanan dalam metodologi pengembangan perangkat lunak (lihat 8.28 dan 8.27);
   2) pedoman pengkodean yang aman untuk setiap bahasa pemrograman yang digunakan (lihat 8.28);
c) persyaratan keamanan dalam spesifikasi dan fase desain (lihat 5.8);
d) titik pemeriksaan keamanan dalam proyek (lihat 5.8);
e) pengujian sistem dan keamanan, seperti pengujian regresi, pemindaian kode, dan uji penetrasi (lihat 8.29);
f) repositori yang aman untuk kode sumber dan konfigurasi (lihat 8.4 dan 8.9);
g) keamanan dalam kontrol versi (lihat 8.32)
h) pengetahuan dan pelatihan keamanan aplikasi yang diperlukan (lihat 8.28);
i) kapabilitas developer untuk mencegah, menemukan, dan memperbaiki kerentanan (lihat 8.28);
j) persyaratan lisensi dan alternatif untuk memastikan solusi hemat biaya sekaligus menghindari masalah lisensi di masa depan (Lihat 5.32).

Jika pengembangan dialihdayakan, organisasi sebaiknya mendapatkan keyakinan bahwa pemasok mematuhi aturan organisasi tentang pengembangan yang aman (lihat 8.30).

Informasi lain
Pengembangan juga dapat dilakukan di dalam aplikasi, seperti aplikasi kantor, penulisan skrip, peramban, dan pangkalan data.

8.26 Persyaratan keamanan aplikasi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi #Pertahanan

Kontrol
Persyaratan keamanan informasi sebaiknya diidentifikasi, dispesifikasi, dan disetujui saat mengembangkan atau memperoleh aplikasi.

Tujuan
Untuk memastikan semua persyaratan keamanan informasi diidentifikasi dan ditangani saat mengembangkan atau memperoleh aplikasi.

Panduan
Umum
Persyaratan keamanan aplikasi sebaiknya diidentifikasi dan dispesifikasi. Persyaratan ini biasanya ditentukan melalui asesmen risiko. Persyaratan sebaiknya dikembangkan dengan dukungan spesialis keamanan informasi.

Persyaratan keamanan aplikasi dapat mencakup berbagai topik, tergantung pada tujuan aplikasi.

Persyaratan keamanan aplikasi sebaiknya mencakup, antara lain:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) level kepercayaan pada identitas entitas [misalnya melalui autentikasi (lihat 5.17, 8.2, dan 8.5)];
b) mengidentifikasi tipe informasi dan level klasifikasi yang akan diproses oleh aplikasi;
c) kebutuhan akan segregasi akses dan level akses ke data dan fungsi dalam aplikasi;
d) resiliensi terhadap serangan berbahaya atau gangguan yang takdisengaja [misalnya proteksi terhadap *buffer overflow* atau injeksi *structured query language* (SQL)];
e) persyaratan legal, statutori dan regulatori di yurisdiksi tempat transaksi dibangkitkan, diproses, diselesaikan, atau disimpan;
f) kebutuhan akan privasi yang terkait dengan semua pihak yang terlibat;
g) persyaratan proteksi dari setiap informasi konfidensial;
h) proteksi data saat diproses, dalam perjalanan, dan saat disimpan;
i) kebutuhan akan mengenkripsi komunikasi secara aman di antara semua pihak yang terlibat;
j) kontrol masukan, termasuk pemeriksaan integritas dan validasi masukan;
k) kontrol otomatis (misalnya batas persetujuan atau persetujuan ganda);
l) kontrol keluaran, juga mempertimbangkan siapa yang dapat mengakses keluaran dan otorisasinya;
m) pembatasan seputar konten bidang "teks bebas", karena dapat menyebabkan penyimpanan takterkontrol atas data konfidensial (misalnya data pribadi);
n) persyaratan yang berasal dari proses bisnis, seperti pencatatan dan pemonitoran transaksi, persyaratan nirsangkal;
o) persyaratan yang diamanatkan oleh kontrol keamanan lainnya (misalnya antarmuka untuk pembuatan log dan pemonitoran atau sistem deteksi kebocoran data);
p) penanganan pesan galat.

Layanan transaksional

Selain itu, untuk aplikasi yang menawarkan layanan transaksional antara organisasi dan mitra, hal-hal berikut sebaiknya dipertimbangkan ketika mengidentifikasi persyaratan keamanan informasi:

a) level kepercayaan yang dipersyaratkan tiap pihak dalam identitas yang diklaim masing-masing;
b) level kepercayaan yang dipersyaratkan dalam integritas informasi yang dipertukarkan atau diproses dan mekanisme identifikasi untuk kurangnya integritas (misalnya pemeriksaan redundansi siklik, *hashing*, tanda tangan digital);
c) otorisasi yang terkait dengan siapa yang dapat menyetujui konten, mengeluarkan, atau menandatangani dokumen transaksional kunci;
d) konfidensialitas, integritas, bukti pengiriman, dan penerimaan dari dokumen-dokumen kunci dan nirsangkal (misalnya kontrak yang terkait dengan proses tender dan kontrak);
e) konfidensialitas dan integritas dari segala transaksi (misalnya pesanan, detail alamat pengiriman, dan konfirmasi tanda terima);
f) persyaratan tentang berapa lama memelihara konfidensialitas transaksi;
g) asuransi dan persyaratan kontraktual lainnya.

Aplikasi pemesanan dan pembayaran elektronik

Selain itu, untuk aplikasi yang melibatkan pemesanan dan pembayaran elektronik, hal-hal berikut ini sebaiknya dipertimbangkan

a) persyaratan untuk memelihara konfidensialitas dan integritas informasi pesanan;
b) derajat verifikasi yang tepatuntuk memverifikasi informasi pembayaran yang diberikan oleh pelanggan;
c) penghindaran kehilangan atau duplikasi informasi transaksi;
d) menyimpan detail transaksi di luar dari lingkungan yang dapat diakses publik (misalnya pada platform penyimpanan pada intranet organisasi, dan tidak dipertahankan dan diekspos pada media penyimpanan elektronik yang dapat diakses langsung dari internet);
e) ketika otoritas tepercaya digunakan (misalnya untuk tujuan menerbitkan dan memelihara

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

tanda tangan digital atau sertifikat digital) keamanan diintegrasikan atau dilekatkan di seluruh proses manajemen sertifikat atau tanda tangan *end-to-end*.

Beberapa konsiderasi di atas dapat diatasi dengan penerapan kriptografi (lihat 8.24), dengan mempertimbangkan persyaratan legal (lihat 5.31 hingga 5.36, khususnya lihat 5.31 untuk legislasi kriptografi).

Informasi lain
Aplikasi yang dapat diakses melalui jaringan adalah subyek berbagai ancaman terkait jaringan, seperti aktivitas penipuan, perselisihan kontrak, atau pengungkapan informasi kepada publik; transmisi taklengkap, salah-rute, perubahan pesan secara takterotorisasi, duplikasi atau pemutaran ulang. Oleh karena itu, asesmen risiko terperinci dan determinasi kontrol yang cermat sangat diperlukan. Kontrol yang dipersyaratkan sering kali mencakup metode kriptografi untuk autentikasi dan pengamanan transfer data.

Informasi lebih lanjut tentang keamanan aplikasi dapat ditemukan dalam seri ISO/IEC 27034.

8.27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Prinsip-prinsip untuk rekayasa sistem yang aman sebaiknya ditetapkan, didokumentasikan, dipelihara, dan diterapkan pada segala aktivitas pengembangan sistem informasi.

Tujuan
Untuk memastikan sistem informasi didesain, diimplementasikan dan dioperasikan secara aman dalam siklus hidup pengembangan.

Panduan
Prinsip-prinsip rekayasa keamanan sebaiknya ditetapkan, didokumentasikan, dan diterapkan pada aktivitas rekayasa sistem informasi. Keamanan sebaiknya didesain ke semua lapisan arsitektur (bisnis, data, aplikasi, dan teknologi). Teknologi baru sebaiknya dianalisis untuk risiko keamanan dan desain sebaiknya direviu terhadap pola serangan yang diketahui.

Prinsip-prinsip rekayasa yang aman memberikan panduan tentang teknik autentikasi pengguna, kontrol sesi yang aman, dan validasi dan sanitasi data.

Prinsip-prinsip rekayasa sistem yang aman sebaiknya mencakup analisis:
a) berbagai kontrol keamanan yang dipersyaratkan untuk memproteksi informasi dan sistem terhadap ancaman yang teridentifikasi;
b) kapabilitas kontrol keamanan untuk mencegah, mendeteksi, atau merespons peristiwa keamanan;
c) kontrol keamanan spesifik yang dipersyaratkan oleh proses bisnis tertentu (misalnya enkripsi informasi sensitif, pemeriksaan integritas, dan penandatanganan informasi secara digital);
d) di mana dan bagaimana kontrol keamanan diterapkan (misalnya dengan mengintegrasikan dengan arsitektur keamanan dan infrastruktur teknis);
e) bagaimana kontrol keamanan individual (manual dan otomatis) bekerja sama untuk menghasilkan serangkaian kontrol terintegrasi.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Prinsip-prinsip rekayasa keamanan sebaiknya memperhitungkan:
a) kebutuhan untuk berintegrasi dengan arsitektur keamanan;
b) infrastruktur keamanan teknis [misalnya infrastruktur kunci publik (*Public Key Infrastructure*-PKI), manajemen identitas dan akses (*Identity and Access Management*-IAM), pencegahan kebocoran data dan manajemen akses dinamis];
c) kapablitas organisasi untuk mengembangkan dan mendukung teknologi yang dipilih;
d) biaya, waktu, dan kompleksitas untuk memenuhi persyaratan keamanan;
e) praktik baik saat ini.

Rekayasa sistem yang aman sebaiknya melibatkan:
a) penggunaan prinsip-prinsip arsitektur keamanan, seperti "keamanan dengan desain", "pertahanan berlapis", "keamanan bawaan", "penolakan bawaan", "gagal secara aman", "input ketidakpercayaan dari aplikasi eksternal", "keamanan dalam pengerahan", "asumsi pelanggaran", "privilese terendah", "kegunaan dan manajemen", dan "fungsionalitas terendah";
b) reviu desain berorientasi keamanan untuk membantu mengidentifikasi kerentanan keamanan informasi, memastikan kontrol keamanan dispesifikasikan dan memenuhi persyaratan keamanan;
c) dokumentasi dan pengakuan formal atas kontrol keamanan yang tidak sepenuhnya memenuhi persyaratan (misalnya karena mengesampingkan persyaratan keselamatan);
d) penguatan sistem.

Organisasi sebaiknya mempertimbangkan prinsip "nol kepercayaan" seperti:
a) mengasumsikan sistem informasi organisasi sudah dilanggar sehingga tidak bergantung pada keamanan perimeter jaringan saja;
b) menggunakan pendekatan "jangan pernah percaya dan selalu verifikasi" untuk akses ke sistem informasi;
c) memastikan bahwa permintaan ke sistem informasi dienkripsi secara *end-to-end*;
d) memverifikasi setiap permintaan ke sistem informasi seolah-olah berasal dari jaringan eksternal yang terbuka, bahkan jika permintaan ini berasal dari internal organisasi (yaitu tidak secara otomatis memercayai apa pun di dalam atau di luar perimeternya);
e) menggunakan "privilese terendah" dan teknik kontrol akses dinamis (lihat 5.15 , 5.18 dan 8.2), ini termasuk mengautentikasi dan mengotorisasi permintaan untuk informasi atau ke sistem berdasarkan informasi kontekstual seperti informasi autentikasi (lihat 5.17), identitas pengguna (lihat 5.16), data tentang peranti titik akhir pengguna, dan klasifikasi data (lihat 5.12);
f) selalu mengautentikasi pemohon dan selalu memvalidasi permintaan otorisasi ke sistem informasi berdasarkan informasi termasuk informasi autentikasi (lihat 5.17) dan identitas pengguna (5.16), data tentang peranti titik akhir pengguna, dan klasifikasi data (lihat 5.12), sebagai contoh menegakkan autentikasi yang kuat (misalnya multifaktor, lihat 8.5).

Prinsip-prinsip rekayasa keamanan yang ditetapkan sebaiknya diterapkan, jika berlaku, untuk pengembangan sistem informasi yang dialihdayakan melalui kontrak dan perjanjian mengikat lainnya antara organisasi dan pemasok kepada siapa organisasi melakukan pengalihdayaan. Organisasi sebaiknya memastikan bahwa praktik rekayasa keamanan pemasok selaras dengan kebutuhan organisasi.

Prinsip rekayasa keamanan dan prosedur rekayasa yang ditetapkan sebaiknya direviu secara reguler untuk memastikan bahwa prinsip tersebut secara efektif berkontribusi pada peningkatan standar keamanan dalam proses rekayasa. Prinsip tersebut juga sebaiknya direviu secara reguler untuk memastikannya tetap mutakhir dalam hal memerangi segala potensi ancaman baru dan tetap berlaku untuk kemajuan dalam teknologi dan solusi yang diterapkan

Informasi lain

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Prinsip rekayasa yang aman dapat diterapkan pada desain atau konfigurasi berbagai teknik, seperti:
— toleransi kesalahan dan teknik resiliensi lainnya;
— segregasi (misalnya melalui virtualisasi atau penampungan);
— resistansi kerusakan.
Teknik virtualisasi yang aman dapat digunakan untuk mencegah interferensi antara aplikasi-aplikasi yang berjalan pada peranti fisik yang sama. Jika contoh virtual dari suatu aplikasi dibobol oleh penyerang, hanya contoh tersebut yang terpengaruh. Serangan itu tidak berpengaruh pada aplikasi atau data lain.

Teknik resistansi gangguan dapat digunakan untuk mendeteksi gangguan kontainer informasi, baik fisik (misalnya alarm pencuri) atau logis (misalnya fail data). Karakteristik dari teknik tersebut adalah bahwa ada rekaman upaya untuk merusak kontainer. Selain itu, kontrol dapat mencegah keberhasilan ekstraksi data melalui destruksinya (misalnya memori peranti dapat dihapus).

8.28 Pengkodean yang aman

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Keamanan domains
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Prinsip pengkodean yang aman sebaiknya diterapkan pada pengembangan perangkat lunak.

Tujuan
Untuk memastikan perangkat lunak ditulis secara aman sehingga mengurangi jumlah kerentanan keamanan informasi potensial dalam perangkat lunak.

Panduan
Umum
Organisasi sebaiknya menetapkan proses di seluruh organisasi untuk menyediakan tata kelola yang baik untuk pengkodean yang aman. Garis acuan keamanan minimum sebaiknya ditetapkan dan diterapkan. Selain itu, proses dan tata kelola tersebut sebaiknya diperluas untuk mencakup komponen perangkat lunak dari pihak ketiga dan perangkat lunak sumber terbuka.

Organisasi sebaiknya memonitor ancaman dunia nyata serta saran dan informasi terkini tentang kerentanan perangkat lunak untuk memandu prinsip pengkodean organisasi yang aman melalui peningkatan dan pembelajaran terus menerus. Ini dapat membantu memastikan praktik pengkodean yang aman yang efektif diimplementasikan untuk memerangi lanskap ancaman yang berubah-cepat.

Perencanaan dan sebelum pengkodean
Prinsip pengkodean yang aman sebaiknya digunakan baik untuk pengembangan baru maupun dalam skenario penggunaan kembali. Prinsip-prinsip ini sebaiknya diterapkan pada aktivitas pengembangan baik dalam organisasi maupun untuk produk dan layanan yang dipasok oleh organisasi kepada organisasi lain. Perencanaan dan prasyarat sebelum pengkodean sebaiknya mencakup:
a) harapan spesifik-organisasi dan prinsip yang disetujui untuk pengkodean aman untuk digunakan baik dalam pengembangan kode internal dan yang dialihdayakan;
b) praktik dan cacat pengkodean biasa dan historis yang mengarah pada kerentanan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

keamanan informasi;
c) mengonfigurasi alat pengembangan, seperti *integrated development environments* (IDE), untuk membantu melaksanakan pembuatan kode aman;
d) mengikuti panduan yang dikeluarkan oleh penyedia alat pengembangan dan lingkungan eksekusi sebagaimana berlaku;
e) pemeliharaan dan penggunaan alat pengembangan yang diperbarui (misalnya kompilator);
f) kualifikasi developer dalam menulis kode yang aman;
g) desain dan arsitektur yang aman, termasuk pemodelan ancaman;
h) standar pengkodean yang aman dan jika relevan mewajibkan penggunaannya;
i) penggunaan lingkungan yang terkontrol untuk pengembangan.

Selama pengkodean
Konsiderasi selama pengkodean sebaiknya mencakup:
a) praktik pengkodean yang aman spesifik untuk bahasa dan teknik pemrograman yang digunakan;
b) menggunakan teknik pemrograman yang aman, seperti pemrograman berpasangan, pemfaktoran ulang, reviu sejawat, iterasi keamanan, dan pengembangan berdasarkan pengujian;
c) menggunakan teknik pemrograman terstruktur;
d) mendokumentasikan kode dan memindahkan cacat pemrograman, yang dapat memungkinkan kerentanan keamanan informasi untuk dieksploitasi;
e) melarang penggunaan teknik desain yang tidak aman (misalnya penggunaan kata sandi kode kuat, sampel kode yang tidak disetujui, dan layanan web yang takterautentikasi).

Pengujian sebaiknya dilakukan selama dan setelah pengembangan (lihat 8.29). Proses *Static application security testing* (SST) dapat mengidentifikasi kerentanan keamanan dalam perangkat lunak.
Sebelum perangkat lunak dioperasikan, hal-hal berikut sebaiknya dievaluasi:
a) permukaan serangan dan prinsip privilese terendah;
b) melakukan analisis galat pemrograman yang paling umum dan mendokumentasikan bahwa hal tersebut telah dimitigasi.

Reviu dan pemeliharaan
Setelah kode dioperasikan:
a) pembaruan sebaiknya dikemas dan digelar secara aman;
b) kerentanan keamanan informasi yang dilaporkan sebaiknya ditangani (lihat 8.8);
c) kesalahan dan dugaan serangan sebaiknya dicatat dan log secara reguler direviu untuk penyesuaian kode jika diperlukan;
d) kode sumber sebaiknya diproteksi dari akses dan gangguan yang takterotorisasi (misalnya dengan menggunakan alat manajemen konfigurasi, yang biasanya menyediakan fitur seperti kontrol akses dan kontrol versi).

Jika menggunakan alat dan pustaka eksternal, organisasi sebaiknya mempertimbangkan:
a) memastikan bahwa pustaka eksternal dimanajemeni (misalnya dengan memelihara inventaris pustaka yang digunakan dan versinya) dan secara reguler diperbarui dengan siklus rilis;
b) seleksi, otorisasi, dan penggunaan kembali komponen yang telah diperiksa dengan baik, khususnya komponen autentikasi dan kriptografi;
c) lisensi, keamanan, dan riwayat komponen eksternal;
d) memastikan bahwa perangkat lunak dapat dipelihara, dilacak, dan berasal dari sumber yang terbukti dan bereputasi;
e) availabilitas yang berjangka cukup panjang dari sumber daya dan artefak pengembangan .

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Jika paket perangkat lunak perlu dimodifikasi, poin-poin berikut sebaiknya dipertimbangkan:
a) risiko kontrol bawaan dan proses integritas yang bobol;
b) apakah akan mendapatkan persetujuan dari vendor;
c) kemungkinan mendapatkan perubahan yang dipersyaratkan dari vendor sebagai pembaruan program standar;
d) dampak jika organisasi menjadi bertanggung jawab atas pemeliharaan perangkat lunak di masa depan sebagai hasil dari perubahan;
e) kompatibilitas dengan perangkat lunak lain yang digunakan.

Informasi lain
Prinsip panduan adalah untuk memastikan kode keamanan yang relevan dipanggil saat diperlukan dan tahan terhadap gangguan. Program yang diinstal dari kode biner terkompilasi juga memiliki properti ini tetapi hanya untuk data yang disimpan dalam aplikasi. Dengan kata lain, konsep ini hanya bekerja ketika kode dieksekusi di server yang sebaliknya tidak dapat diakses oleh pengguna dan proses yang menggunakannya, dan datanya disimpan dalam pangkalan data yang diproteksi secara serupa. Sebagai contoh, kode yang diinterpretasikan dapat dijalankan pada layanan *cloud* yang akses ke kodenya sendiri mensyaratkan privilese administrator. Akses administrator tersebut sebaiknya diproteksi oleh mekanisme keamanan seperti prinsip administrasi tepat waktu dan autentikasi yang kuat. Jika pemilik aplikasi dapat mengakses skrip dengan akses jarak jauh langsung ke server pada prinsipnya penyerang juga bisa. Server web sebaiknya dikonfigurasi untuk mencegah perambanan direktori dalam kasus seperti itu.

Kode aplikasi paling baik didesain dengan asumsi bahwa kode tersebut selalu subyek serangan, melalui galat atau aksi berbahaya. Selain itu, aplikasi kritis dapat didesain untuk toleran terhadap kesalahan internal. Sebagai contoh, keluaran dari algoritma kompleks dapat dicek untuk memastikan bahwa keluaran tersebut berada dalam batas aman sebelum data digunakan dalam aplikasi seperti aplikasi kritis keselamatan atau finansial kritis. Kode yang melakukan pemeriksaan batas sederhana sehingga jauh lebih mudah untuk membuktikan kebenaran.

Beberapa aplikasi web rentan terhadap berbagai kerentanan yang muncul karena desain dan pengkodean yang buruk, seperti injeksi pangkalan data dan serangan skrip lintas-situs. Dalam serangan ini, permintaan dapat dimanipulasi untuk menyalahgunakan fungsionalitas server web.

Informasi lebih lanjut tentang evaluasi keamanan TIK dapat ditemukan dalam seri ISO/IEC 15408.

8.29 Pengujian keamanan dalam pengembangan dan penerimaan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Keamanan_aplikasi #Jaminan_keamanan_informasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Proses pengujian keamanan sebaiknya didefinisikan dan diimplementasikan dalam siklus hidup pengembangan

Tujuan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Untuk memvalidasi jika persyaratan keamanan informasi terpenuhi ketika aplikasi atau kode digelar ke lingkungan produksi.

Panduan

Sistem informasi baru, peningkatan, dan versi baru sebaiknya diuji dan diverifikasi secara menyeluruh selama proses pengembangan. Pengujian keamanan sebaiknya menjadi bagian integral dari pengujian untuk sistem atau komponen.

Pengujian keamanan sebaiknya dilakukan terhadap serangkaian persyaratan, yang dapat dinyatakan sebagai fungsional atau nonfungsional. Pengujian keamanan sebaiknya mencakup pengujian terhadap:

a) fungsi keamanan [misalnya autentikasi pengguna (lihat 8.5), pembatasan akses (lihat 8.3), dan penggunaan kriptografi (lihat 8.24)];
b) pengkodean aman (lihat 8.28);
c) konfigurasi yang aman (lihat 8.9, 8.20, dan 8.22) termasuk sistem operasi, *firewall*, dan komponen keamanan lainnya.

Rencana uji sebaiknya ditentukan menggunakan serangkaian kriteria. Cakupan pengujian sebaiknya dalam proporsi dengan kepentingan, sifat sistem, dan dampak potensial dari perubahan yang muncul. Rencana uji sebaiknya mencakup:

a) jadwal aktivitas dan uji secara detail;
b) masukan dan keluaran yang diharapkan dalam berbagai kondisi;
c) kriteria untuk mengevaluasi hasil;
d) keputusan untuk tindak lanjut yang diperlukan.

Organisasi dapat memanfaatkan alat otomatis, seperti alat analisis kode atau pemindai kerentanan, dan sebaiknya memverifikasi remediasi cacat terkait keamanan.

Untuk pengembangan secara mandiri, pengujian semacam itu pada awalnya sebaiknya dilakukan oleh tim pengembangan. Pengujian penerimaan independen kemudian sebaiknya dilakukan untuk memastikan bahwa sistem bekerja seperti yang diharapkan dan hanya seperti yang diharapkan (lihat 5.8). Hal-hal berikut sebaiknya dipertimbangkan:

a) melakukan aktivitas reviu kode sebagai elemen yang relevan untuk pengujian kekurangan keamanan, termasuk input dan kondisi yang takdiantisipasi;
b) melakukan pemindaian kerentanan untuk mengidentifikasi konfigurasi yang takaman dan kerentanan sistem;
c) melakukan pengujian penetrasi untuk mengidentifikasi kode dan desain yang takaman.

Untuk pengembangan dan pembelian komponen yang dialihdayakan, proses akuisisi sebaiknya diikuti. Kontrak dengan pemasok sebaiknya membahas persyaratan keamanan yang diidentifikasi (lihat 5.20). Produk dan layanan sebaiknya dievaluasi terhadap kriteria ini sebelum akuisisi.

Pengujian sebaiknya dilakukan dalam lingkungan uji yang cocok dengan lingkungan produksi sedekat mungkin untuk memastikan bahwa sistem tidak memunculkan kerentanan pada lingkungan organisasi dan bahwa pengujian dapat diandalkan (lihat 8.31).

Informasi lain

Dapat ditetapkan beberapa lingkungan pengujian, yang dapat digunakan untuk berbagai tipe pengujian (misalnya pengujian fungsional dan kinerja). Lingkungan yang berbeda ini dapat berupa virtual, dengan konfigurasi individual untuk menyimulasikan berbagai lingkungan operasi.

Pengujian dan pemonitoran lingkungan uji, alat dan teknologi juga butuh dipertimbangkan untuk memastikan pengujian yang efektif. Konsiderasi yang sama berlaku untuk pemonitoran

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

sistem pemonitoran yang digelar dalam pengaturan pengembangan, uji, dan produksi. Asesmen dibutuhkan, dipandu oleh sensitivitas sistem dan data, untuk menentukan berapa banyak lapisan *meta-testing* yang berguna.

8.30 Pengembangan yang dialihdayakan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi #Mendeteksi	#Keamanan_sistem_dan_jaringan #Keamanan_aplikasi #Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi

Kontrol
Organisasi sebaiknya mengarahkan, memonitor, dan mereviu aktivitas yang terkait dengan pengembangan sistem yang dialihdayakan.

Tujuan
Untuk memastikan langkah-langkah keamanan informasi yang dipersyaratkan oleh organisasi diimplementasikan dalam pengembangan sistem yang dialihdayakan.

Panduan
Jika pengembangan sistem dialihdayakan, organisasi sebaiknya mengomunikasikan dan menyetujui persyaratan dan ekspektasi, dan terus memonitor dan mereviu apakah pengiriman pekerjaan yang dialihdayakan memenuhi harapan tersebut. Poin-poin berikut sebaiknya dipertimbangkan di seluruh rantai pasokan eksternal organisasi:

a) perjanjian lisensi, kepemilikan kode dan hak kekayaan intelektual yang terkait dengan alih daya konten (lihat 5.32);
b) persyaratan kontraktual untuk praktik desain, pengkodean, dan pengujian yang aman (lihat 8.25 hingga 8.29);
c) penyediaan model ancaman untuk dipertimbangkan oleh developer eksternal;
d) pengujian penerimaan untuk kualitas dan akurasi hasil pekerjaan(lihat 8.29);
e) penyediaan bukti bahwa level keamanan dan kapabilitas privasi minimum yang akseptabel telah ditetapkan (misalnya laporan jaminan);
f) penyediaan bukti bahwa pengujian yang cukup telah diterapkan untuk menjaga terhadap keberadaan konten berbahaya (baik disengaja maupun takdisengaja) pada saat pengiriman;
g) pemberian bukti bahwa pengujian yang cukup telah diterapkan untuk menjaga terhadap adanya kerentanan yang diketahui;
h) perjanjian eskro untuk kode sumber perangkat lunak (misalnya jika pemasok berhenti beroperasi);
i) hak kontraktual untuk mengaudit proses dan kontrol pengembangan;
j) persyaratan keamanan untuk lingkungan pengembangan (lihat 8.31);
k) mempertimbangkan legislasi yang berlaku (misalnya tentang proteksi data pribadi).

Informasi lain
Informasi lebih lanjut tentang hubungan pemasok dapat ditemukan di seri ISO/IEC 27036.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.31 Pemisahan lingkungan pengembangan, uji, dan produksi

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Lingkungan pengembangan, pengujian, dan produksi sebaiknya dipisahkan dan diamankan.

Tujuan
Untuk memproteksi lingkungan produksi dan data dari pemobobolan oleh aktivitas pengembangan dan uji.

Panduan
Level separasi antara lingkungan produksi, pengujian, dan pengembangan yang diperlukan untuk mencegah masalah produksi sebaiknya diidentifikasi dan diimplementasikan.
Hal-hal berikut sebaiknya dipertimbangkan:

a) memisahkan sistem pengembangan dan produksi secara cukup dan mengoperasikannya dalam domain yang berbeda (misalnya dalam lingkungan virtual atau fisik yang terpisah);
b) mendefinisikan, mendokumentasikan, dan mengimplementasikan aturan dan otorisasi untuk pengerahan perangkat lunak dari pengembangan ke status produksi;
c) menguji perubahan pada sistem produksi dan aplikasi dalam lingkungan pengujian atau pentahapan sebelum diterapkan pada sistem produksi (lihat 8.29);
d) tidak menguji di lingkungan produksi kecuali dalam keadaan yang telah didefinisikan dan disetujui;
e) kompilator, editor, dan alat pengembangan atau program utilitas lainnya yang tidak dapat diakses dari sistem produksi jika tidak dipersyaratkan;
f) menampilkan label identifikasi lingkungan yang tepat dalam menu untuk mengurangi risiko eror;
g) tidak menyalin informasi sensitif ke dalam lingkungan sistem pengembangan dan pengujian kecuali kontrol ekuivalen disediakan untuk sistem pengembangan dan pengujian .

Dalam semua kasus, lingkungan pengembangan dan pengujian sebaiknya diproteksi dengan mempertimbangkan:

a) menambal dan memperbarui semua alat pengembangan, integrasi, dan pengujian (termasuk pembangun, integrator, kompilator, sistem konfigurasi, dan pustaka);
b) konfigurasi sistem dan perangkat lunak yang aman;
c) kontrol akses ke lingkungan;
d) pemonitoran perubahan lingkungan dan kode yang tersimpan di dalamnya;
e) pemonitoran lingkungan secara aman;
f) membuat pencadangan lingkungan.

Seseorang sebaiknya tidak boleh memiliki kemampuan untuk membuat perubahan pada pengembangan dan produksi tanpa reviu dan persetujuan sebelumnya. Hal ini dapat dicapai misalnya melalui pemisahan hak akses atau melalui aturan yang dimonitor. Dalam situasi luar biasa, langkah langkah tambahan seperti pemebrlakuan log terperinci dan pemonitoran waktu nyata sebaiknya diimplementasikan untuk mendeteksi dan menindak perubahan yang takterotorisasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi lain
Tanpa langkah-langkah dan prosedur yang cukup, developer dan penguji yang memiliki akses ke sistem produksi dapat memunculkan risiko yang signifikan (misalnya modifikasi fail atau lingkungan sistem yang tidak diinginkan, kegagalan sistem, menjalankan kode yang takterotorisasi dan belum teruji dalam sistem produksi, pengungkapan data konfidensial, isu integritas dan availabilitas data). Ada kebutuhan untuk memelihara lingkungan yang dikenal dan stabil sebagai tempat melakukan pengujian yang berarti dan mencegah akses developer yang taktepat ke lingkungan produksi.

Langkah-langkah dan prosedur termasuk peran yang didesain secara hati-hati dalam hubungannya dengan mengimplementasikan segregasi persyaratan tugas dan memiliki proses pemonitoran yang cukup.

Personel pengembangan dan pengujian juga menimbulkan ancaman terhadap konfidensialitas informasi produksi. Kegiatan pengembangan dan pengujian dapat menyebabkan perubahan yang takdisengaja pada perangkat lunak atau informasi jika berbagi lingkungan komputasi yang sama. Pemisahan lingkungan pengembangan, pengujian, dan produksi diinginkan untuk mengurangi risiko perubahan yang tidak disengaja atau akses yang takterotorisasi ke perangkat lunak produksi dan data bisnis (lihat 8.33 untuk proteksi informasi uji).

Dalam beberapa kasus, pebedaan antara lingkungan pengembangan, uji dan produksi dapat dengan sengaja dikaburkan dan pengujian dapat dilakukan di lingkungan pengembangan atau melalui peluncuran terkontrol ke pengguna atau server (misalnya populasi kecil pengguna percontohan). Dalam beberapa kasus, pengujian produk dapat terjadi melalui penggunaan langsung produk di dalam organisasi. Lebih jauh lagi, untuk mengurangi waktu henti pengerahan langsung, dua lingkungan produksi yang identik dapat didukung dengan hanya satu yang aktif pada satu waktu.

Proses pendukung untuk penggunaan data produksi dalam lingkungan pengembangan dan pengujian (8.33) diperlukan.

Organisasi juga dapat mempertimbangkan panduan yang disediakan di bagian ini untuk lingkungan pelatihan saat melakukan pelatihan pengguna akhir.

8.32 Manajemen perubahan

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi

Kontrol
Perubahan fasilitas pemrosesan informasi dan sistem informasi sebaiknya menjadi subyek bagi prosedur manajemen perubahan.

Tujuan
Untuk menjaga keamanan informasi saat melaksanakan perubahan.

Panduan
Pengenalan sistem baru dan perubahan besar pada sistem yang ada sebaiknya mengikuti aturan yang disepakati dan proses formal dokumentasi, spesifikasi, pengujian, pengendalian kualitas, dan implementasi terkelola. Tanggung jawab dan prosedur manajemen sebaiknya

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

ada untuk memastikan kontrol yang memuaskan terhadap semua perubahan.

Prosedur pengendalian perubahan sebaiknya didokumentasikan dan ditegakkan untuk memastikan konfidensialitas, integritas, dan availabilitas informasi di fasilitas pengolahan informasi dan sistem informasi, untuk seluruh siklus hidup pengembangan sistem dari tahap desain awal melalui semua upaya pemeliharaan berikutnya

Jika memungkinkan, prosedur kontrol perubahan untuk infrastruktur dan perangkat lunak TIK sebaiknya terintegrasi.

Prosedur pengendalian perubahan sebaiknya mencakup:
a) merencanakan dan menilai potensi dampak perubahan dengan mempertimbangkan semua ketergantungan;
b) otorisasi perubahan;
c) mengomunikasikan perubahan kepada pihak terkait yang berkepentingan;
d) uji dan penerimaan uji untuk perubahan (lihat 8.29);
e) implementasi perubahan termasuk rencana pengerahan;
f) konsiderasi darurat dan kontingensi termasuk prosedur *fall-back*;
g) memelihara rekaman perubahan yang mencakup semua hal di atas;
h) memastikan bahwa dokumentasi operasi (lihat 5.37) dan prosedur pengguna diubah jika perlu agar tetap tepat;
i) memastikan bahwa rencana kontinuitas TIK dan prosedur respons dan pemulihan (lihat 5.30) diubah jika perlu agar tetap tepat.

Informasi lain
kontrol yang takmemadai atas perubahan fasilitas pemrosesan informasi dan sistem informasi merupakan penyebab umum kegagalan sistem atau keamanan. Perubahan lingkungan produksi, terutama ketika mentransfer perangkat lunak dari lingkungan pengembangan ke operasional, dapat berdampak pada integritas dan availabilitas aplikasi.

Mengubah perangkat lunak dapat berdampak pada lingkungan produksi dan sebaliknya. Praktik yang baik mencakup pengujian komponen TIK dalam lingkungan yang dipisahkan dari lingkungan produksi dan pengembangan (lihat 8.31). Ini menyediakan sarana untuk memiliki kontrol atas perangkat lunak baru dan mengizinkan proteksi tambahan atas informasi operasional yang digunakan untuk tujuan pengujian. Ini sebaiknya mencakup tambalan, pak layanan, dan pembaruan lainnya.

Lingkungan produksi meliputi sistem operasi, pangkalan data dan platform *middleware*. kontrol sebaiknya diterapkan untuk perubahan aplikasi dan infrastruktur.

8.33 Informasi uji

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas	#Memproteksi	#Proteksi_informasi	#Proteksi

Kontrol
Informasi uji sebaiknya dipilih, diproteksi, dan dimanajemeni secara tepat.

Tujuan
Untuk memastikan relevansi pengujian dan proteksi informasi operasional yang digunakan untuk pengujian.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Panduan
Informasi uji sebaiknya dipilih untuk memastikan reliabilitas hasil uji dan konfidensialitas informasi operasional yang relevan. Informasi sensitif (termasuk informasi pengidentifikasi diri) tidak boleh disalin ke lingkungan pengembangan dan pengujian (lihat 8.31)

Pedoman berikut sebaiknya diterapkan untuk memproteksi salinan informasi operasional, ketika digunakan untuk tujuan pengujian, terlepas apakah lingkungan uji dibangun secara internal atau di layanan *cloud*:
a) menerapkan prosedur kontrol akses yang sama untuk lingkungan uji seperti yang diterapkan untuk lingkungan operasional;
b) memiliki otorisasi terpisah setiap kali informasi operasional disalin ke lingkungan uji;
c) membuat log penyalinan dan penggunaan informasi operasional untuk menyediakan jejak audit;
d) memproteksi informasi sensitif dengan pemindahan atau menyamarkannys (lihat 8.11) jika digunakan untuk pengujian;
e) menghapus secara layak (lihat8.10) informasi operasional dari lingkungan uji segera setelah pengujian selesai untuk mencegah penggunaan informasi uji yang takterotorisasi.

Informasi uji sebaiknya disimpan secara aman (untuk mencegah gangguan, yang dapat menyebabkan hasil yang tidak valid) dan hanya digunakan untuk tujuan pengujian.

Informasi lain
Pengujian sistem dan penerimaan mungkin mensyaratkan volume substansial dari informasi uji yang semirip mungkin dengan informasi operasional.

8.34 Proteksi sistem informasi selama pengujian audit

Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan #Proteksi_informasi	#Tata_kelola_dan Ekosistem #Proteksi

Kontrol
Uji audit dan aktivitas keyakinan lainnya yang melibatkan asesmen sistem operasional sebaiknya direncanakan dan disepakati antara penguji dan manajemen yang tepat.

Tujuan
Untuk meminimalkan dampak audit dan aktivitas keyakinan lainnya terhadap sistem operasional dan proses bisnis.

Panduan
Pedomanberikut sebaiknya diamati:
a) menyetujui permintaan audit untuk akses ke sistem dan data dengan manajemen yang tepat;
b) menyetujui dan mengontrol ruang lingkup pengujian audit teknis;
c) membatasi uji audit pada akses hanya-baca ke perangkat lunak dan data. Jika akses hanya-baca tidak tersedia untuk mendapatkan informasi yang diperlukan, melakukan uji oleh administrator berpengalaman yang memiliki hak akses yang diperlukan atas nama auditor;
d) jika akses diberikan, menetapkan dan memverifikasi persyaratan keamanan (misalnya antivirus dan penambalan) dari peranti yang digunakan untuk mengakses sistem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

(misalnya laptop atau tablet) sebelum mengizinkan akses;

e) hanya mengizinkan akses selain hanya-baca untuk salinan fail sistem yang diisolasi, menghapusnya ketika audit selesai, atau memberinya proteksi yang tepat jika ada kewajiban untuk menyimpan fail tersebut berdasarkan persyaratan dokumentasi audit;
f) mengidentifikasi dan menyetujui permintaan untuk pemrosesan khusus atau tambahan, seperti menjalankan alat audit;
g) menjalankan uji audit yang dapat memengaruhi availabilitas sistem di luar jam kerja;
h) memonitor dan *logging* semua akses untuk tujuan audit dan uji.

Informasi lain

uji audit dan aktivitas keyakinan lainnya juga dapat terjadi pada sistem pengembangan dan uji, di mana uji tersebut dapat berdampak pada misalnya integritas kode atau mengarah pada pengungkapan informasi sensitif yang disimpan di lingkungan tersebut.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Lampiran A
(Informatif)
Penggunaan atribut

A.1 Umum

Lampiran ini menyediakan tabel untuk menunjukkan penggunaan atribut sebagai cara untuk membuat pandangan yang berbeda terhadap kontrol. Lima contoh atribut tersebut yaitu (lihat 4.2):

a) Tipe kontrol (#Preventif, #Detektif, #Korektif)
b) Properti keamanan informasi (#Konfidensialitas, #Integritas, #Availabilitas)
c) Konsep keamanan siber (#Mengidentifikasi, #Memproteksi, #Mendeteksi, #Merespons, #Memulihkan)
d) Kemampuan operasional (#Tata_kelola, #Manajemen_aset, #Proteksi_informasi, #Keamanan_SDM, #Keamanan_fisik, #Keamanan_sistem_dan_jaringan, #Keamanan_aplikasi, #Konfigurasi_yang_aman, #Manajemen_identitas_dan_akses, #Manajemen_ancaman_dan_kerentanan, #Kontinuitas, #Keamanan_hubungan_pemasok, #Legal_dan_kepatuhan, #Manajemen_peristiwa_keamanan_informasi, #Jaminan_keamanan_informasi)
e) Domain keamanan (#Tata_kelola_dan_Ekosistem, #Proteksi, #Pertahanan, #Resiliensi)

Tabel A.1 berisi matriks semua kontrol dalam dokumen ini dengan nilai atributnya masing-masing.

Pemfilteran atau penyortiran matriks dapat dicapai dengan menggunakan alat seperti lembar kerja sederhana atau pangkalan data, yang dapat mencakup lebih banyak informasi seperti teks kontrol, panduan, panduan atau atribut spesifik organisasi (lihat A.2).

Tabel A.1 — Matriks kontrol dan nilai atribut

Pengidentifikasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.1	Kebijakan keamanan informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem #Resiliensi
5.2	Peran dan tanggung jawab keamanan informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem #Proteksi #Resiliensi
5.3	Segregasi tugas	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Protek	#Tata_kelola #Manajemen_identitas_dan_akses	#Tata_kelola_dan_Ekosistem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.4	Tanggung jawab manajemen	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Tata_kelola	#Tata_kelola_dan_Ekosistem
5.5	Kontak dengan otoritas	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi #Merespons #Memulihkan	#Tata_kelola	#Pertahanan #Resiliensi
5.6	Kontak dengan kelompok kepentingan khusus	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Protek #Merespons #Memulihkan	#Tata_kelola	#Pertahanan
5.7	Intelijen ancaman	#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Deteksi #Merespons	#Manajemen_ancaman_dan_kerentanan	#Pertahanan #Resiliensi
5.8	Keamanan informasi dalam manajemen proyek	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Protek	#Tata_kelola	#Tata_kelola_dan_Ekosistem #Proteksi
5.9	Inventori informasi dan aset terkait lainnya	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Manajemen_aset	#Tata_kelola_dan_Ekosistem #Proteksi
5.10	Penggunaan yang akseptabel dari informasi dan aset terkait lainnya	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_aset #Proteksi_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Resiliensi
5.11	Pengembalian aset	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_aset	#Proteksi
5.12	Klasifikasi informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Proteksi_informasi	#Proteksi #Pertahanan
5.13	Pelabelan informasi	#Preventif	#Konfidensialitas #Integritas	#Memprotek si	#Proteksi_informasi	#Proteksi #Pertahanan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
			#Availabilitas			
5.14	Transfer informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_ aset #Proteksi_info rmasi	#Proteksi
5.15	Kontrol akses	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
5.16	Manajemen identitas	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
5.17	Informasi autentkasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
5.18	Hak akses	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
5.19	Keamanan informasi dalam hubungan pemasok	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi	#Keamanan_h ubungan_pem asok	#Tata_kelol a_dan_Eko sistem #Proteksi
5.20	Menangani keamanan informasi dalam perjanjian pemasok	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi	#Keamanan_h ubungan_pem asok	#Tata_kelol a_dan_Eko sistem #Proteksi
5.21	Memanajeme ni keamanan informasi dalam rantai pasokan TIK	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi	#Keamanan_h ubungan_pem asok	#Tata_kelol a_dan_Eko sistem #Proteksi
5.22	Pemonitoran, reviu, dan manajemen perubahan layanan pemasok	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi	#Keamanan_h ubungan_pem asok	#Tata_kelol a_dan_Eko sistem #Proteksi #Pertahana n #Jaminan_ keamanan_ informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.23	Keamanan informasi untuk penggunaan layanan *cloud*	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_hubungan_pemasok	#Tata_kelola_dan_Ekosistem #Proteksi
5.24	Perencanaan dan persiapan manajemen insiden keamanan informasi	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons #Memulihkan	#Tata_kelola #Manajemen_kejaidan_keamanan_informasi	#Pertahanan
5.25	Asesmen dan keputusan tentang peristiwa keamanan informasi	#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Deteksi #Merespons	#Manajemen_kejaidan_keamanan_informasi	#Pertahanan
5.26	Respons terhadap insiden keamanan informasi	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons Pemulihan	#Manajemen_kejaidan_keamanan_informasi	#Pertahanan
5.27	Belajar dari insiden keamanan informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Protek	#Manajemen_kejaidan_keamanan_informasi	#Pertahanan
5.28	Pengumpulan bukti	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Deteksi #Merespons	#Manajemen_kejaidan_keamanan_informasi	#Pertahanan
5.29	Gangguan keamanan informasi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si #Merespons	#Kontinuitas	#Proteksi #Resiliensi
5.30	Kesiapan TIK untuk kontinuitas bisnis	#Korektif	#Availabilitas	#Merespons	#Kontinuitas	#Resiliensi
5.31	Persyaratan legal, statutori, regulatori, dan kontraktual	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Legal_dan_kepatuhan	#Tata_kelola_dan_Ekosistem #Proteksi
5.32	Hak kekayaan intelektual	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi	#Legal_dan_kepatuhan	#Tata_kelola_dan_Ekosistem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.33	Proteksi rekaman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	##Legal_dan_kepatuhan #Manajemen_aset #Proteksi_informasi	#Pertahanan
5.34	Privasi dan proteksi PII	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Proteksi_informasi #Legal_dan_kepatuhan	#Proteksi
5.35	Reviu independen terhadap keamanan informasi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Jaminan_keamanan_informasi	#Tata_kelola_dan_Ekosistem
5.36	Kepatuhan terhadap kebijakan, aturan, dan standar informasi keamanan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Legal_dan_kepatuhan #Jaminan_keamanan_informasi	#Tata_kelola_dan_Ekosistem
5.37	Prosedur operasi terdokumentasi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Memulihkan	#Manajemen_aset #Keamanan_fisik #Keamanan_sistem_adn_jaringan #Keamaman_aplikasi #Konfigurasi_yang_aman #Manajemen_identitas_dan_akses #Manajemen_ancaman_dan_kerentanan #Kontinuitas #Manajemen_peristiwa_keamanan_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Resiliensi
6.1	Skrining	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
6.2	Syarat dan ketentuan ketenagakerjaan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ SDM	#Tata_kelol a_dan_Eko sistem
6.3	Kesadaran, pendidikan, dan pelatihan keamanan informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ SDM	#Tata_kelol a_dan_Eko sistem
6.4	Poses kedisiplinan	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si #Merespons	#Keamanan_ SDM	#Tata_kelol a_dan_Eko sistem
6.5	Tanggung jawab setelah terminasi atau perubahan pekerjaan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ SDM #Manajemen_ aset	#Tata_kelol a_dan_Eko sistem
6.6	Perjanjian konfidensialitas atau nirungkap	#Preventif	#Konfidensialitas	#Memprotek si	#Keamanan_ SDM #Memproteksi_informasi #Hubungan_pemasok	#Tata_kelol a_dan_Eko sistem
6.7	Telekarya (*Remote Working*)	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_ aset #Proteksi_informasi #Keamanan_fisik #Keamaann_sistem_dan_jaringan	#Proteksi
6.8	Pelaporan peristiwa keamanan informasi	#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi	#Tata_kelola #Manajemen_peristiwa_keamanan_informasi	#Pertahanan
7.1	Perimeter keamanan fisik	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_fisik	#Proteksi
7.2	Entri Fisik	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_fisik #Manajemen_identitas_dan_akses	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
7.3	Mengamankan kantor, ruangan, dan fasilitas	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi
7.4	Pemonitoran keamanan fisik	#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_fisik	#Proteksi #Pertahanan
7.5	Memproteksi terhadap ancaman fisik dan lingkungan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi
7.6	Bekerja di area aman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi
7.7	Meja bersih dan layar bersih	#Preventif	#Konfidensialitas	#Memproteksi	#Keamanan_fisik	#Proteksi
7.8	Penempatan dan proteksi peralatan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi
7.9	Keamanan aset di luar premis	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi
7.10	Media penyimpanan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi
7.11	Utilitas pendukung	#Preventif #Detektif	#Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_fisik	#Proteksi
7.12	Keamanan perkabelan	#Preventif	#Konfidensialitas #Availabilitas	#Memproteksi	#Keamanan_fisik	#Proteksi
7.13	Pemeliharaan peralatan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi #Resiliensi
7.14	Penghapusan atau penggunaan kembali peralatan dengan aman	#Preventif	#Konfidensialitas	#Memproteksi	#Keamanan_fisik #Manajemen_aset	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
8.1	Perangkat titik akhir pengguna	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_ aset #Proteksi_info rmasi	#Proteksi
8.2	Hak akses privilese	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
8.3	Pembatasan akses informasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
8.4	Akses ke kode sumber	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses #Keamanan_a plikasi #Manajemen_ konfigurasi_ya ng_aman	#Proteksi
8.5	Autentikasi aman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Manajemen_i dentitas_dan_ akses	#Proteksi
8.6	Manajemen kapasitas	#Preventif #Detektif	#Integritas #Availabilitas	#Mengidentif ikasi #Memprotek si #Mendeteksi	#Kontinuitas	#Tata_kelol a_dan_Eko sistem #Proteksi
8.7	Proteksi terhadap perangkat perusak	#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si#Mendetek si	#Keamanan_s istem_dan_jari ngan #Proteksi_info rmasi	#Proteksi #Pertahana n
8.8	Manajemen kerentanan teknis	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi #Memprotek si	#Manajemen_ ancaman_dan _kerentanan	#Tata_kelol a_dan_Eko sistem #Proteksi #Pertahana n
8.9	Manajemen konfigurasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Konfigurasi_ yang_aman	#Proteksi
8.10	Penghapusan informasi	#Preventif	#Konfidensialitas	#Memprotek si	#Proteksi_nfor masi #Legal_dan_k epatuhan	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
8.11	Penyamaran (*masking*) data	#Preventif	#Konfidensialitas	#Memprotek si	#Proteksi_info rmasi	#Proteksi
8.12	Pencegahan kebocoran data	#Preventif #Detektif	#Konfidensialitas	#Memprotek si #Mendeteksi	#Proteksi_info rmasi	#Proteksi #Pertahana n
8.13	Pencadanga n informasi	#Korektif	#Integritas #Availabilitas	#Memulihka n	#Kontinuitas	#Proteksi
8.14	Redundansi fasilitas pemrosesan informasi	#Preventif	#Availabilitas	#Memprotek si	#Kontinuitas #Manajemen_ aset	#Proteksi #Resiliensi
8.15	Membuat log	#Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi	#Manajemen_ peristiwa_kea manan_infor masi	#Proteksi #Pertahana n
8.16	pemonitoran aktivitas	#Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi #Merespons	#Manajemen_ peristiwa_kea manan_infor masi	#Pertahana n
8.17	Sinkronisasi jam	#Detektif	#Integritas	#Memprotek si #Mendeteksi	#Manajemen_ peristiwa_kea manan_infor masi	#Proteksi #Pertahana n
8.18	Penggunaan program utilitas privilese	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ sistem_dan_j aringan #Konfigurasi_ yang_aman #Keamanan_ aplikasi	#Proteksi
8.19	Instalasi perangkat lunak pada sistem operasional	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Konfigurasi_ yang_aman #Keamanan_ aplikasi	#Proteksi
8.20	Keamanan jaringan	#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si #Mendeteksi	#Keamanan_ sistem_dan_j aringan	#Proteksi
8.21	Keamanan layanan jaringan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ sistem_dan_j aringan	#Proteksi
8.22	Segregasi jaringan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ sistem_dan_j aringan	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
8.23	Pemfilteran web	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ sistem_dan_j aringan	#Proteksi
8.24	Penggunaan kriptografi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Konfigurasi_ yang_aman	#Proteksi
8.25	Siklus hidup pengembanga n yang aman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ aplikasi #Keamanan_ sistem_dan_j aringan	#Proteksi
.26	Persyaratan keamanan aplikasi	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ aplikasi #Keamanan_ sistem_dan_j aringan	#Proteksi #Pertahana n
8.27	Prinsip-prinsip arsitektur dan rekayasa sistem yang aman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ aplikasi #Keamanan_ sistem_dan_j aringan	#Proteksi
8.28	Pengkodean yang aman	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ aplikasi #Keamanan_ sistem_dan_j aringan	#Proteksi
8.29	Pengujian keamanan dalam pengembang an dan penerimaan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi	#Keamanan_ aplikasi #Jaminan_ke amanan_infor masi #Keamanan_ sistem_dan_j aringan	#Proteksi
8.30	Pengembang an yang dialihdayakan	#Preventif #Detektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentif ikasi #Memprotek si #Mendeteksi	#Keamanan_ sistem_dan_j aringan #Keamanan_ aplikasi #Keamanan_ hubungan_pe masok	#Tata_kelol a_dan_Eko sistem #Proteksi
8.31	Pemisahan lingkungan pengembang an,	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memprotek si	#Keamanan_ aplikasi #Keamanan_ sistem_dan_j	#Proteksi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifi-kasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
	pengujian, dan produksi				aringan	
8.32	Manajemen perubahan	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_aplikasi #Keamanan_sistem_dan_jaringan	#Proteksi
8.33	Informasi pengujian	#Preventif	#Konfidensialitas #Integritas	#Memproteksi	#Proteksi_informasi	#Proteksi
8.34	Proteksi sistem informasi selama audit pengujian	#Preventif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi	#Keamanan_sistem_dan_jaringan #Proteksi_informasi	#Tata_kelola_dan_Ekosistem #Proteksi

Tabel A.2 menunjukkan contoh cara membuat pandangan dengan memfilter berdasarkan nilai atribut tertentu, dalam hal ini #Korektif.

Tabel A.2 — Tampilan kontrol #Korektif

Pengidentifikasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.5	Kontak dengan otoritas	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi #Merespons #Memulihkan	#Tata_kelola	#Pertahanan #Resiliensi
5.6	Kontak dengan kelompok kepentingan khusus	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons #Memulihkan	#Tata_kelola	#Pertahanan
5.7	Intelijen ancaman	#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Mendeteksi #Merespons	#Manajemen_ancaman_dan_kerentanan	#Pertahanan #Resiliensi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifikasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
5.24	Perencanaan dan persiapan manajemen insiden keamanan informasi	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons #Memulihkan	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan
5.26	Respons terhadap insiden keamanan informasi	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Merespons #Memulihkan	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan
5.28	Pengumpulan bukti	#Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi #Merespons	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan
5.29	Keamanan informasi selama disrupsi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons	#Kontinuitas	#Proteksi #Resiliensi
5.30	Kesiapan TIK untuk kontinuitas bisnis	#Korektif	#Availabilitas	#Merespons	#Kontinuitas	#Resiliensi
5.35	Reviu independen terhadap keamanan informasi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mengidentifikasi #Memproteksi	#Jaminan_keamanan_informasi	#Tata_kelola_dan_Ekosistem
5.37	Prosedur operasi terdokumentasi	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Memulihkan	#Manajemen_aset #Keamanan_fisik #Keamanan_sistem_dan_jaringan #Keamanan_aplikasi #Konfigurasi_yang_aman #Manajemen_identitas_dan_aakses #Manajemen_ancaman_dan_kerentanan #Kontinuitas #Manajemen_peristiwa_keamanan_informasi	#Tata_kelola_dan_Ekosistem #Proteksi #Pertahanan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Pengidentifikasi kontrol ISO/ IEC 27002	Nama kontrol	Tipe kontrol	Properti keamanan informasi	Konsep keamanan siber	Kemampuan operasional	Domain keamanan
6.4	Proses kedisiplinan	#Preventif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Merespons	#Keamanan_SDM	#Tata_kelola_dan_Ekosistem
8.7	Proteksi terhadap perangkat perusak	#Preventif #Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Memproteksi #Mendeteksi	#Keamanan_sistem_dan_jaringan #Proteksi_informasi	#Proteksi #Pertahanan
8.13	Pencadangan informasi	#Korektif	#Integritas #Availabilitas	#Memulihkan	#Kontinuitas	#Proteksi
8.16	Pemonitoran aktivitas	#Detektif #Korektif	#Konfidensialitas #Integritas #Availabilitas	#Mendeteksi #Merespons	#Manajemen_peristiwa_keamanan_informasi	#Pertahanan

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

A.2 Pandangan organisasi

Karena atribut digunakan untuk membuat berbagai pandangan kontrol yang berbeda, organisasi dapat membuang contoh atribut yang diusulkan dalam dokumen ini dan membuat atributnya sendiri dengan nilai yang berbeda untuk mengatasi kebutuhan tertentu dalam organisasi. Selain itu, nilai-nilai yang ditetapkan untuk setiap atribut dapat berbeda antara berbagai organisasi karena organisasi dapat memiliki pandangan yang berbeda tentang penggunaan atau penerapan kontrol atau nilai-nilai yang terkait dengan atribut tersebut (ketika nilai-nilai tersebut spesifik untuk konteks organisasi). Langkah pertama adalah memahami mengapa atribut spesifik organisasi diperlukan. Misalnya, jika suatu organisasi telah menyusun rencana penanganan risikonya [lihat ISO/IEC 27001:2013, 6.1.3 e)] berdasarkan peristiwa, organisasi dapat mengaitkan skenario risiko dengan setiap kontrol dalam dokumen ini.

Keuntungan dari atribut tersebut adalah untuk mempercepat proses pemenuhan persyaratan ISO/IEC 27001 yang terkait dengan penanganan risiko, yaitu untuk membandingkan kontrol yang ditentukan melalui proses perlakuan risiko (disebut sebagai kontrol "yang diperlukan"), dengan yang ada di ISO/IEC 27001:2013, Lampiran A (yang diuraikan ke dalam dokumen ini) untuk memastikan bahwa tidak ada kontrol yang diperlukan yang terabaikan.

Setelah diketahui tujuan dan manfaatnya, langkah selanjutnya adalah menentukan nilai atribut. Misalnya, organisasi dapat mengidentifikasi 9 peristiwa:

1) kehilangan atau pencurian peranti mobil;
2) kehilangan atau pencurian dari premis organisasi;
3) keadaan kahar, vandalisme, dan terorisme;
4) kegagalan perangkat lunak, perangkat keras, daya, internet, dan komunikasi;
5) penipuan,
6) peretasan;
7) pengungkapan.
8) pelanggaran hukum;
9) rekayasa sosial.

Oleh karena itu, langkah kedua dapat dicapai dengan menetapkan pengidentifikasi untuk setiap peristiwa (misalnya E1, E2, ..., E9).

Langkah ketiga adalah menyalin pengidentifikasi kontrol dan nama kontrol dari dokumen ini ke dalam lembar kerja atau pangkalan data dan mengaitkan nilai atribut dengan setiap kontrol, mengingat bahwa setiap kontrol dapat memiliki lebih dari satu nilai atribut.

Langkah terakhir adalah mengurutkan lembar kerja atau melakukan kueri pangkalan data untuk mengekstrak informasi yang diperlukan. Contoh lain dari atribut organisasi (dan nilai-nilai yang mungkin) termasuk:

a) maturitas (nilai dari seri ISO/IEC 33000 atau model maturitas lainnya);
b) kondisi implementasi (akan dilaksanakan, dalam progres, terimplementasi parsial, terimplementasi seluruhnya);
c) prioritas (1, 2, 3, dst);
d) area organisasi yang terlibat (keamanan, TIK, sumber daya manusia, manajemen puncak, dll.);
e) peristiwa
f) aset yang terlibat;
g) bangun dan jalankan, untuk membedakan kontrol yang digunakan dalam langkah-langkah yang berbeda dari siklus hidup layanan;
h) kerangka kerja lain yang digunakan organisasi atau yang akan beralih dari kerangka kerja itu.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Lampiran B
(informatif)
Padanan ISO/IEC 27002:2022 (dokumen ini) dengan ISO/IEC 27002:2013

Tujuan dari lampiran ini adalah untuk memberikan kompatibilitas balik dengan ISO/IEC 27002:2013 untuk organisasi yang saat ini menggunakan standar tersebut dan sekarang ingin beralih ke edisi ini.

Tabel B.1 menyediakan padanan kontrol yang ditentukan dalam Pasal 5 hingga 8 dengan yang ada di ISO/IEC 27002:2013.

Tabel B.1 — Padanan antara kontrol dalam dokumen ini dan kontrol dalam ISO/IEC 27002:2013

Pengidentifikasi kontrol ISO/IEC 27002: 2022	Pengidentifikasi kontrol ISO/IEC 27002:2013	Nama kontrol
5.1	05.1.1, 05.1.2	Kebijakan untuk keamanan informasi
5.2	06.1.1	Peran dan tanggung jawab keamanan informasi
5.3	06.1.2	Segregasi tugas
5.4	07.2.1	Tanggung jawab manajemen
5.5	06.1.3	Kontak dengan otoritas
5.6	06.1.4	Kontak dengan kelompok kepentingan khusus
5.7	Baru	Intelijen ancaman
5.8	06.1.5, 14.1.1	Keamanan informasi dalam manajemen proyek
5.9	08.1.1, 08.1.2	Inventarisasi informasi dan aset terkait lainnya
5.10	08.1.3, 08.2.3	Penggunaan informasi yang akseptabel dan aset terkait lainnya
5.11	08.1.4	Pengembalian aset
5.12	08.2.1	Klasifikasi informasi
5.13	08.2.2	Pelabelan informasi
5.14	13.2.1, 13.2.2, 13.2.3	Transfer informasi
5.15	09.1.1, 09.1.2	Kontrol akses
5.16	09.2.1	Manajemen identitas
5.17	09.2.4, 09.3.1, 09.4.3	Informasi autentikasi
5.18	09.2.2, 09.2.5, 09.2.6	Hak akses
5.19	15.1.1	Keamanan informasi dalam hubungan pemasok
5.20	15.1.2	Menangani keamanan informasi dalam perjanjian pemasok
5.21	15.1.3	Memanajemeni keamanan informasi dalam rantai pasokan TIK
5.22	15.2.1, 15.2.2	Pemonitoran, reviu, dan manajemen perubahan layanan pemasok
5.23	Baru	Keamanan informasi untuk penggunaan layanan *cloud*

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.1 (*lanjutan)*

Pengidentifikasi kontrol ISO/IEC 27002: 2022	Pengidentifikasi kontrol ISO/IEC 27002:2013	Nama kontrol
5.24	16.1.1	Perencanaan dan persiapan manajemen insiden keamanan informasi
5.25	16.1.4	Asesmen dan keputusan tentang keamanan peristiwa informasi
5.26	16.1.5	Respons terhadap insiden keamanan informasi
5.27	16.1.6	Belajar dari insiden keamanan informasi
5.28	16.1.7	Pengumpulan bukti
5.29	17.1.1, 17.1.2, 17.1.3	Keamanan informasi selama disrupsi
5.30	Baru	Kesiapan TIK untuk kontinuitas bisnis
5.31	18.1.1, 18.1.5	Persyaratan legal, statutori, regulatori, dan kontraktual
5.32	18.1.2	Hak kekayaan intelektual
5.33	18.1.3	Proteksi rekaman
5.34	18.1.4	Privasi dan proteksi PII
5.35	18.2.1	Reviu independen terhadap keamanan informasi
5.36	18.2.2, 18.2.3	Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi
5.37	12.1.1	Prosedur operasi terdokumentasi
6.1	07.1.1	Skrining
6.2	07.1.2	Syarat dan ketentuan ketenagakerjaan
6.3	07.2.2	Kesadaran, pendidikan dan pelatihan keamanan informasi
6.4	07.2.3	Proses kedisiplinan
6.5	07.3.1	Tanggung jawab setelah terminasi atau perubahan pekerjaan
6.6	13.2.4	Perjanjian konfidensialitas atau nirungkap
6.7	06.2.2	Telekarya (*remote working*)
6.8	16.1.2, 16.1.3	Pelaporan peristiwa keamanan informasi
7.1	11.1.1	Perimeter kamanan fisik
7.2	11.1.2, 11.1.6	Entri fisik
7.3	11.1.3	Mengamankan kantor, ruangan, dan fasilitas
7.4	Baru	Pemonitoran keamanan fisik
7.5	11.1.4	Memproteksi dari ancaman fisik dan lingkungan
7.6	11.1.5	Bekerja di area yang aman
7.7	11.2.9	Meja bersih dan layar bersih
7.8	11.2.1	Penempatan dan proteksi peralatn
7.9	11.2.6	Keamanan aset di luar premis
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Media penyimpanan
7.11	11.2.2.	Utilitas pendukung
7.12	11.2.3	Keamanan perkabelan
7.13	11.2.4	Pemeliharaan peralatan
7.14	11.2.7	Pemusnahan atau penggunaan kembali peralatan dengan aman

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.1 (*lanjutan)*

Pengidentifikasi kontrol ISO/IEC 27002: 2022	Pengidentifikasi kontrol ISO/IEC 27002:2013	Nama kontrol
8.1	06.2.1, 11.2.8	Perangkat titik akhir pengguna
8.2	09.2.3	Hak akses privilese
8.3	09.4.1	Pembatasan akses informasi
8.4	09.4.5	Akses ke kode sumber
8.5	09.4.2	Autentikasi aman
8.6	12.1.3	Manajemen kapasitas
8.7	12.2.1	Proteksi terhadap perangkat perusak
8.8	12.6.1, 18.2.3	Manajemen kerentanan teknis
8.9	Baru	Manajemen konfigurasi
8.10	Baru	Penghapusan informasi
8.11	Baru	Penyamaran (*masking*) data
8.12	Baru	Pencegahan kebocoran data
8.13	12.3.1	Pencadangan informasi
8.14	17.2.1	Redundansi fasilitas pemrosesan informasi
8.15	12.4.1, 12.4.2, 12.4.3	Membuat log
8.16	Baru	Pemonitoran aktivitas
8.17	12.4.4	Sinkronisasi jam
8.18	09.4.4	Penggunaan program utilitas privilese
8.19	12.5.1, 12.6.2	Instalasi perangkat lunak pada sistem operasional
8.20	13.1.1	Keamanan jaringan
8.21	13.1.2	Keamanan layanan jaringan
8.22	13.1.3	Segregasi jaringan
8.23	Baru	Pemfilteran web
8.24	10.1.1, 10.1.2	Penggunaan kriptografi
8.25	14.2.1	Siklus hidup pengembangan yang aman
8.26	14.1.2, 14.1.3	Persyaratan keamanan aplikasi
8.27	14.2.5	Prinsip-prinsip arsitektur dan rekayasa sistem yang aman
8.28	Baru	Pengkodean yang aman
8.29	14.2.8, 14.2.9	Pengujian keamanan dalam pengembangan dan penerimaan
8.30	14.2.7	Pengembangan yang dialihdayakan
8.31	12.1.4, 14.2.6	Pemisahan lingkungan pengembangan, uji, dan produksi
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Manajemen perubahan
8.33	14.3.1	Informasi uji
8.34	12.7.1	Proteksi sistem informasi selama pengujian audit

Tabel B.2 menyediakan padanan kontrol yang ditentukan dalam ISO/IEC 27002:2013 dengan yang ada di dokumen ini.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.2 — Padanan antara kontrol dalam ISO/IEC 27002:2013 dan kontrol dalam dokumen ini

Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002:2022	Nama kontrol menurut ISO/IEC 27002:2013
5		Kebijakan keamanan informasi
5.1		Arah manajemen untuk keamanan informasi
5.1.1	5.1	Kebijakan untuk keamanan informasi
5.1.2	5.1	Tinjauan kebijakan untuk keamanan informasi
6		Organisasi keamanan informasi
6.1		Organisasi internal
6.1.1	5.2	Peran keamanan dan tanggung jawab informasi
6.1.2	5.3	Pemisahan tugas
6.1.3	5.5	Kontak dengan pihak berwenang
6.1.4	5.6	Kontak dengan kelompok kepentingan khusus
6.1.5	5.8	Keamanan informasi dalam proyek manajemen
6.2		Perangkat seluler dan *teleworking*
6.2.1	8.1	Kebijakan peranti seluler
6.2.2	6.7	*Teleworking*
7		Keamanan sumber daya manusia
7.1		Sebelum perekrutan
7.1.1	6.1	Seleksi
7.1.2	6.2	Syarat dan ketentuan ketenagakerjaan
7.2		Selama bekerja
7.2.1	5.4	Manajemen tanggung jawab
7.2.2	6.3	Kesadaran, pendidikan dan pelatihan keamanan informasi
7.2.3	6.4	Proses disiplin
7.3		Pemutusan hubungan kerja dan perubahan pekerjaan
7.3.1	6.5	Tanggung jawab setelah pemutusan hubungan kerja atau perubahan pekerjaan
8		Manajemen aset;
8.1		Tanggung jawab atas aset
8.1.1	5.9	Inventarisasi aset
8.1.2	5.9	Kepemilikan aset
8.1.3	5.10	Penggunaan aset yang berterima
8.1.4	5.11	Pengembalian aset;
8.2		Klasifikasi informasi
8.2.1	5.12	Klasifikasi informasi
8.2.2	5.13	Pelabelan informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.2 (*lanjutan*)

Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002:2022	Nama kontrol menurut ISO/IEC 27002:2013
8.2.3	5.10	Penanganan aset
8.3		Penanganan media
8.3.1	7.10	Pengelolaan media yang dapat dipindahkan
8.3.2	7.10	Pembuangan media
8.3.3	7.10	Transfer media fisik
9		Kontrol akses
9.1		Persyaratan bisnis kontrol akses
9.1.1	5.15	Kebijakan kontrol akses
9.1.2	5.15	Akses ke jaringan dan layanan jaringan
9.2		Manajemen akses pengguna
9.2.1	5.16	Registrasi dan deregistrasi pengguna
9.2.2	5.18	Penyediaan akses pengguna
9.2.3	8.2	Pengelolaan hak akses istimewa
9.2.4	5.17	Pengelolaan informasi autentikasi konfidensial pengguna
9.2.5	5.18	Tinjauan hak akses pengguna
9.2.6	5.18	Penghapusan atau penyesuaian hak akses
9.3		Tanggung jawab pengguna
9.3.1	5.17	Penggunaan informasi autentikasi konfidensial
9.4		kontrol akses sistem dan aplikasi
9.4.1	8.3	Pembatasan akses informasi
9.4.2	8.5	Prosedur masuk yang aman
9.4.3	5.17	Sistem manajemen kata sandi
9.4.4	8.18	Penggunaan program utilitas istimewa
9.4.5	8.4	kontrol akses ke kode sumber program
10		Kriptografi
10.1		kontrol kriptografi
10.1.1	8.24	Kebijakan tentang penggunaan kontrol kriptografi
10.1.2	8.24	Manajemen kunci
11		Keamanan fisik dan lingkungan
11.1		Area aman
11.1.1	7.1	Perimeter keamanan fisik
11.1.2	7.2	Kontrol entri fisik
11.1.3	7.3	Mengamankan kantor, ruangan, dan fasilitas
11.1.4	7.5	Melindungi dari ancaman eksternal dan lingkungan
11.1.5	7.6	Bekerja di area yang aman
11.1.6	7.2	Area pengiriman dan pemuatan
11.2		Peralatan
11.2.1	7.8	Penempatan dan proteksi peralatan
11.2.2	7.11	Utilitas pendukung

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.2 (*lanjutan*)

Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013
11.2.3	7.12	Keamanan pengkabelan
11.2.4	7.13	Pemeliharaan peralatan
11.2.5	7.10	Penghapusan aset
11.2.6	7.9	Keamanan peralatan dan aset di luar lokasi
11.2.7	7.14	Penghapusan atau penggunaan kembali peralatan secara aman
11.2.8	8.1	Peralatan pengguna yang tidak diawasi
11.2.9	7.7	Meja bersih dan layar bersih
12		Keamanan operasi
12.1		Prosedur dan tanggung jawab operasional
12.1.1	5.37	Prosedur operasi terdokumentasi
12.1.2	8.32	Manajemen perubahan
12.1.3	8.6	Manajemen kapasitas
12.1.4	8.31	Pemisahan lingkungan pengembangan, pengujian dan produksi
12.2		Proteksi dari *malware*
12.2.1	8.7	kontrol terhadap *malware*
12.3		Pencadangan
12.3.1	8.13	Pencadangan informasi
12.4		Melakukan log dan pemonitoran
12.4.1	8.15	Melakukan log peristiwa
12.4.2	8.15	Proteksi informasi log
12.4.3	8.15	Log administrator dan operator
12.4.4	8.17	Sinkronisasi jam
12.5		Pengendalian perangkat lunak operasional
12.5.1	8.19	Instalasi perangkat lunak pada sistem operasi
12.6		Manajemen kerentanan teknis
12.6.1	8.8	Manajemen kerentanan teknis
12.6.2	8.19	Pembatasan pada instalasi perangkat lunak
12.7		Konsiderasi audit sistem informasi
12.7.1	8.34	Pengendalian audit sistem informasi
13		Keamanan komunikasi
13.1		Fasilitas manajemen keamanan jaringan
13.1.1	8.20	kontrol jaringan
13.1.2	8.21	Keamanan layanan jaringan
13.1.3	8.22	Pemisahan jaringan
13.2		Transfer information
13.2.1	5.14	Kebijakan dan prosedur transfer informasi
13.2.2	5.14	Perjanjian tentang transfer informasi
13.2.3	5.14	Pesan elektronik
13.2.4	6.6	Perjanjian konfidensialitas atau nonpengungkapan
14		Akuisisi, pengembangan, dan pemeliharaan sistem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.2 (*lanjutan*)

Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013
14.1		Persyaratan keamanan sistem informasi
14.1.1	5.8	Analisis dan spesifikasi persyaratan keamanan informasi
14.1.2	8.26	Mengamankan layanan aplikasi di jaringan publik
14.1.3	8.26	Melindungi transaksi layanan aplikasi
14.2		Keamanan dalam proses pengembangan dan dukungan
14.2.1	8.25	Kebijakan pengembangan yang aman
14.2.2	8.32	Prosedur pengendalian perubahan sistem
14.2.3	8.32	Tinjauan teknis aplikasi setelah perubahan platform operasi
14.2.4	8.32	Pembatasan pada perubahan paket perangkat lunak
14.2.5	8.27	Prinsip rekayasa sistem yang aman
14.2.6	8.31	Lingkungan pengembangan yang aman
14.2.7	8.30	Pengembangan yang dialihdayakan
14.2.8	8.29	Pengujian keamanan sistem
14.2.9	8.29	Pengujian penerimaan sistem
14.3		Data pengujian
14.3.1	8.33	Proteksi data pengujian
15		Hubungan dengan Vendor
15.1		Keamanan informasi dalam hubungan pemasok
15.1.1	5.19	Kebijakan keamanan informasi untuk hubungan pemasok
15.1.2	5.20	Mengatasi keamanan informasi dalam pemasok
15.1.3	5.21	Rantai pasokan teknologi informasi dan komunikasi
15.2		Manajemen pengiriman layanan pemasok
15.2.1	5.22	Pemonitorandan tinjauan layanan pemasok
15.2.2	5.22	Memanajemeni perubahan pada layanan pemasok
16		Manajemen insiden keamanan informasi
16.1		Manajemen insiden dan peningkatan keamanan informasi
16.1.1	5.24	Tanggung jawab dan prosedur
16.1.2	6.8	Pelaporan peristiwa keamanan informasi
16.1.3	6.8	Pelaporan kelemahan keamanan informasi
16.1.4	5.25	Asesmen dan keputusan tentang peristiwa keamanan informasi
16.1.5	5.26	Respons terhadap insiden keamanan informasi
16.1.6	5.27	Belajar dari insiden keamanan informasi
16.1.7	5.28	Pengumpulan bukti
17		Aspek keamanan informasi dari manajemen kontinuitas bisnis
17.1		Kelangsungan keamanan informasi
17.1.1	5.29	Merencanakan kontinuitas keamanan informasi

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Tabel B.2 (*lanjutan*)

Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013	Pengidentifikasi kontrol ISO/IEC 27002: 2013
17.1.2	5.29	Menerapkan kontinuitas keamanan informasi
17.1.3	5.29	Verifikasi, tinjauan, dan evaluasi kontinuitas keamanan informasi
17.2		Redundansi
17.2.1	8.14	Ketresediaan fasilitas pengolahan informasi
18		Kepatuhan
18.1		Kepatuhan terhadap persyaratan hukum dan kontrak
18.1.1	5.31	Identifikasi peraturan perundang-undangan dan persyaratan kontrak yang berlaku
18.1.2	5.32	Hak kekayaan intelektual
18.1.3	5.33	Proteksi rekaman
18.1.4	5.34	Privasi dan proteksi informasi pengidentifikasi diri
18.1.5	5.31	Aturan kontrol kriptografi
18.2		Tinjauan keamanan informasi
18.2.1	5.35	Tinjauan independen terhadap keamana informasi
18.2.2	5.36	Kepatuhan terhadap kebijakan, aturan, dan standar keamanan informasi
18.2.3	5.36, 8.8	Tinjauan kepatuhan teknis

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Bibliografi

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
[2] ISO 55001, *Asset management — Management systems — Requirements*
[3] ISO/IEC 11770 (seluruh bagian), *Information security — Key management*
[4] ISO/IEC 15408 (seluruh bagian), *Information technology — Security techniques — Evaluation criteria for IT security*
[5] ISO 15489 (seluruh bagian), *Information and documentation — Records management*
[6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
[7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
[8] ISO/IEC 19086 (seluruh bagian), *Cloud computing — Service level agreement (SLA) framework*
[9] ISO/IEC 19770 (seluruh bagian), *Information technology — IT asset management*
[10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
[11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
[12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
[13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
[14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
[15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
[16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
[17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
[18] ISO/IEC TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
[19] ISO/IEC 23751:—[2)], *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
[20] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*
[21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
[22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
[23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
[24] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*

[2)] Dalam penyusunan. Stage at the time of publication: ISO/IEC PRF 23751:2022.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

[25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*
[26] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
[27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
[28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
[29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
[30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*
[31] ISO/IEC 27033 (seluruh bagian), *Information technology — Security techniques — Network security*
[32] ISO/IEC 27034 (seluruh bagian), *Information technology — Application security*
[33] ISO/IEC 27035 (seluruh bagian), *Information technology — Security techniques — Information security incident management*
[34] ISO/IEC 27036 (seluruh bagian), *Information technology — Security techniques — Information security for supplier relationships*
[35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
[36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
[37] ISO/IEC 27050 (seluruh bagian), *Information technology — Electronic discovery*
[38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
[39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
[40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
[41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
[42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
[43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impact assessment*
[44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
[45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
[46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
[47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
[48] ISO 31000:2018, *Risk management — Guidelines*
[49] IEC 31010, *Risk management — Risk assessment techniques*
[50] ISO/IEC 22123 (seluruh bagian), *Information technology — Cloud computing*
[51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*
[52] Information Security Forum (ISF). The ISF Standard of Good Practice for Information Security 2020, Agustus 2018. Tersedia di https: /www.securityforum.org/tool/standard-of -good-practice-for-information-security-2020/
[53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

[54] National Institute of Standards and Technology (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. Desember 2018 [dilihat 2020-07-31]. Tersedia https://doi.org/10.6028/NIST.SP.800-37r2

[55] Open Web Application Security Project (OWASP). OWASP Top Ten - 2017, The Ten Most Critical Web Application Security Risks, 2017 [dilihat 2020-07-31]. Tersedia di https://owasp .org/www-project-top-ten/OWASP_Top_Ten_2017/

[56] Open Web Application Security Project (OWASP). OWASP Developer Guide, [daring] [dilihat 2020-10-22]. Tersedia di https://github.com/OWASP/DevGuide

[57] National Institute of Standards and Technology (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. Februari 2020 [dilihat 2020-07-31]. Tersedia https://doi.org/10.6028/NIST.SP.800-63b

[58] OASIS, Structured Threat Information Expression. Tersedia di https://www.oasis-open.org/standards#stix2.0

[59] OASIS, Trusted Automated Exchange of Indicator Information. Tersedia di https://www.oasis-open.org/standards#taxii2

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Information security, cybersecurity and privacyprotection — Information security controls

1 Scope

This document provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

a) within the context of an information security management system (ISMS) based on ISO/IEC 27001;
b) for implementing information security controls based on internationally recognized best practices;
c) for developing organization-specific information security management guidelines.

2 Normative references

There are no normative references in this document.

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.
ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp
— IEC Electropedia: available at https://www.electropedia.org/

3.1.1 access control

means to ensure that physical and logical access to *assets* (3.1.2) is authorized and restricted based on business and information security requirements

3.1.2 asset

anything that has value to the organization
Note 1 to entry: In the context of information security, two kinds of assets can be distinguished:

— the primary assets:
  — information;
  — business *processes* (3.1.27) and activities;
— the supporting assets (on which the primary assets rely) of all types, for example:
  — hardware;
  — software;
  — network;
  — *personnel* (3.1.20);
  — site;
  — organization's structure.

3.1.3 attack

successful or unsuccessful unauthorized attempt to destroy, alter, disable, gain access to an *asset* (3.1.2) or any attempt to expose, steal, or make unauthorized use of an *asset* (3.1.2)

3.1.4 authentication

provision of assurance that a claimed characteristic of an *entity* (3.1.11) is correct

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3.1.5 authenticity
property that an *entity* (3.1.11) is what it claims to be

3.1.6 chain of custody
demonstrable possession, movement, handling and location of material from one point in time until another Note 1 to entry: Material includes information and other associated *assets* (3.1.2) in the context of ISO/IEC 27002.

[SOURCE: ISO/IEC 27050-1:2019, 3.1, modified — “Note 1 to entry” added]

3.1.7 confidential information
information that is not intended to be made available or disclosed to unauthorized individuals, *entities* (3.1.11) or *processes* (3.1.27)

3.1.8 control
measure that maintains and/or modifies risk Note 1 to entry: Controls include, but are not limited to, any *process* (3.1.27), *policy* (3.1.24), device, practice or other conditions and/or actions which maintain and/or modify risk.

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO 31000:2018, 3.8]

3.1.9 disruption
incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization’s objectives

[SOURCE: ISO 22301:2019, 3.10]

3.1.10 endpoint device
network connected information and communication technology (ICT) hardware device

Note 1 to entry: Endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware including smart meters and Internet of things (IoT) devices.

3.1.11 entity
item relevant for the purpose of operation of a domain that has recognizably distinct existence Note 1 to entry: An entity can have a physical or a logical embodimentEXAMPLE A person, an organization, a device, a group of such items, a human subscriber to a telecom service, a SIM card, a passport, a network interface card, a software application, a service or a website.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12 information processing facility
any information processing system, service or infrastructure, or the physical location housing it

[SOURCE: ISO/IEC 27000:2018, 3.27, modified — "facilities" has been replaced with facility.]

3.1.13 information security breach
compromise of information security that leads to the undesired destruction, loss, alteration, disclosure of, or access to, protected information transmitted, stored or otherwise processed

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3.1.14 nformation security event
occurrence indicating a possible *information security breach* (3.1.13) or failure of *controls* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modified — “breach of information security” has been replacedwith “information security breach”]

3.1.15 information security incident
one or multiple related and identified *information security events* (3.1.14) that can harm an organization’s *assets* (3.1.2) or compromise its operations

[SOURCE: ISO/IEC 27035-1:2016, 3.4]

3.1.16 information security incident management
exercise of a consistent and effective approach to the handling of *information security incidents* (3.1.15)

[SOURCE: ISO/IEC 27035-1:2016, 3.5]

3.1.17 information system
set of applications, services, information technology *assets* (3.1.2), or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.1.18 interested party
Stakeholder person or organization that can affect, be affected by, or perceive itself to be affected by a decision oractivity

[SOURCE: ISO/IEC 27000:2018, 3.37]

3.1.19 non-repudiation
ability to prove the occurrence of a claimed event or action and its originating *entities* (3.1.11)

3.1.20 personnel
persons doing work under the organization’s direction

Note 1 to entry: The concept of personnel includes the organization’s members, such as the governing body, top management, employees, temporary staff, contractors and volunteers.

3.1.21 personally identifiable information PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The “natural person” in the definition is the *PII principal* (3.1.22). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3.1.22 PII principal
natural person to whom the *personally identifiable information (PII)* (3.1.21) relates

Note 1 to entry: Depending on the jurisdiction and the particular data protection and privacy legislation, the synonym “data subject” can also be used instead of the term “PII principal”.
[SOURCE: ISO/IEC 29100:2011, 2.11]

3.1.23 PII processor
privacy stakeholder that processes *personally identifiable information (PII)* (3.1.21) on behalf of and in accordance with the instructions of a PII controller

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.1.24 policy
intentions and direction of an organization, as formally expressed by its top management

[SOURCE: ISO/IEC 27000:2018, 3.53]

3.1.25 privacy impact assessment
PIA
overall *process* (3.1.27) of identifying, analysing, evaluating, consulting, communicating and planning the treatment of potential privacy impacts with regard to the processing of *personally identifiableinformation (PII)* (3.1.21), framed within an organization’s broader risk management framework

[SOURCE: ISO/IEC 29134:2017, 3.7, modified — Note 1 to entry removed.]

3.1.26 procedure
specified way to carry out an activity or a *process* (3.1.27)

[SOURCE: ISO 30000:2009, 3.12]

3.1.27 process
set of interrelated or interacting activities that uses or transforms inputs to deliver a result

[SOURCE: ISO 9000:2015, 3.4.1, modified— Notes to entry removed.]

3.1.28 record
information created, received and maintained as evidence and as an *asset* (3.1.2) by an organization or person, in pursuit of legal obligations or in the transaction of business

Note 1 to entry: Legal obligations in this context include all legal, statutory, regulatory and contractual requirements.

[SOURCE: ISO 15489-1:2016, 3.14, modified— “Note 1 to entry” added.]

3.1.29 recovery point objective
RPO
point in time to which data are to be recovered after a *disruption* (3.1.9) has occurred

[SOURCE: ISO/IEC 27031:2011, 3.12, modified — "must" replaced by "are to be".]

3.1.30 recovery time objective
RTO
period of time within which minimum levels of services and/or products and the supporting systems, applications, or functions are to be recovered after a *disruption* (3.1.9) has occurred

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

[SOURCE: ISO/IEC 27031:2011, 3.13, modified — "must" replaced by "are to be".]

3.1.31 reliability
property of consistent intended behaviour and results

3.1.32 rule
accepted principle or instruction that states the organization's expectations on what is required to be done, what is allowed or not allowed
Note 1 to entry: Rules can be formally expressed in *topic-specific policies* (3.1.35) and in other types of documents.

3.1.33 sensitive information
information that needs to be protected from unavailability, unauthorized access, modification or public disclosure because of potential adverse effects on an individual, organization, national security or public safety

3.1.34 threat
potential cause of an unwanted incident, which can result in harm to a system or organization

[SOURCE: ISO/IEC 27000:2018, 3.74]

3.1.35 topic-specific policy
intentions and direction on a specific subject or topic, as formally expressed by the appropriate level of management

Note 1 to entry: Topic-specific policies can formally express *rules* (3.1.32) or organization standards.
Note 2 to entry: Some organizations use other terms for these topic-specific policies.
Note 3 to entry: The topic-specific policies referred to in this document are related to information security.
EXAMPLE Topic-specific policy on *access control* (3.1.1), topic-specific policy on clear desk and clear screen.

3.1.36 user
interested party (3.1.18) with access to the organization's *information systems* (3.1.17)

EXAMPLE *Personnel* (3.1.20), customers, suppliers.

3.1.37 user endpoint device
endpoint device (3.1.10) used by users to access information processing services

Note 1 to entry: User endpoint device can refer to desktop computers, laptops, smart phones, tablets, thin clients, etc.

3.1.38 vulnerability
weakness of an *asset* (3.1.2) or *control* (3.1.8) that can be exploited by one or more *threats* (3.1.34)

[SOURCE: ISO/IEC 27000:2018, 3.77]

3.2 Abbreviated terms

ABAC	*attribute-based access control*
ACL	*access control list*
BIA	*business impact analysis*

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

BYOD	*bring your own device*
CAPTCHA	*completely automated public Turing test to tell computers and humans apart*
CPU	*central processing unit*
DAC	*discretionary access control*
DNS	*domain name system*
GPS	*global positioning system*
IAM	*identity and access management*
ICT	*information and communication technology*
ID	*identifier*
IDE	*integrated development environment*
IDS	*intrusion detection system*
IoT	*Internet of Things*
IP	*internet protocol*
IPS	*intrusion prevention system*
IT	*information technology*
ISMS	*information security management system*
MAC	*mandatory access control*
NTP	*network time protocol*
PIA	*privacy impact assessment*
PII	*personally identifiable information*
PIN	*personal identification number*
PKI	*public key infrastructure*
PTP	*precision time protocol*
RBAC	*role-based access control*
RPO	*recovery point objective*
RTO	*recovery time objective*
SAST	*static application security testing*
SD	*secure digital*
SDN	*software-defined networking*
SD-WAN	*software-defined wide area networking*
SIEM	*security information and event management*
SMS	*short message service*
SQL	*structured query language*
SSO	*single sign on*

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

SWID	*software identification*
UEBA	*user and entity behaviour analytics*
UPS	*uninterruptible power supply*
URL	*uniform resource locator*
USB	*universal serial bus*
VM	*virtual machine*
VPN	*virtual private network*
WiFi	*wireless fidelity*

4 Structure of this document

4.1 Clauses

This document is structured as follows:

a) Organizational controls (Clause 5)
b) People controls (Clause 6)
c) Physical controls (Clause 7)
d) Technological controls (Clause 8) There are 2 informative annexes:

— Annex A — Using attributes
— Annex B — Correspondence with ISO/IEC 27002:2013

Annex A explains how an organization can use attributes (see 4.2) to create its own views based on the control attributes defined in this document or of its own creation.

Annex B shows the correspondence between the controls in this edition of ISO/IEC 27002 and the previous 2013 edition.

4.2 Themes and attributes

The categorization of controls given in Clauses 5 to 8 are

referred to as themes. Controls are categorized as:

a) people, if they concern individual people;
b) physical, if they concern physical objects;
c) technological, if they concern technology;
d) otherwise they are categorized as organizational.

The organization can use attributes to create different views which are different categorizations of controls as seen from a different perspective to the themes. Attributes can be used to filter, sort or present controls in different views for different audiences. Annex A explains how this can be achieved and provides an example of a view.

By way of example, each control in this document has been associated with five attributes with corresponding attribute values (preceded by "#" to make them searchable), as follows:

a) Control type
   Control type is an attribute to view controls from the perspective of when and how the control modifies the risk with regard to the occurrence of an information security incident. Attribute values consist of Preventive (the control that is intended to prevent the occurrence of an information security incident), Detective (the control acts when an information security incident occurs) and Corrective (the control acts after an information security incident occurs).

b) Information security properties
   Information security properties is an attribute to view controls from the perspective of

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

which characteristic of information the control will contribute to preserving. Attribute values consist of Confidentiality, Integrity and Availability.

c) Cybersecurity concepts
Cybersecurity concepts is an attribute to view controls from the perspective of the association of controls to cybersecurity concepts defined in the cybersecurity framework described in ISO/IEC TS 27110. Attribute values consist of Identify, Protect, Detect, Respond and Recover.

d) Operational capabilities
Operational capabilities is an attribute to view controls from the practitioner's perspective of information security capabilities. Attribute values consist of Governance, Asset_management, Information_protection, Human_resource_security, Physical_security, System_and_network_ security, Application_security, Secure_configuration, Identity_and_access_management, Threat_and_vulnerability_management, Continuity, Supplier_relationships_security, Legal_and_ compliance, Information_security_event_management and Information_security_assurance.

e) Security domains
Security domains is an attribute to view controls from the perspective of four information security domains: "Governance and Ecosystem" includes "Information System Security Governance & Risk Management" and "Ecosystem cybersecurity management" (including internal and external stakeholders); "Protection" includes "IT Security Architecture", "IT Security Administration", "Identity and access management", "IT Security Maintenance" and "Physical and environmental security"; "Defence" includes "Detection" and "Computer Security Incident Management"; "Resilience" includes "Continuity of operations" and "Crisis management". Attribute values consist of Governance_and_Ecosystem, Protection, Defence and Resilience.

The attributes given in this document are selected because they are considered generic enough to be used by different types of organizations. Organizations can choose to disregard one or more of the attributes given in this document. They can also create attributes of their own (with the corresponding attribute values) to create their own organizational views. Clause A.2 includes examples of such attributes.

4.3 Control layout

The layout for each control contains the following:

— **Control title:** Short name of the control;
— **Attribute table**: A table shows the value(s) of each attribute for the given control;
— **Control:** What the control is;
— **Purpose**: Why the control should be implemented;
— **Guidance:** How the control should be implemented;
— **Other information:** Explanatory text or references to other related documents.

Subheadings are used in the guidance text for some controls to aid readability where guidance is lengthy and addresses multiple topics. Such headings are not necessarily used in all guidance text. Subheadings are underlined.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5 Organizational controls

5.1 Policies for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience

Control
Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.

Purpose
To ensure continuing suitability, adequacy, effectiveness of management direction and supportfor information security in accordance with business, legal, statutory, regulatory and contractual requirements.

Guidance
At the highest level, the organization should define an “information security policy” which is approved by top management and which sets out the organization’s approach to managing its information security.
The information security policy should take into consideration requirements derived from:
a) business strategy and requirements;
b) regulations, legislation and contracts;
c) the current and projected information security risks and threats. The information

security policy should contain statements concerning:

a) definition of information security;
b) information security objectives or the framework for setting information security objectives;
c) principles to guide all activities relating to information security;
d) commitment to satisfy applicable requirements related to information security;
e) commitment to continual improvement of the information security management system;
f) assignment of responsibilities for information security management to defined roles;
g) procedures for handling exemptions and exceptions.

Top management should approve any changes to the information security policy.

At a lower level, the information security policy should be supported by topic-specific policies as needed, to further mandate the implementation of information security controls. Topic-specific policies are typically structured to address the needs of certain target groups within an organization or to cover certain security areas. Topic-specific policies should be aligned with and complementary to the information security policy of the organization.

Examples of such topics include:
a) access control;
b) physical and environmental security;
c) asset management;
d) information transfer;
e) secure configuration and handling of user endpoint devices;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

f) networking security;
g) information security incident management;
h) backup;
i) cryptography and key management;
j) information classification and handling;
k) management of technical vulnerabilities;
l) secure development.

The responsibility for the development, review and approval of the topic-specific policies should be allocated to relevant personnel based on their appropriate level of authority and technical competency. The review should include assessing opportunities for improvement of the organization's information security policy and topic-specific policies and managing information security in response to changes to:
a) the organization's business strategy;
b) the organization's technical environment;
c) regulations, statutes, legislation and contracts;
d) information security risks;
e) the current and projected information security threat environment;
f) lessons learned from information security events and incidents.

The review of information security policy and topic-specific policies should take the results of management reviews and audits into account. Review and update of other related policies should be considered when one policy is changed to maintain consistency.

The information security policy and topic-specific policies should be communicated to relevant personnel and interested parties in a form that is relevant, accessible and understandable to the intended reader. Recipients of the policies should be required to acknowledge they understand and agree to comply with the policies where applicable. The organization can determine the formats and names of these policy documents that meet the organization's needs. In some organizations, the information security policy and topic-specific policies can be in a single document. The organization can name these topic-specific policies as standards, directives, policies or others.

If the information security policy or any topic-specific policy is distributed outside the organization, care should be taken not to improperly disclose confidential information.

Table 1 illustrates the differences between information security policy and topic-specific policy.

Table 1 — Differences between information security policy and topic-specific policy

	Information security policy	Topic-specific policy
Level of detail	General or high-level	Specific and detailed
Documented and formallyapproved by	Top management	Appropriate level of management

Other information
Topic-specific policies can vary across organizations.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.2 Information security roles and responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosys-tem #Protection #Resilience

Control
Information security roles and responsibilities should be defined and allocated according to the organization needs.

Purpose
To establish a defined, approved and understood structure for the implementation, operation andmanagement of information security within the organization.

Guidance
Allocation of information security roles and responsibilities should be done in accordance with the information security policy and topic-specific policies (see 5.1). The organization should define and manage responsibilities for:

a) protection of information and other associated assets;
b) carrying out specific information security processes;
c) information security risk management activities and in particular acceptance of residual risks (e.g. to risk owners);
d) all personnel using an organization's information and other associated assets.

These responsibilities should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Individuals with allocated information security responsibilities can assign security tasks to others. However, they remain accountable and shoulddetermine that any delegated tasks have been correctly performed.

Each security area for which individuals are responsible should be defined, documented and communicated. Authorization levels should be defined and documented. Individuals who take on a specific information security role should be competent in the knowledge and skills required by the role and should be supported to keep up to date with developments related to the role and required in orderto fulfil the responsibilities of the role.

Other information

Many organizations appoint an information security manager to take overall responsibility for the development and implementation of information security and to support the identification of risks and mitigating controls.

However, responsibility for resourcing and implementing the controls often remains with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

Depending on the size and resourcing of an organization, information security can be covered bydedicated roles or duties carried out in addition to existing roles.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.3 Segregation of duties

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosys- tem

Control
Conflicting duties and conflicting areas of responsibility should be segregated.

Purpose
To reduce the risk of fraud, error and bypassing of information security controls.

Guidance
Segregation of duties and areas of responsibility aims to separate conflicting duties between different individuals in order to prevent one individual from executing potential conflicting duties on their own.

The organization should determine which duties and areas of responsibility need to be segregated. The following are examples of activities that can require segregation:
a) initiating, approving and executing a change;
b) requesting, approving and implementing access rights;
c) designing, implementing and reviewing code;
d) developing software and administering production systems;
e) using and administering applications;
f) using applications and administering databases;
g) designing, auditing and assuring information security controls.

The possibility of collusion should be considered in designing the segregation controls. Small organizations can find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls should be considered, such as monitoring of activities, audit trails and management supervision.

Care should be taken when using role-based access control systems to ensure that persons are not granted conflicting roles. When there is a large number of roles, the organization should consider using automated tools to identify conflicts and facilitate their removal. Roles should be carefully defined and provisioned to minimize access problems if a role is removed or reassigned.

Other information
No other information.

5.4 Management responsibilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosys-tem

Control

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organization.

Purpose
To ensure management understand their role in information security and undertake actions aiming to ensure all personnel are aware of and fulfil their information security responsibilities.

Guidance
Management should demonstrate support of the information security policy, topic-specific policies, procedures and information security controls.
Management responsibilities should include ensuring that personnel:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to the organization's information and other associated assets;
b) are provided with guidelines which state the information security expectations of their role within the organization;
c) are mandated to fulfil the information security policy and topic-specific policies of the organization;
d) achieve a level of awareness of information security relevant to their roles and responsibilities within the organization (see 6.3);
e) compliance with the terms and conditions of employment, contract or agreement, including the organization's information security policy and appropriate methods of working;
f) continue to have the appropriate information security skills and qualifications through ongoing professional education;
g) where practicable, are provided with a confidential channel for reporting violations of information security policy, topic-specific policies or procedures for information security ("whistleblowing"). This can allow for anonymous reporting, or have provisions to ensure that knowledge of the identity of the reporter is known only to those who need to deal with such reports;
h) are provided with adequate resources and project planning time for implementing the organization's security-related processes and controls.

Other information
No other information.

5.5 Contact with authorities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Control
The organization should establish and maintain contact with relevant authorities.

Purpose
To ensure appropriate flow of information takes place with respect to information security between the organization and relevant legal, regulatory and supervisory authorities.

Guidance
The organization should specify when and by whom authorities (e.g. law enforcement, regulatory bodies, supervisory authorities) should be contacted and how identified information security incidents should be reported in a timely manner.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Contacts with authorities should also be used to facilitate the understanding about the current and upcoming expectations of these authorities (e.g. applicable information security regulations).

Other information
Organizations under attack can request authorities to take action against the attack source. Maintaining such contacts can be a requirement to support information security incident management (see 5.24 to 5.28) or the contingency planning and business continuity processes (see 5.29 and 5.30). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in relevant laws or regulations that affect the organization. Contacts with other authorities include utilities, emergency services, electricity suppliers and health and safety [e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability) and water suppliers (in connection with cooling facilities for equipment)].

5.6 Contact with special interest groups

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence

Control
The organization should establish and maintain contact with special interest groups or other specialist security forums and professional associations.

Purpose
To ensure appropriate flow of information takes place with respect to information security.

Guidance
Membership of special interest groups or forums should be considered as a means to:
a) improve knowledge about best practices and stay up to date with relevant security information;
b) ensure the understanding of the information security environment is current;
c) receive early warnings of alerts, advisories and patches pertaining to attacks and vulnerabilities;
d) gain access to specialist information security advice;
e) share and exchange information about new technologies, products, services, threats orvulnerabilities;
f) provide suitable liaison points when dealing with information security incidents (see 5.24 to 5.28).

Other information
No other information.

5.7 Threat intelligence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulner-ability_management	#Defence #Resilience

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Control
Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose
To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

Guidance
Information about existing or emerging threats is collected and analysed in order to:
a) facilitate informed actions to prevent the threats from causing harm to the organization;
b) reduce the impact of such threats.

Threat intelligence can be divided into three layers, which should all be considered:
a) strategic threat intelligence: exchange of high-level information about the changing threat landscape (e.g. types of attackers or types of attacks);
b) tactical threat intelligence: information about attacker methodologies, tools and technologies involved;
c) operational threat intelligence: details about specific attacks, including technical indicators.

Threat intelligence should be:
a) relevant (i.e. related to the protection of the organization);
b) insightful (i.e. providing the organization with an accurate and detailed understanding of the threat landscape);
c) contextual, to provide situational awareness (i.e. adding context to the information based on the time of events, where they occur, previous experiences and prevalence in similar organizations);
d) actionable (i.e. the organization can act on information quickly and effectively).

Threat intelligence activities should include:
a) establishing objectives for threat intelligence production;
b) identifying, vetting and selecting internal and external information sources that are necessary and appropriate to provide information required for the production of threat intelligence;
c) collecting information from selected sources, which can be internal and external;
d) processing information collected to prepare it for analysis (e.g. by translating, formatting or corroborating information);
e) analysing information to understand how it relates and is meaningful to the organization;
f) communicating and sharing it to relevant individuals in a format that can be understood.

Threat intelligence should be analysed and later used:
a) by implementing processes to include information gathered from threat intelligence sources into the organization's information security risk management processes;
b) as additional input to technical preventive and detective controls like firewalls, intrusion detection system, or anti malware solutions;
c) as input to the information security test processes and techniques.

The organization should share threat intelligence with other organizations on a mutual basis in order to improve overall threat intelligence.

Other information
Organizations can use threat intelligence to prevent, detect, or respond to threats. Organizations can produce threat intelligence, but more typically receive and make use of threat intelligence produced by other sources. Threat intelligence is often provided by independent providers or advisors, government agencies or collaborative threat intelligence groups.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

The effectiveness of controls such as 5.25, 8.7, 8.16 or 8.23, depends on the quality of available threat intelligence.

5.8 Information security in project management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Governance	#Governance_and_Ecosys- tem #Protection

Control
Information security should be integrated into project management.

Purpose
To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle.

Guidance
Information security should be integrated into project management to ensure information security risksare addressed as part of the project management. This can be applied to any type of project regardless of its complexity, size, duration, discipline or application area (e.g. a project for a core business process, ICT, facility management or other supporting processes).

The project management in use should require that:
a) information security risks are assessed and treated at an early stage and periodically as part of project risks throughout the project life cycle;
b) information security requirements [e.g. application security requirements (8.26), requirementsfor complying with intellectual property rights (5.32), etc.] are addressed in the early stages of projects;
c) information security risks associated with the execution of projects, such as security of internal and external communication aspects are considered and treated throughout the project life cycle;
d) progress on information security risk treatment is reviewed and effectiveness of the treatment is evaluated and tested.

The appropriateness of the information security considerations and activities should be followed up at predefined stages by suitable persons or governance bodies, such as the project steering committee.

Responsibilities and authorities for information security relevant to the project should be defined and allocated to specified roles.

Information security requirements for products or services to be delivered by the project should be determined using various methods, including deriving compliance requirements from information security policy, topic-specific policies and regulations. Further information security requirements can be derived from activities such as threat modelling, incident reviews, use of vulnerability thresholds or contingency planning, thus ensuring that the architecture and design of information systems are protected against known threats based on the operational environment.

Information security requirements should be determined for all types of projects, not only ICT development projects. The following should also be considered when determining these requirements:
a) what information is involved (information determination), what are the corresponding informationsecurity needs (classification; see 5.12) and the potential negative business

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

impact which can resultfrom lack of adequate security;
b) the required protection needs of information and other associated assets involved, particularly in terms of confidentiality, integrity and availability;
c) the level of confidence or assurance required towards the claimed identity of entities in order to derive the authentication requirements;
d) access provisioning and authorization processes, for customers and other potential business users as well as for privileged or technical users such as relevant project members, potential operation staff or external suppliers;
e) informing users of their duties and responsibilities;
f) requirements derived from business processes, such as transaction logging and monitoring, non- repudiation requirements;
g) requirements mandated by other information security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
h) compliance with the legal, statutory, regulatory and contractual environment in which the organization operates;
i) level of confidence or assurance required for third parties to meet the organization's information security policy and topic-specific policies including relevant security clauses in any agreements or contracts.

Other information
The project development approach, such as waterfall life cycle or agile life cycle, should support information security in a structured way that can be adapted to suit the assessed severity of the information security risks, based on the character of the project. Early consideration of information security requirements for the product or service (e.g. at the planning and design stages), can lead to more effective and cost-efficient solutions for quality and information security. ISO 21500 and ISO 21502 provide guidance on concepts and processes of project management that are important for the performance of projects.

ISO/IEC 27005 provides guidance on the use of risk management processes to identify controls to meet information security requirements.

5.9 Inventory of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Asset_management	#Governance_and_Eco- system #Protection

Control
An inventory of information and other associated assets, including owners, should be developed and maintained.

Purpose
To identify the organization's information and other associated assets in order to preserve their information security and assign appropriate ownership.

Guidance
Inventory
The organization should identify its information and other associated assets and determine their importance in terms of information security. Documentation should be maintained in dedicated or existing inventories as appropriate.

The inventory of information and other associated assets should be accurate, up to date, consistent and aligned with other inventories. Options for ensuring accuracy of an inventory of information and other associated assets include:
a) conducting regular reviews of identified information and other associated assets against

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

the asset inventory;
b) automatically enforcing an inventory update in the process of installing, changing or removing an asset.

The location of an asset should be included in the inventory as appropriate.

The inventory does not need to be a single list of information and other associated assets. Considering that the inventory should be maintained by the relevant functions, it can be seen as a set of dynamic inventories, such as inventories for information assets, hardware, software, virtual machines (VMs), facilities, personnel, competence, capabilities and records.

Each asset should be classified in accordance with the classification of the information (see 5.12) associated to that asset.

The granularity of the inventory of information and other associated assets should be at a level appropriate for the needs of the organization. Sometimes specific instances of assets in the information life cycle are not feasible to be documented due to the nature of the asset. An example of a short-lived asset is a VM instance whose life cycle can be of short duration.

Ownership
For the identified information and other associated assets, ownership of the asset should be assigned to an individual or a group and the classification should be identified (see 5.12, 5.13). A process to ensure timely assignment of asset ownership should be implemented. Ownership should be assigned when assets are created or when assets are transferred to the organization. Asset ownership should be reassigned as necessary when current asset owners leave or change job roles.

Owner duties
The asset owner should be responsible for the proper management of an asset over the whole asset life cycle, ensuring that:
a) information and other associated assets are inventoried;
b) information and other associated assets are appropriately classified and protected;
c) the classification is reviewed periodically;
d) components supporting technology assets are listed and linked, such as database, storage, software components and sub-components;
e) requirements for the acceptable use of information and other associated assets (see 5.10) are established;
f) access restrictions correspond with the classification and that they are effective and are reviewed periodically;
g) information and other associated assets, when deleted or disposed, are handled in a secure manner and removed from the inventory;
h) they are involved in the identification and management of risks associated with their asset(s);
i) they support personnel who have the roles and responsibilities of managing their information.

Other information
Inventories of information and other associated assets are often necessary to ensure the effective protection of information and can be required for other purposes, such as health and safety, insurance or financial reasons. Inventories of information and other associated assets also support risk management, audit activities, vulnerability management, incident response and recovery planning.

Tasks and responsibilities can be delegated (e.g. to a custodian looking after the assets on a daily basis), but the person or group who delegated them remains accountable.

It can be useful to designate groups of information and other associated assets which act together to provide a particular service. In this case, the owner of this service is accountable for the delivery of the service, including the operation of its assets.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

See ISO/IEC 19770-1 for additional information on information technology (IT) asset management. See ISO 55001 for additional information on asset management.

5.10 Acceptable use of information and other associated assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information protection	#Governance_and_Ecosystem #Protection

Control
Rules for the acceptable use and procedures for handling information and other associated assetsshould be identified, documented and implemented.

Purpose
To ensure information and other associated assets are appropriately protected, used and handled.

Guidance
Personnel and external party users using or having access to the organization's information and other associated assets should be made aware of the information security requirements for protecting and handling the organization's information and other associated assets. They should be responsible for their use of any information processing facilities.

The organization should establish a topic-specific policy on the acceptable use of information and other associated assets and communicate it to anyone who uses or handles information and other associated assets. The topic-specific policy on acceptable use should provide clear direction on how individuals are expected to use information and other associated assets. The topic-specific policy should state:

a) expected and unacceptable behaviours of individuals from an information security perspective;
b) permitted and prohibited use of information and other associated assets;
c) monitoring activities being performed by the organization.

Acceptable use procedures should be drawn up for the full information life cycle in accordance with its classification (see 5.12) and determined risks. The following items should be considered:

a) access restrictions supporting the protection requirements for each level of classification;
b) maintenance of a record of the authorized users of information and other associated assets;
c) protection of temporary or permanent copies of information to a level consistent with the protection of the original information;
d) storage of assets associated with information in accordance with manufacturers' specifications (see 7.8);
e) clear marking of all copies of storage media (electronic or physical) for the attention of theauthorized recipient (see 7.10);
f) authorization of disposal of information and other associated assets and supported deletion method(s) (see 8.10).

Other information
It can be the case that the assets concerned do not directly belong to the organization, such as public cloud services. The use of such third-party assets and any assets of the organization associated with such external assets (e.g. information, software) should be identified as applicable and controlled,for example, through agreements with cloud service providers. Care

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

should also be taken when acollaborative working environment is used.

5.11 Return of assets

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management	#Protection

Control
Personnel and other interested parties as appropriate should return all the organization's assets in their possession upon change or termination of their employment, contract or agreement.

Purpose
To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement.

Guidance
The change or termination process should be formalized to include the return of all previously issued physical and electronic assets owned by or entrusted to the organization.
In cases where personnel and other interested parties purchase the organization's equipment or use their own personal equipment, procedures should be followed to ensure that all relevant information is traced and transferred to the organization and securely deleted from the equipment (see 7.14).

In cases where personnel and other interested parties have knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

During the notice period and thereafter, the organization should prevent unauthorized copying ofrelevant information (e.g. intellectual property) by personnel under notice of termination.

The organization should clearly identify and document all information and other associated assets tobe returned which can include:
a) user endpoint devices;
b) portable storage devices;
c) specialist equipment;
d) authentication hardware (e.g. mechanical keys, physical tokens and smartcards) for information systems, sites and physical archives;
e) physical copies of information.

to return information held on assets which are not owned by the organization. In such cases, it is necessary to restrict the use of information using other information security controls such as access rights management (5.18) or use of cryptography (8.24).

5.12 Classification of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Information_protection	#Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Control
Information should be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.

Purpose
To ensure identification and understanding of protection needs of information in accordance with its importance to the organization.

Guidance
The organization should establish a topic-specific policy on information classification and communicate it to all relevant interested parties.
The organization should take into account requirements for confidentiality, integrity and availability in the classification scheme.

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information, for protecting integrity of information and for assuring availability, as well as legal requirements concerning the confidentiality, integrity or availability of the information. Assets other than information can also be classified in compliance with classification of information, which is stored in, processed by or otherwise handled or protected by the asset.

Owners of information should be accountable for their classification.

The classification scheme should include conventions for classification and criteria for review of the classification over time. Results of classification should be updated in accordance with changes of the value, sensitivity and criticality of information through their life cycle.

The scheme should be aligned to the topic-specific policy on access control (see 5.1) and should be able to address specific business needs of the organization.

The classification can be determined by the level of impact that the information's compromise would have for the organization. Each level defined in the scheme should be given a name that makes sense in the context of the classification scheme’s application.

The scheme should be consistent across the whole organization and included in its procedures so that everyone classifies information and applicable other associated assets in the same way. In this manner, everyone has a common understanding of protection requirements and applies appropriate protection.

The classification scheme used within the organization can be different from the schemes used by other organizations, even if the names for levels are similar. In addition, information moving between organizations can vary in classification depending on its context in each organization, even if their classification schemes are identical. Therefore, agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification levels from other organizations. Correspondence between different schemes can be determined by looking for equivalence in the associated handling and protection methods.

Other information
Classification provides people who deal with information with a concise indication of how to handle and protect it. Creating groups of information with similar protection needs and specifying information security procedures that apply to all the information in each group facilitates this. This approach reduces the need for case-by-case risk assessment and custom design of controls.

Information can cease to be sensitive or critical after a certain period of time. For example, when the information has been made public, it no longer has confidentiality requirements but can still require protection for its integrity and availability properties. These aspects should

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense or, on the contrary, under-classification can lead to insufficient controls to protect the information from compromise.

As an example, an information confidentiality classification scheme can be based on four levels as follows:
a) disclosure causes no harm;
b) disclosure causes minor reputational damage or minor operational impact;
c) disclosure has a significant short-term impact on operations or business objectives;
d) disclosure has a serious impact on long term business objectives or puts the survival of the organization at risk.

5.13 Labelling of information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Information_ protection	#Defence #Protection

Control
An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

Purpose
To facilitate the communication of classification of information and support automation of information processing and management.

Guidance
Procedures for information labelling should cover information and other associated assets in all formats. The labelling should reflect the classification scheme established in 5.12. The labels should be easily recognizable. The procedures should give guidance on where and how labels are attached in consideration of how the information is accessed or the assets are handled depending on the types of storage media. The procedures can define:
a) cases where labelling is omitted (e.g. labelling of non-confidential information to reduce workloads);
b) how to label information sent by or stored on electronic or physical means, or any other format;
c) how to handle cases where labelling is not possible (e.g. due to technical restrictions).

Examples of labelling techniques include:
a) physical labels;
b) headers and footers;
c) metadata;
d) watermarking;
e) rubber-stamps.

Digital information should utilize metadata in order to identify, manage and control information, especially with regard to confidentiality. Metadata should also enable efficient and correct searching for information. Metadata should facilitate systems to interact and make decisions based on the associated classification labels.

The procedures should describe how to attach metadata to information, what labels to use and how data should be handled, in line with the organization's information model and ICT architecture.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Relevant additional metadata should be added by systems when they process information depending on its information security properties.

Personnel and other interested parties should be made aware of labelling procedures. All personnel should be provided with the necessary training to ensure that information is correctly labelled and handled accordingly.

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label.

Other information
Labelling of classified information is a key requirement for information sharing.

Other useful metadata that can be attached to the information is which organizational process created the information and at what time.

Labelling of information and other associated assets can sometimes have negative effects. Classified assets can be easier to identify by malicious actors for potential misuse.

Some systems do not label individual files or database records with their classification but protect all information at the highest level of classification of any of the information that it contains or is permitted to contain. It is usual in such systems to determine and then label information when it is exported.

5.14 Information transfer

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control
Information transfer rules, procedures, or agreements should be in place for all types of transfer facilities within the organization and between the organization and other parties.

Purpose
To maintain the security of information transferred within an organization and with any external interested party.

Guidance
General
The organization should establish and communicate a topic-specific policy on information transfer to all relevant interested parties. Rules, procedures and agreements to protect information in transit should reflect the classification of the information involved. Where information is transferred between the organization and third parties, transfer agreements (including recipient authentication) should be established and maintained to protect information in all forms in transit (see 5.10).

Information transfer can happen through electronic transfer, physical storage media transfer and verbal transfer.

For all types of information transfer, rules, procedures and agreements should include:
a) controls designed to protect transferred information from interception, unauthorized access, copying, modification, misrouting, destruction and denial of service, including levels of access control commensurate with the classification of the information involved and any special controls that are required to protect sensitive information, such as use

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

of cryptographic techniques (see 8.24);
b) controls to ensure traceability and non-repudiation, including maintaining a chain of custody for information while in transit;
c) identification of appropriate contacts related to the transfer including information owners, risk owners, security officers and information custodians, as applicable;
d) responsibilities and liabilities in the event of information security incidents, such as loss of physical storage media or data;
e) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected (see 5.13);
f) reliability and availability of the transfer service;
g) the topic-specific policy or guidelines on acceptable use of information transfer facilities (see 5.10);
h) retention and disposal guidelines for all business records, including messages;
NOTE Local legislation and regulations can exist regarding retention and disposal of business records.
i) the consideration of any other relevant legal, statutory, regulatory and contractual requirements (see 5.31, 5.32, 5.33, 5.34) related to transfer of information (e.g. requirements for electronic signatures).

Electronic transfer

Rules, procedures and agreements should also consider the following items when using electronic communication facilities for information transfer:
a) detection of and protection against malware that can be transmitted through the use of electronic communications (see 8.7);
b) protection of communicated sensitive electronic information that is in the form of an attachment;
c) prevention against sending documents and messages in communications to the wrong address or number;
d) obtaining approval prior to using external public services such as instant messaging, social networking, file sharing or cloud storage;
e) stronger levels of authentication when transferring information via publicly accessible networks;
f) restrictions associated with electronic communication facilities (e.g. preventing automatic forwarding of electronic mail to external mail addresses);
g) advising personnel and other interested parties not to send short message service (SMS) or instant messages with critical information since these can be read in public places (and therefore by unauthorized persons) or stored in devices not adequately protected;
h) advising personnel and other interested parties about the problems of using fax machines or services, namely:
1) unauthorized access to built-in message stores to retrieve messages;
2) deliberate or accidental programming of machines to send messages to specific numbers.

Physical storage media transfer

When transferring physical storage media (including paper), rules, procedures and agreements should also include:
a) responsibilities for controlling and notifying transmission, dispatch and receipt;
b) ensuring correct addressing and transportation of the message;
c) packaging that protects the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications, for example protecting against any environmental factors that can reduce the effectiveness of restoring storage media such as exposure to heat, moisture or electromagnetic fields; using minimum technical standards for packaging and transmission (e.g. the use of opaque envelopes);
d) a list of authorized reliable couriers agreed by management;
e) courier identification standards;
f) depending on the classification level of the information in the storage media to be

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

transported, use tamper evident or tamper-resistant controls (e.g. bags, containers);
g) procedures to verify the identification of couriers;
h) approved list of third parties providing transportation or courier services depending on the classification of the information;
i) keeping logs for identifying the content of the storage media, the protection applied as well as recording the list of authorised recipients, the times of transfer to the transit custodians and receipt at the destination.

Verbal transfer
To protect verbal transfer of information, personnel and other interested parties should be reminded that they should:
a) not have confidential verbal conversations in public places or over insecure communication channels since these can be overheard by unauthorized persons;
b) not leave messages containing confidential information on answering machines or voice messages since these can be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;
c) be screened to the appropriate level to listen to the conversation;
d) ensure that appropriate room controls are implemented (e.g. sound-proofing, closed door);
e) begin any sensitive conversations with a disclaimer so those present know the classification level and any handling requirements of what they are about to hear.

Other information
No other information.

5.15 Access control

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.

Purpose
To ensure authorized access and to prevent unauthorized access to information and other associated assets.

Guidance
Owners of information and other associated assets should determine information security and business requirements related to access control. A topic-specific policy on access control should be defined whichtakes account of these requirements and should be communicated to all relevant interested parties.
These requirements and the topic-specific policy should consider the following:
a) determining which entities require which type of access to the information and other associated assets;
b) security of applications (see 8.26);
c) physical access, which needs to be supported by appropriate physical entry controls (see 7.2, 7.3, 7.4);
d) information dissemination and authorization (e.g. the need-to-know principle) and information security levels and classification of information (see 5.10, 5.12, 5.13);
e) restrictions to privileged access (see 8.2);
f) segregation of duties (see 5.3);
g) relevant legislation, regulations and any contractual obligations regarding limitation of

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

access to data or services (see 5.31, 5.32, 5.33, 5.34, 8.3);
h) segregation of access control functions (e.g. access request, access authorization, access administration);
i) formal authorization of access requests (see 5.16 and 5.18);
j) the management of access rights (see 5.18);
k) logging (see 8.15).

Access control rules should be implemented by defining and mapping appropriate access rights and restrictions to the relevant entities (see 5.16). An entity can represent a human user as well as a technical or logical item (e.g. a machine, device or a service). To simplify the access control management, specific roles can be assigned to entity groups.

The following should be taken into account when defining and implementing access control rules:
a) consistency between the access rights and information classification;
b) consistency between the access rights and the physical perimeter security needs and requirements;
c) considering all types of available connections in distributed environments so entities are only provided with access to information and other associated assets, including networks and network services, that they are authorized to use;
d) considering how elements or factors relevant to dynamic access control can be reflected.

Other information
There are often overarching principles used in the context of access control. Two of the most frequently used principles are:
a) need-to-know: an entity is only granted access to the information which that entity requires in order to perform its tasks (different tasks or roles mean different need-to-know information and hence different access profiles);
b) need-to-use: an entity is only assigned access to information technology infrastructure where a clear need is present.

Care should be taken when specifying access control rules to consider:
a) establishing rules based on the premise of least privilege, “Everything is generally forbidden unless expressly permitted”, rather than the weaker rule, “Everything is generally permitted unless expressly forbidden”;
b) changes in information labels (see 5.13) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;
c) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;
d) when to define and regularly review the approval.

Access control rules should be supported by documented procedures (see 5.16, 5.17, 5.18, 8.2, 8.3, 8.4, 8.5, 8.18) and defined responsibilities (see 5.2, 5.17).

There are several ways to implement access control, such as MAC (mandatory access control), DAC (discretionary access control), RBAC (role-based access control) and ABAC (attribute-based access control).

Access control rules can also contain dynamic elements (e.g. a function that evaluates past accesses or specific environment values). Access control rules can be implemented in different granularity, ranging from covering whole networks or systems to specific data fields and can also consider properties such as user location or the type of network connection that is used for access. These principles and how granular access control is defined can have a significant cost impact. Stronger rules and more granularity typically lead to higher cost. Business requirements and risk considerations should be used to define which access control rules are applied and which granularity is required.

5.16 Identity management

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
The full life cycle of identities should be managed.

Purpose
To allow for the unique identification of individuals and systems accessing the organization's information and other associated assets and to enable appropriate assignment of access rights.

Guidance
The processes used in the context of identity management should ensure that:
a) for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity;
b) identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval and documentation;
c) identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight;
d) identities are disabled or removed in a timely fashion if they are no longer required (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the organization or changed the role);
e) in a specific domain, a single identity is mapped to a single entity, [i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided];
f) records of all significant events concerning the use and management of user identities and of authentication information are kept.

The organization should have a supporting process in place to handle changes to information related to user identities. These processes can include re-verification of trusted documents related to a person.

When using identities provided or issued by third parties (e.g. social media credentials), the organization should ensure the third-party identities provide the required trust level and any associated risks are known and sufficiently treated. This can include controls related to the third parties (see 5.19) as well as controls related to associated authentication information (see 5.17).

Other information
Providing or revoking access to information and other associated assets is usually a multi-step procedure:
a) confirming the business requirements for an identity to be established;
b) verifying the identity of an entity before allocating them a logical identity;
c) establishing an identity;
d) configuring and activating the identity. This also includes configuration and initial setup of related authentication services;
e) providing or revoking specific access rights to the identity, based on appropriate authorization or entitlement decisions (see 5.18).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.17 Authentication information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.

Purpose
To ensure proper entity authentication and prevent failures of authentication processes.

Guidance
Allocation of authentication information
The allocation and management process should ensure that:
a) personal passwords or personal identification numbers (PINs) generated automatically during enrolment processes as temporary secret authentication information are non-guessable and uniquefor each person, and that users are required to change them after the first use;
b) procedures are established to verify the identity of a user prior to providing new, replacement or temporary authentication information;
c) authentication information, including temporary authentication information, is transmitted to users in a secure manner (e.g. over an authenticated and protected channel) and the use of unprotected (clear text) electronic mail messages for this purpose is avoided;
d) users acknowledge receipt of authentication information;
e) default authentication information as predefined or provided by vendors is changed immediately following installation of systems or software;
f) records of significant events concerning allocation and management of authentication information are kept and their confidentiality is granted, and that the record-keeping method is approved (e.g. by using an approved password vault tool).

User responsibilities
Any person having access to or using authentication information should be advised to ensure that:
a) secret authentication information such as passwords are kept confidential. Personal secret authentication information is not to be shared with anyone. Secret authentication information used in the context of identities linked to multiple users or linked to non-personal entities are solely shared with authorized persons;
b) affected or compromised authentication information is changed immediately upon notification of or any other indication of a compromise;
c) when passwords are used as authentication information, strong passwords according to best practice recommendations are selected, for example:
    1) passwords are not based on anything somebody else can easily guess or obtain using person- related information (e.g. names, telephone numbers and dates of birth);
    2) passwords are not based on dictionary words or combinations thereof;
    3) use easy to remember passphrases and try to include alphanumerical and special characters;
    4) passwords have a minimum length;
d) the same passwords are not used across distinct services and systems;
e) the obligation to follow these rules is also included in terms and conditions of employment (see 6.2).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Password management system
When passwords are used as authentication information, the password management system should:

a) allow users to select and change their own passwords and include a confirmation procedure to address input errors;
b) enforce strong passwords according to good practice recommendations [see c) of "User responsibilities];
c) force users to change their passwords at first login;
d) enforce password changes as necessary, for example after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities);
e) prevent re-use of previous passwords;
f) prevent the use of commonly-used passwords and compromised usernames, passwordcombinations from hacked systems;
g) not display passwords on the screen when being entered;
h) store and transmit passwords in protected form.

Password encryption and hashing should be performed according to approved cryptographic techniques for passwords (see 8.24).

Other information
Passwords or passphrases are a commonly used type of authentication information and are a common means of verifying a user's identity. Other types of authentication information are cryptographic keys, data stored on hardware tokens (e.g. smart cards) that produce authentication codes and biometric data such as iris scans or fingerprints. Additional information can be found in the ISO/IEC 24760 series.

Requiring frequent change of passwords can be problematic because users can get annoyed by the frequent changes, forget new passwords, note them down in unsafe places, or choose unsafe passwords. Provision of single sign on (SSO) or other authentication management tools (e.g. password vaults) reduces the amount of authentication information that users are required to protect and can thereby increase the effectiveness of this control. However, these tools can also increase the impact of disclosureof authentication information.

Some applications require user passwords to be assigned by an independent authority. In such cases, a), c) and d) of "Password management system" do not apply.

5.18 Access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.

Purpose
To ensure access to information and other associated assets is defined and authorized according to the business requirements.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance

Provision and revocation of access rights

The provisioning process for assigning or revoking physical and logical access rights granted to an entity's authenticated identity should include:

a) obtaining authorization from the owner of the information and other associated assets for the use of the information and other associated assets (see 5.9). Separate approval for access rights by management can also be appropriate;
b) considering the business requirements and the organization's topic-specific policy and rules on access control;
c) considering segregation of duties, including segregating the roles of approval and implementationof the access rights and separation of conflicting roles;
d) ensuring access rights are removed when someone does not need to access the information and other associated assets, in particular ensuring access rights of users who have left the organization are removed in a timely fashion;
e) considering giving temporary access rights for a limited time period and revoking them at the expiration date, in particular for temporary personnel or temporary access required by personnel;
f) verifying that the level of access granted is in accordance with the topic-specific policies on access control (see 5.15) and is consistent with other information security requirements such as segregation of duties (see 5.3);
g) ensuring that access rights are activated (e.g. by service providers) only after authorization procedures are successfully completed;
h) maintaining a central record of access rights granted to a user identifier (ID, logical or physical) to access information and other associated assets;
i) modifying access rights of users who have changed roles or jobs;
j) removing or adjusting physical and logical access rights, which can be done by removal, revocation or replacement of keys, authentication information, identification cards or subscriptions;
k) maintaining a record of changes to users' logical and physical access rights.

Review of access rights

Regular reviews of physical and logical access rights should consider the following:

a) users' access rights after any change within the same organization (e.g. job change, promotion, demotion) or termination of employment (see 6.1 to 6.5);
b) authorizations for privileged access rights.

Consideration before change or termination of employment

A user's access rights to information and other associated assets should be reviewed and adjusted or removed before any change or termination of employment based on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the user or by management and the reason for termination;
b) the current responsibilities of the user;
c) the value of the assets currently accessible.

Other information

Consideration should be given to establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews of access rights are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel (see 5.20, 6.2, 6.4, 6.6).

In cases of management-initiated termination, disgruntled personnel or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they can be tempted to collect information for future

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

use.

Cloning is an efficient way for organizations to assign access to users. However, it should be donewith care based on distinct roles identified by the organization rather than just cloning an identitywith all associated access rights. Cloning has an inherent risk of resulting in excessive access rights to information and other associated assets.

5.19 Information security in supplier relationships

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relation-ships_security	#Governance_and_ Ecosystem #Protec-tion

Control
Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.

Purpose
To maintain an agreed level of information security in supplier relationships.

Guidance
The organization should establish and communicate a topic-specific policy on supplier relationships to all relevant interested parties.

The organization should identify and implement processes and procedures to address security risks associated with the use of products and services provided by suppliers. This should also apply to the organization's use of resources of cloud service providers. These processes and procedures should include those to be implemented by the organization, as well as those the organization requires the supplier to implement for the commencement of use of a supplier's products or services or for thetermination of use of a supplier's products and services, such as:

a) identifying and documenting the types of suppliers (e.g. ICT services, logistics, utilities, financial services, ICT infrastructure components) which can affect the confidentiality, integrity and availability of the organization's information;
b) establishing how to evaluate and select suppliers according to the sensitivity of information, products and services (e.g. with market analysis, customer references, review of documents, on- site assessments, certifications);
c) evaluating and selecting supplier's products or services that have adequate information security controls and reviewing them; in particular, accuracy and completeness of controls implemented by the supplier that ensure integrity of the supplier's information and information processing and hence the organization's information security;
d) defining the organization's information, ICT services and the physical infrastructure that suppliers can access, monitor, control or use;
e) defining the types of ICT infrastructure components and services provided by suppliers which can affect the confidentiality, integrity and availability of the organization's information;
f) assessing and managing the information security risks associated with:
    1) the suppliers' use of the organization's information and other associated assets, including risksoriginating from potential malicious supplier personnel;
    2) malfunctioning or vulnerabilities of the products (including software components and sub- components used in these products) or services provided by the suppliers;
g) monitoring compliance with established information security requirements for each type of supplier and type of access, including third-party review and product validation;
h) mitigating non-compliance of a supplier, whether this was detected through monitoring or by othermeans;
i) handling incidents and contingencies associated with supplier products and services

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

including responsibilities of both the organization and suppliers;
j) resilience and, if necessary, recovery and contingency measures to ensure the availability of the supplier's information and information processing and hence the availability of the organization's information;
k) awareness and training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement, topic-specific policies, processes and procedures and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
l) managing the necessary transfer of information, other associated assets and anything else that needs to be changed and ensuring that information security is maintained throughout the transfer period;
m) requirements to ensure a secure termination of the supplier relationship, including:
   1) de-provisioning of access rights;
   2) information handling;
   3) determining ownership of intellectual property developed during the engagement;
   4) information portability in case of change of supplier or insourcing;
   6) records management;
   7) return of assets;
   8) secure disposal of information and other associated assets;
   9) ongoing confidentiality requirements;
n) level of personnel security and physical security expected from supplier's personnel and facilities.

The procedures for continuing information processing in the event that the supplier becomes unable to supply its products or services (e.g. because of an incident, because the supplier is no longer in business, or no longer provides some components due to technology advancements) should be considered to avoid any delay in arranging replacement products or services (e.g. identifying an alternative supplier in advance or always using alternative suppliers).

Other information
In cases where it is not possible for an organization to place requirements on a supplier, the organization should:
a) consider the guidance given in this control in making decisions about choosing a supplier and its product or service;
b) implement compensating controls as necessary based on a risk assessment.

Information can be put at risk by suppliers with inadequate information security management. Controls should be determined and applied to manage the supplier's access to information and other associated assets. For example, if there is a special need for confidentiality of the information, non-disclosure agreements or cryptographic techniques can be used. Another example is personal data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

Risks can also be caused by inadequate controls of ICT infrastructure components or services provided by suppliers. Malfunctioning or vulnerable components or services can cause information security breaches in the organization or to another entity (e.g. they can cause malware infection, attacks or other harm on entities other than the organization).

See ISO/IEC 27036-2 for more detail.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.20 Addressing information security within supplier agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relation-ships_security	#Governance_and_Ecosystem #Protec-tion

Control
Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.

Purpose
To maintain an agreed level of information security in supplier relationships.

Guidance
Supplier agreements should be established and documented to ensure that there is clear understanding between the organization and the supplier regarding both parties' obligations to fulfil relevant information security requirements.

The following terms can be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;
b) classification of information according to the organization's classification scheme (see 5.10, 5.12, 5.13);
c) mapping between the organization's own classification scheme and the classification scheme of the supplier;
d) legal, statutory, regulatory and contractual requirements, including data protection, handling of personally identifiable information (PII), intellectual property rights and copyright and a description of how it will be ensured that they are met;
e) obligation of each contractual party to implement an agreed set of controls, including access control, performance review, monitoring, reporting and auditing, and the supplier's obligations to comply with the organization's information security requirements;
f) rules of acceptable use of information and other associated assets, including unacceptable use if necessary;
g) procedures or conditions for authorization and removal of the authorization for the use of the organization's information and other associated assets by supplier personnel (e.g. through an explicit list of supplier personnel authorized to use the organization's information and other associated assets);
h) Information security requirements regarding the supplier's ICT infrastructure; in particular, minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and risk criteria;
i) indemnities and remediation for failure of contractor to meet requirements;
j) incident management requirements and procedures (especially notification and collaboration during incident remediation);
k) training and awareness requirements for specific procedures and information security requirements (e.g. for incident response, authorization procedures);
l) relevant provisions for sub-contracting, including the controls that need to be implemented, suchas agreement on the use of sub-suppliers (e.g. requiring to have them under the same obligations of the supplier, requiring to have a list of sub-suppliers and notification before any change);
m) relevant contacts, including a contact person for information security issues;
n) any screening requirements, where legally permissible, for the supplier's personnel, including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

o) the evidence and assurance mechanisms of third-party attestations for relevant information security requirements related to the supplier processes and an independent report on effectiveness of controls;
p) right to audit the supplier processes and controls related to the agreement;
q) supplier's obligation to periodically deliver a report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
r) defect resolution and conflict resolution processes;
s) providing backup aligned with the organization's needs (in terms of frequency and type and storage location);
t) ensuring the availability of an alternate facility (i.e. disaster recovery site) not subject to the same threats as the primary facility and considerations for fall back controls (alternate controls) in the event primary controls fail;
u) having a change management process that ensures advance notification to the organization and the possibility for the organization of not accepting changes;
v) physical security controls commensurate with the information classification;
w) information transfer controls to protect the information during physical transfer or logical transmission;
x) termination clauses upon conclusion of the agreement including records management, return of assets, secure disposal of information and other associated assets, and any ongoing confidentiality obligations;
y) provision of a method of securely destroying the organization's information stored by the supplier as soon as it is no longer required;
z) ensuring, at the end of the contract, handover support to another supplier or to the organization itself.

The organization should establish and maintain a register of agreements with external parties (e.g. contracts, memorandum of understanding, information-sharing agreements) to keep track of where their information is going. The organization should also regularly review, validate and update their agreements with external parties to ensure they are still required and fit for purpose with relevant information security clauses.

Other information
The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant requirements for addressing information security risks.

For details on supplier agreements, see ISO/IEC 27036 series. For cloud service agreements, see ISO/IEC 19086 series.

5.21 Managing information security in the ICT supply chain

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relatio n-ships_security	#Governance_and _ Ecosystem #Protec-tion

Control
Processes and procedures should be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.

Purpose
To maintain an agreed level of information security in supplier relationships.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance
The following topics should be considered to address information security within ICT supply chain security in addition to the general information security requirements for supplier relationships:

a) defining information security requirements to apply to ICT product or service acquisition;
b) requiring that ICT services suppliers propagate the organization's security requirements throughout the supply chain if they sub-contract for parts of the ICT service provided to the organization;
c) requiring that ICT products suppliers propagate appropriate security practices throughout thesupply chain if these products include components purchased or acquired from other suppliers or other entities (e.g. sub-contracted software developers and hardware component providers);
d) requesting that ICT products suppliers provide information describing the software components used in products;
e) requesting that ICT products suppliers provide information describing the implemented security functions of their product and the configuration required for its secure operation;
f) implementing a monitoring process and acceptable methods for validating that delivered ICT products and services comply with stated security requirements. Examples of such supplier review methods can include penetration testing and proof or validation of third-party attestations for the supplier's information security operations;
g) implementing a process for identifying and documenting product or service components that are critical for maintaining functionality and therefore require increased attention, scrutiny and further follow up required when built outside of the organization especially if the supplier outsources aspects of product or service components to other suppliers;
h) obtaining assurance that critical components and their origin can be traced throughout the supply chain;
i) obtaining assurance that the delivered ICT products are functioning as expected without any unexpected or unwanted features;
j) implementing processes to ensure that components from suppliers are genuine and unaltered from their specification. Example measures include anti-tamper labels, cryptographic hash verifications or digital signatures. Monitoring for out of specification performance can be an indicator of tampering or counterfeits. Prevention and detection of tampering should be implemented during multiple stages in the system development life cycle, including design, development, integration, operations and maintenance;
k) obtaining assurance that ICT products achieve required security levels, for example, through formal certification or an evaluation scheme such as the Common Criteria Recognition Arrangement;
l) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;
m) implementing specific processes for managing ICT component life cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements. Identification of an alternative supplier and the process to transfer software and competence to the alternative supplier should be considered.

Other information
The specific ICT supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the ICT supply chain and any matters that have an important effect on the products and services being provided. The organization can influence ICT supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the ICT supply chain.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

ICT should be acquired from reputable sources. The reliability of software and hardware is a matter of quality control. While it is generally not possible for an organization to inspect the quality control systems of its vendors, it can make reliable judgments based on the reputation of the vendor.

ICT supply chain as addressed here includes cloud services. Examples of ICT supply chains are:

a) cloud services provisioning, where the cloud service provider relies on the software developers, telecommunication service providers, hardware providers;
b) IoT, where the service involves the device manufacturers, the cloud service providers (e.g. the IoT platform operators), the developers for mobile and web applications, the vendor of software libraries;
c) hosting services, where the provider relies on external service desks including first, second and third support levels.

See ISO/IEC 27036-3 for more details including risk assessment guidance.

Software identification (SWID) tags can also help to achieve better information security in the supply chain, by providing information about software provenance. See ISO/IEC 19770-2 for more details.

5.22 Monitoring, review and change management of supplier services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relation-ships_security #Information_secu-rity_assurance	#Governance_and_ Ecosystem #Protec-tion #Defence

Control
The organization should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.

Purpose
To maintain an agreed level of information security and service delivery in line with supplier agreements.

Guidance
Monitoring, review and change management of supplier services should ensure the information security terms and conditions of the agreements are complied with, information security incidents and problems are managed properly and changes in supplier services or business status do not affect service delivery.

This should involve a process to manage the relationship between the organization and the supplier to:

a) monitor service performance levels to verify compliance with the agreements;
b) monitor changes made by suppliers including:
   1) enhancements to the current services offered;
   2) development of any new applications and systems;
   3) modifications or updates of the supplier's policies and procedures;
   4) new or changed controls to resolve information security incidents and to improve information security;
c) monitor changes in supplier services including:
   1) changes and enhancement to networks;
   2) use of new technologies;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

3) adoption of new products or newer versions or releases;
4) new development tools and environments;
5) changes to physical location of service facilities;
6) change of sub-suppliers;
7) sub-contracting to another supplier;

d) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
e) conduct audits of suppliers and sub-suppliers, in conjunction with review of independent auditor's reports, if available and follow-up on issues identified;
f) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;
g) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
h) respond to and manage any identified information security events or incidents;
i) identify information security vulnerabilities and manage them;
j) review information security aspects of the supplier's relationships with its own suppliers;
k) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 5.29, 5.30, 5.35, 5.36, 8.14);
l) ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements;
m) evaluate regularly that the suppliers maintain adequate information security levels.

The responsibility for managing supplier relationships should be assigned to a designated individual or team. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate actions should be taken when deficiencies in the service delivery are observed.

Other information
See ISO/IEC 27036-3 for more detail.

5.23 Information security for use of cloud services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Supplier_relation-ships_security	#Governance_and_Ecosystem #Protection

Control
Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Purpose
To specify and manage information security for the use of cloud services.

Guidance
The organization should establish and communicate topic-specific policy on the use of cloud services to all relevant interested parties.

The organization should define and communicate how it intends to manage information security risks associated with the use of cloud services. It can be an extension or part of the existing approach for how an organization manages services provided by external parties (see 5.21 and 5.22).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

The use of cloud services can involve shared responsibility for information security and collaborative effort between the cloud service provider and the organization acting as the cloud service customer. It is essential that the responsibilities for both the cloud service provider and the organization, acting as the cloud service customer, are defined and implemented appropriately.
The organization should define:

a) all relevant information security requirements associated with the use of the cloud services;
b) cloud service selection criteria and scope of cloud service usage;
c) roles and responsibilities related to the use and management of cloud services;
d) which information security controls are managed by the cloud service provider and which are managed by the organization as the cloud service customer;
e) how to obtain and utilize information security capabilities provided by the cloud service provider;
f) how to obtain assurance on information security controls implemented by cloud service providers;
g) how to manage controls, interfaces and changes in services when an organization uses multiple cloud services, particularly from different cloud service providers;
h) procedures for handling information security incidents that occur in relation to the use of cloud services;
i) its approach for monitoring, reviewing and evaluating the ongoing use of cloud services to manage information security risks;
j) how to change or stop the use of cloud services including exit strategies for cloud services.

Cloud service agreements are often pre-defined and not open to negotiation. For all cloud services, the organization should review cloud service agreements with the cloud service provider(s). A cloud service agreement should address the confidentiality, integrity, availability and information handling requirements of the organization, with appropriate cloud service level objectives and cloud service qualitative objectives. The organization should also undertake relevant risk assessments to identify the risks associated with using the cloud service. Any residual risks connected to the use of the cloud service should be clearly identified and accepted by the appropriate management of the organization.

An agreement between the cloud service provider and the organization, acting as the cloud service customer, should include the following provisions for the protection of the organization's data and availability of services:

a) providing solutions based on industry accepted standards for architecture and infrastructure;
b) managing access controls of the cloud service to meet the requirements of the organization;
c) implementing malware monitoring and protection solutions;
d) processing and storing the organization's sensitive information in approved locations (e.g. particular country or region) or within or subject to a particular jurisdiction;
e) providing dedicated support in the event of an information security incident in the cloud service environment;
f) ensuring that the organization's information security requirements are met in the event of cloud services being further sub-contracted to an external supplier (or prohibiting cloud services from being sub-contracted);
g) supporting the organization in gathering digital evidence, taking into consideration laws and regulations for digital evidence across different jurisdictions;
h) providing appropriate support and availability of services for an appropriate time frame when the organization wants to exit from the cloud service;
i) Providing required backup of data and configuration information and securely managing backups as applicable, based on the capabilities of the cloud service provider used by the organization, acting as the cloud service customer;
j) providing and returning information such as configuration files, source code and data that are owned by the organization, acting as the cloud service customer, when

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

requested during the service provision or at termination of service.

The organization, acting as the cloud service customer, should consider whether the agreement should require cloud service providers to provide advance notification prior to any substantive customerimpacting changes being made to the way the service is delivered to the organization, including:

a) changes to the technical infrastructure (e.g. relocation, reconfiguration, or changes in hardware or software) that affect or change the cloud service offering;
b) processing or storing information in a new geographical or legal jurisdiction;
c) use of peer cloud service providers or other sub-contractors (including changing existing or using new parties).

The organization using cloud services should maintain close contact with its cloud service providers. These contacts enable mutual exchange of information about information security for the use of the cloud services including a mechanism for both cloud service provider and the organization, acting as thecloud service customer, to monitor each service characteristic and report failures to the commitments contained in the agreements.

Other information

This control considers cloud security from the perspective of the cloud service customer.

Additional information relating to cloud services can be found in ISO/IEC 17788, ISO/IEC 17789 and ISO/IEC 22123-1. Specifics related to cloud portability in support of exit strategies can be found in ISO/IEC 19941. Specifics related to information security and public cloud services are described in ISO/IEC 27017. Specifics related to PII protection in public clouds acting as PII processor are described in ISO/IEC 27018. Supplier relationships for cloud services are covered by ISO/IEC 27036-4 and cloud service agreements and their contents are dealt with in the ISO/IEC 19086 series, with security and privacy specifically covered by ISO/IEC 19086-4.

5.24 Information security incident management planning and preparation

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence

Control

The organization should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.

Purpose

To ensure quick, effective, consistent and orderly response to information security incidents, including communication on information security events.

Guidance

Roles and responsibilities

The organization should establish appropriate information security incident management processes. Roles and responsibilities to carry out the incident management procedures should be determined and effectively communicated to the relevant internal and external interested parties.

The following should be considered:

a) establishing a common method for reporting information security events including point of contact (see 6.8);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) establishing an incident management process to provide the organization with capability for managing information security incidents including administration, documentation, detection, triage, prioritization, analysis, communication and coordinating interested parties;
c) establishing an incident response process to provide the organization with capability for assessing, responding to and learning from information security incidents;
d) only allowing competent personnel to handle the issues related to information security incidents within the organization. Such personnel should be provided with procedure documentation and periodic training;
e) establishing a process to identify required training, certification and ongoing professional development for incident response personnel.

Incident management procedures
The objectives for information security incident management should be agreed with management and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents including resolution time frame based on potential consequences and severity. Incident management procedures should be implemented to meet these objectives and priorities.

Management should ensure that an information security incident management plan is created considering different scenarios and procedures are developed and implemented for the following activities:
a) evaluation of information security events according to criteria for what constitutes an information security incident;
b) monitoring (see 8.15 and 8.16), detecting (see 8.16), classifying (see 5.25), analysing and reporting (see 6.8) of information security events and incidents (by human or automatic means);
c) managing information security incidents to conclusion, including response and escalation (see 5.26), according to the type and the category of the incident, possible activation of crisis management and activation of continuity plans, controlled recovery from an incident and communication to internal and external interested parties;
d) coordination with internal and external interested parties such as authorities, external interest groups and forums, suppliers and clients (see 5.5 and 5.6);
e) logging incident management activities;
f) handling of evidence (see 5.28);
g) root cause analysis or post-mortem procedures;
h) identification of lessons learned and any improvements to the incident management procedures or information security controls in general that are required.

Reporting procedures
Reporting procedures should include:
a) actions to be taken in case of an information security event (e.g. noting all pertinent details immediately such as malfunction occurring and messages on screen, immediately reporting to the point of contact and only taking coordinated actions);
b) use of incident forms to support personnel to perform all necessary actions when reporting information security incidents;
c) suitable feedback processes to ensure that those persons reporting information security events are notified, to the extent possible, of outcomes after the issue has been addressed and closed;
d) creation of incident reports.

Any external requirements on reporting of incidents to relevant interested parties within the defined time frame (e.g. breach notification requirements to regulators) should be considered when implementing incident management procedures.

Other information
Information security incidents can transcend organizational and national boundaries. To

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

respond to such incidents, it is beneficial to coordinate response and share information about these incidents with external organizations as appropriate.

Detailed guidance on information security incident management is provided in the ISO/IEC 27035 series.

5.25 Assessment and decision on information security events

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control
The organization should assess information security events and decide if they are to be categorized as information security incidents.

Purpose
To ensure effective categorization and prioritization of information security events.

Guidance
A categorization and prioritization scheme of information security incidents should be agreed for the identification of the consequences and priority of an incident. The scheme should include the criteria to categorize events as information security incidents. The point of contact should assess each informationsecurity event using the agreed scheme.

Personnel responsible for coordinating and responding to information security incidents should perform the assessment and make a decision on information security events.
Results of the assessment and decision should be recorded in detail for the purpose of future reference and verification.

Other information
The ISO/IEC 27035 series provides further guidance on incident management.

5.26 Response to information security incidents

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Control
Information security incidents should be responded to in accordance with the documented procedures.

Purpose
To ensure efficient and effective response to information security incidents.

Guidance
The organization should establish and communicate procedures on information security incident response to all relevant interested parties.

Information security incidents should be responded to by a designated team with the required competency (see 5.24).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

The response should include the following:
a) containing, if the consequences of the incident can spread, the systems affected by the incident;
b) collecting evidence (see 5.28) as soon as possible after the occurrence;
c) escalation, as required including crisis management activities and possibly invoking business continuity plans (see 5.29 and 5.30);
d) ensuring that all involved response activities are properly logged for later analysis;
e) communicating the existence of the information security incident or any relevant details thereof to all relevant internal and external interested parties following the need-to-know principle;
f) coordinating with internal and external parties such as authorities, external interest groups and forums, suppliers and clients to improve response effectiveness and help to minimize consequencesfor other organizations;
g) once the incident has been successfully addressed, formally closing and recording it;
h) conducting information security forensic analysis, as required (see 5.28);
i) performing post-incident analysis to identify root cause. Ensure it is documented and communicated according to defined procedures (see 5.27);
j) identifying and managing information security vulnerabilities and weaknesses including those related to controls which have caused, contributed to or failed to prevent the incident.

Other information
The ISO/IEC 27035 series provides further guidance on incident management.

5.27 Learning from information security incidents

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence

Control
Knowledge gained from information security incidents should be used to strengthen and improve theinformation security controls.

Purpose
To reduce the likelihood or consequences of future incidents.

Guidance
The organization should establish procedures to quantify and monitor the types, volumes and costs of information security incidents.

The information gained from the evaluation of information security incidents should be used to:
a) enhance the incident management plan including incident scenarios and procedures (see 5.24);
b) identify recurring or serious incidents and their causes to update the organization's information security risk assessment and determine and implement necessary additional controls to reduce the likelihood or consequences of future similar incidents. Mechanisms to enable that include collecting, quantifying and monitoring information about incident types, volumes and costs;
c) enhance user awareness and training (see 6.3) by providing examples of what can happen, how to respond to such incidents and how to avoid them in the future.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Other information
The ISO/IEC 27035 series provides further guidance.

5.28 Collection of evidence

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control
The organization should establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.

Purpose
To ensure a consistent and effective management of evidence related to information security incidents for the purposes of disciplinary and legal actions.

Guidance
Internal procedures should be developed and followed when dealing with evidence related to information security events for the purposes of disciplinary and legal actions. The requirements of different jurisdictions should be considered to maximize chances of admission across the relevant jurisdictions.

In general, these procedures for the management of evidence should provide instructions for the identification, collection, acquisition and preservation of evidence in accordance with different types of storage media, devices and status of devices (i.e. powered on or off). Evidence typically needs to be collected in a manner that is admissible in the appropriate national courts of law or another disciplinary forum. It should be possible to show that:

a) records are complete and have not been tampered with in any way;
b) copies of electronic evidence are probably identical to the originals;
c) any information system from which evidence has been gathered was operating correctly at the time the evidence was recorded.

Where available, certification or other relevant means of qualification of personnel and tools should be sought, so as to strengthen the value of the preserved evidence.

Digital evidence can transcend organizational or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as digital evidence.

Other information
When an information security event is first detected, it is not always obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve legal advice or law enforcement early in any contemplated legal action and take advice on the evidence required.

ISO/IEC 27037 provides definitions and guidelines for identification, collection, acquisition and preservation of digital evidence.

The ISO/IEC 27050 series deals with electronic discovery, which involves the processing of electronically stored information as evidence.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.29 Information security during disruption

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience

Control
The organization should plan how to maintain information security at an appropriate level during disruption.

Purpose
To protect information and other associated assets during disruption.

Guidance
The organization should determine its requirements for adapting information security controls during disruption. Information security requirements should be included in the business continuity management processes.

Plans should be developed, implemented, tested, reviewed and evaluated to maintain or restore the security of information of critical business processes following interruption or failure. Security of information should be restored at the required level and in the required time frames.

The organization should implement and maintain:
a) information security controls, supporting systems and tools within business continuity and ICT continuity plans;
b) processes to maintain existing information security controls during disruption;
c) compensating controls for information security controls that cannot be maintained during disruption.

Other information
In the context of business continuity and ICT continuity planning, it can be necessary to adapt the information security requirements depending on the type of disruption, compared to normal operational conditions. As part of the business impact analysis and risk assessment performed within business continuity management, the consequences of loss of confidentiality and integrity of information should be considered and prioritized in addition to the need for maintaining availability.

Information on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on business impact analysis (BIA) can be found in ISO/TS 22317.

5.30 ICT readiness for business continuity

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Availability	#Respond	#Continuity	#Resilience

Control
ICT readiness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.

Purpose
To ensure the availability of the organization's information and other associated assets during disruption.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance
ICT readiness for business continuity is an important component in business continuity management and information security management to ensure that the organization's objectives can continue to be met during disruption.

The ICT continuity requirements are the outcome of the business impact analysis (BIA). The BIA process should use impact types and criteria to assess the impacts over time resulting from the disruption of business activities that deliver products and services. The magnitude and duration of the resulting impact should be used to identify prioritized activities which should be assigned a recovery time objective (RTO). The BIA should then determine which resources are needed to support prioritized activities. An RTO should also be specified for these resources. A subset of these resources should include ICT services.

The BIA involving ICT services can be expanded to define performance and capacity requirements of ICT systems and recovery point objectives (RPO) of information required to support activities during disruption.

Based on the outputs from the BIA and risk assessment involving ICT services, the organization should identify and select ICT continuity strategies that consider options for before, during and after disruption. The business continuity strategies can comprise one or more solutions. Based on the strategies, plans should be developed, implemented and tested to meet the required availability level of ICT services and in the required time frames following interruption to, or failure of, critical processes.

The organization should ensure that:
a) an adequate organizational structure is in place to prepare for, mitigate and respond to a disruption supported by personnel with the necessary responsibility, authority and competence;
b) ICT continuity plans, including response and recovery procedures detailing how the organization is planning to manage an ICT service disruption, are:
    1) regularly evaluated through exercises and tests;
    2) approved by management;
c) ICT continuity plans include the following ICT continuity information:
    1) performance and capacity specifications to meet the business continuity requirements and objectives as specified in the BIA;
    2) RTO of each prioritized ICT service and the procedures for restoring those components;
    3) RPO of the prioritized ICT resources defined as information and the procedures for restoring the information.

Other information
Managing ICT continuity forms a key part of business continuity requirements concerning availability to be able to:
a) respond and recover from disruption to ICT services regardless of the cause;
b) ensure continuity of prioritized activities are supported by the required ICT services;
c) respond before a disruption to ICT services occurs, and upon detection of at least one incident that can result in a disruption to ICT services.

Further guidance on ICT readiness for business continuity can be found in ISO/IEC 27031.

Further guidance on business continuity management systems can be found in ISO 22301 and ISO 22313. Further guidance on BIA can be found in ISO/TS 22317.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

5.31 Legal, statutory, regulatory and contractual requirements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection

Control
Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements should be identified, documented and kept up to date.

Purpose
To ensure compliance with legal, statutory, regulatory and contractual requirements related to information security.

Guidance
General
External requirements including legal, statutory, regulatory or contractual requirements should be taken into consideration when:
a) developing information security policies and procedures;
b) designing, implementing or changing information security controls;
c) classifying information and other associated assets as part of the process for setting information security requirements for internal needs or for supplier agreements;
d) performing information security risk assessments and determining information security risk treatment activities;
e) determining processes along with related roles and responsibilities relating to information security;
f) determining suppliers' contractual requirements relevant to the organization and the scope of supply of products and services.

Legislation and regulations
The organization should:
a) identify all legislation and regulations relevant to the organization's information security in order to be aware of the requirements for their type of business;
b) take into consideration compliance in all relevant countries, if the organization:
   — conducts business in other countries;
   — uses products and services from other countries where laws and regulations can affect the organization;
   transfers information across jurisdictional borders where laws and regulations can affect the organization;
c) review the identified legislation and regulation regularly in order to keep up to date with the changes and identify new legislation;
d) define and document the specific processes and individual responsibilities to meet these requirements.

Cryptography
Cryptography is an area that often has specific legal requirements. Compliance with the relevant agreements, laws and regulations relating to the following items should be taken into consideration:
a) restrictions on import or export of computer hardware and software for performing cryptographic functions;
b) restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;
c) restrictions on the usage of cryptography;
d) mandatory or discretionary methods of access by the countries' authorities to encrypted

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

information;
e) validity of digital signatures, seals and certificates.

It is recommended to seek legal advice when ensuring compliance with relevant legislation and regulations, especially when encrypted information or cryptography tools are moved across jurisdictional borders.

Contracts
Contractual requirements related to information security should include those stated in:
a) contracts with clients;
b) contracts with suppliers (see 5.20);
c) insurance contracts.

Other information
No other information.

5.32 Intellectual property rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem

Control
The organization should implement appropriate procedures to protect intellectual property rights.

Purpose
To ensure compliance with legal, statutory, regulatory and contractual requirements related to intellectual property rights and use of proprietary products.

Guidance
The following guidelines should be considered to protect any material that can be considered intellectual property:
a) defining and communicating a topic-specific policy on protection of intellectual property rights;
b) publishing procedures for intellectual property rights compliance that define compliant use ofsoftware and information products;
c) acquiring software only through known and reputable sources, to ensure that copyright is not infringed upon;
d) maintaining appropriate asset registers and identifying all assets with requirements to protect intellectual property rights;
e) maintaining proof and evidence of ownership of licences, manuals, etc.;
f) ensuring that any maximum number of users or resources [e.g. central processing units (CPUs)] permitted within the licence is not exceeded;
g) carrying out reviews to ensure that only authorized software and licensed products are installed;
h) providing procedures for maintaining appropriate licence conditions;
i) providing procedures for disposing of or transferring software to others;
j) complying with terms and conditions for software and information obtained from public networks and outside sources;
k) not duplicating, converting to another format or extracting from commercial recordings (video, audio) other than permitted by copyright law or the applicable licences;
l) not copying, in full or in part, standards (e.g. ISO/IEC International Standards), books, articles, reports or other documents, other than permitted by copyright law or the

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

applicable licences.

Other information
Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Proprietary software products are usually supplied under a licence agreement that specifies licence terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of backup copies only. See the ISO/IEC 19770 series for details about IT asset management.

Data can be acquired from outside sources. It is generally the case that such data is obtained under the terms of a data sharing agreement or similar legal instrument. Such data sharing agreements should make it clear what processing is permitted for the acquired data. It is also advisable that the provenance of the data is clearly stated. See ISO/IEC 23751 for details about data sharing agreements.

Legal, statutory, regulatory and contractual requirements can place restrictions on the copying of proprietary material. In particular, they can require that only material that is developed by the organization or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which can involve fines and criminal proceedings.

Aside from the organization needing to comply with its obligations towards third party intellectual property rights, the risks of personnel and third parties failing to uphold the organization's own intellectual property rights should also be managed.

5.33 Protection of records

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence

Control
Records should be protected from loss, destruction, falsification, unauthorized access and unauthorized release.

Purpose
To ensure compliance with legal, statutory, regulatory and contractual requirements, as well as community or societal expectations related to the protection and availability of records.

Guidance
The organization should take the following steps to protect the authenticity, reliability, integrity and usability of records, as their business context and requirements for their management change over time:

a) issue guidelines on the storage, handling chain of custody and disposal of records, which includes prevention of manipulation of records. These guidelines should be aligned with the organization's topic-specific policy on records management and other records requirements;
b) draw up a retention schedule defining records and the period of time for which they should be retained.

The system of storage and handling should ensure identification of records and of their retention period taking into consideration national or regional legislation or regulations, as well

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

as community or societal expectations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

When deciding on protection of specific organizational records, their corresponding information security classification, based on the organization's classification scheme, should be considered. Records should be categorized into record types (e.g. accounting records, business transaction records, personnel records, legal records), each with details of retention periods and type of allowable storage media which can be physical or electronic.

Data storage systems should be chosen such that required records can be retrieved in an acceptable time frame and format, depending on the requirements to be fulfilled.

Where electronic storage media are chosen, procedures to ensure the ability to access records (both storage media and format readability) throughout the retention period should be established to safeguard against loss due to future technology change. Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be retained to enable decryption of the records for the length of time the records are retained (see 8.24).

Storage and handling procedures should be implemented in accordance with recommendations provided by manufacturers of storage media. Consideration should be given to the possibility of deterioration of media used for storage of records.

Other information
Records document individual events or transactions or can form aggregations that have been designed to document work processes, activities or functions. They are both evidence of business activity and information assets. Any set of information, regardless of its structure or form, can be managed as a record. This includes information in the form of a document, a collection of data or other types of digital or analogue information which are created, captured and managed in the course of business.

In the management of records, metadata is data describing the context, content and structure of records, as well as their management over time. Metadata is an essential component of any record.

It can be necessary to retain some records securely to meet legal, statutory, regulatory or contractual requirements, as well as to support essential business activities. National law or regulation can set the time period and data content for information retention. Further information about records management can be found in ISO 15489.

5.34 Privacy and protection of PII

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection

Control
The organization should identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.

Purpose
To ensure compliance with legal, statutory, regulatory and contractual requirements related to the information security aspects of the protection of PII.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance
The organization should establish and communicate a topic-specific policy on privacy and protection of PII to all relevant interested parties.

The organization should develop and implement procedures for the preservation of privacy and protection of PII. These procedures should be communicated to all relevant interested parties involved in the processing of personally identifiable information.

Compliance with these procedures and all relevant legislation and regulations concerning the preservation of privacy and protection of PII requires appropriate roles, responsibilities and controls. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to personnel, service providers and other interested parties on their individual responsibilities and the specific procedures that should be followed.

Responsibility for handling PII should be dealt with taking into consideration relevant legislation and regulations.
Appropriate technical and organizational measures to protect PII should be implemented.

Other information
A number of countries have introduced legislation placing controls on the collection, processing, transmission and deletion of PII. Depending on the respective national legislation, such controls can impose duties on those collecting, processing and disseminating PII and can also restrict the authority to transfer PII to other countries.

ISO/IEC 29100 provides a high-level framework for the protection of PII within ICT systems. Further information on privacy information management systems can be found in ISO/IEC 27701. Specific information regarding privacy information management for public clouds acting as PII processors can be found in ISO/IEC 27018.

ISO/IEC 29134 provides guidelines for privacy impact assessment (PIA) and gives an example of the structure and content of a PIA report. Compared with ISO/IEC 27005, this is focused on PII processing and relevant to those organizations that process PII. This can help identify privacy risks and possible mitigations to reduce these risks to acceptable levels.

5.35 Independent review of information security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem

Control
The organization's approach to managing information security and its implementation including people, processes and technologies should be reviewed independently at planned intervals, or when significant changes occur.

Purpose
To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security.

Guidance
The organization should have processes to conduct independent reviews.
Management should plan and initiate periodic independent reviews. The reviews should

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

include assessing opportunities for improvement and the need for changes to the approach to information security, including the information security policy, topic-specific policies and other controls.

Such reviews should be carried out by individuals independent of the area under review (e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews). Individuals carrying out these reviews should have the appropriate competence. The person conducting the reviews should not be in the line of authority to ensure they have the independence to make an assessment.

The results of the independent reviews should be reported to the management who initiated the reviews and, if appropriate, to top management. These records should be maintained.

If the independent reviews identify that the organization's approach and implementation to managing information security is inadequate [e.g. documented objectives and requirements are not met or are not compliant with the direction for information security stated in the information security policy and topic-specific policies (see 5.1)], management should initiate corrective actions.

In addition to the periodic independent reviews, the organization should consider conducting independent reviews when:

a) laws and regulations which affect the organization change;
b) significant incidents occur;
c) the organization starts a new business or changes a current business;
d) the organization starts to use a new product or service, or changes the use of a current product orservice;
e) the organization changes the information security controls and procedures significantly.

Other information

ISO/IEC 27007 and ISO/IEC TS 27008 provide guidance for carrying out independent reviews.

5.36 Compliance with policies, rules and standards for information security

Control type	Information security properties	Cybersecurity concepts	Operational capabil-ities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compli-ance #Information_securi-ty_assurance	#Governance_and_ Ecosystem

Control

Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly reviewed.

Purpose

To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards.

Guidance

Managers, service, product or information owners should identify how to review that information security requirements defined in the information security policy, topic-specific policies, rules,standards and other applicable regulations are met. Automatic measurement and reporting tools should be considered for efficient regular review.

If any non-compliance is found as a result of the review, managers should:

a) identify the causes of the non-compliance;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) evaluate the need for corrective actions to achieve compliance;
c) implement appropriate corrective actions;
d) review corrective actions taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers, service, product or information owners should be recorded and these records should be maintained. Managers should report the resultsto the persons carrying out independent reviews (see 5.35) when an independent review takes place in the area of their responsibility.

Corrective actions should be completed in a timely manner as appropriate to the risk. If not completed by the next scheduled review, progress should at least be addressed at that review.

Other information
Operational monitoring of system use is covered in 8.15, 8.16, 8.17.

5.37 Documented operating procedures

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protec-tion #Defence

Control
Operating procedures for information processing facilities should be documented and made available to personnel who need them.

Purpose
To ensure the correct and secure operation of information processing facilities.

Guidance
Documented procedures should be prepared for the organization's operational activities associated with information security, for example:
a) when the activity needs to be performed in the same way by many people;
b) when the activity is performed rarely and when next performed the procedure is likely to havebeen forgotten;
c) when the activity is new and presents a risk if not performed correctly;
d) prior to handing over the activity to new personnel.

The operating procedures should specify:
a) the responsible individuals;
b) the secure installation and configuration of systems;
c) processing and handling of information, both automated and manual;
d) backup (see 8.13) and resilience;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

e) scheduling requirements, including interdependencies with other systems;
f) instructions for handling errors or other exceptional conditions [e.g. restrictions on the use of utility programs (see 8.18)], which can arise during job execution;
g) support and escalation contacts including external support contacts in the event of unexpected operational or technical difficulties;
h) storage media handling instructions (see 7.10 and 7.14);
i) system restart and recovery procedures for use in the event of system failure;
j) the management of audit trail and system log information (see 8.15 and 8.17) and video monitoring systems (see 7.4);
k) monitoring procedures such as capacity, performance and security (see 8.6 and 8.16);
l) maintenance instructions.

Documented operating procedures should be reviewed and updated when needed. Changes to documented operating procedures should be authorized. Where technically feasible, information systems should be managed consistently, using the same procedures, tools and utilities.

Other information
No other information.

6 People controls

6.1 Screening

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control
Background verification checks on all candidates to become personnel should be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.

Purpose
To ensure all personnel are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

Guidance
A screening process should be performed for all personnel including full-time, part-time and temporary staff. Where these individuals are contracted through suppliers of services, screening requirements should be included in the contractual agreements between the organization and the suppliers.

Information on all candidates being considered for positions within the organization should be collected and handled taking into consideration any appropriate legislation existing in the relevant jurisdiction. In some jurisdictions, the organization can be legally required to inform the candidates beforehand about the screening activities.

Verification should take into consideration all relevant privacy, PII protection and employment-based legislation and should, where permitted, include the following:
a) availability of satisfactory references (e.g. business and personal references);
b) a verification (for completeness and accuracy) of the applicant's curriculum vitae;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

c) confirmation of claimed academic and professional qualifications;
d) independent identity verification (e.g. passport or other acceptable document issued by appropriate authorities);
e) more detailed verification, such as credit review or review of criminal records if the candidatetakes on a critical role.

When an individual is hired for a specific information security role, the organization should make sure the candidate:
a) has the necessary competence to perform the security role;
b) can be trusted to take on the role, especially if the role is critical for the organization.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities and, in particular, if these involve handling confidential information (e.g. financial information, personal information or health care information) the organization should also consider further, more detailed verifications.

Procedures should define criteria and limitations for verification reviews (e.g. who is eligible to screen people and how, when and why verification reviews are carried out).

In situations where verification cannot be completed in a timely manner, mitigating controls should be implemented until the review has been finished, for example:
a) delayed onboarding;
b) delayed deployment of corporate assets;
c) onboarding with reduced access;
d) termination of employment.

Verification checks should be repeated periodically to confirm ongoing suitability of personnel, depending on the criticality of a person's role.

Other information
No other information.

6.2 Terms and conditions of employment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control
The employment contractual agreements should state the personnel's and the organization's responsibilities for information security.

Purpose
To ensure personnel understand their information security responsibilities for the roles for which they are considered.

Guidance
The contractual obligations for personnel should take into consideration the organization's information security policy and relevant topic-specific policies. In addition, the following points can be clarified and stated:
a) confidentiality or non-disclosure agreements that personnel who are given access to confidential information should sign prior to being given access to information and other associated assets (see 6.6);
b) legal responsibilities and rights [e.g. regarding copyright laws or data protection

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

legislation (see 5.32 and 5.34)];
c) responsibilities for the classification of information and management of the organization's information and other associated assets, information processing facilities and information services handled by the personnel (see 5.9 to 5.13);
d) responsibilities for the handling of information received from interested parties;
e) actions to be taken if personnel disregard the organization's security requirements (see 6.4).

Information security roles and responsibilities should be communicated to candidates during the pre- employment process.

The organization should ensure that personnel agree to terms and conditions concerning information security. These terms and conditions should be appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services. The terms and conditions concerning information security should be reviewed when laws, regulations, the information security policy or topic-specific policies change.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see 6.5).

Other information
A code of conduct can be used to state personnel's information security responsibilities regarding confidentiality, PII protection, ethics, appropriate use of the organization's information and other associated assets, as well as reputable practices expected by the organization.

An external party, with which supplier personnel are associated, can be required to enter into contractual agreements on behalf of the contracted individual.

If the organization is not a legal entity and does not have employees, the equivalent of contractual agreement and terms and conditions can be considered in line with the guidance of this control.

6.3 Information security awareness, education and training

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_ security	#Governance_and_ Ecosystem

Control
Personnel of the organization and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.

Purpose
To ensure personnel and relevant interested parties are aware of and fulfil their information security responsibilities.

Guidance
General
An information security awareness, education and training programme should be established in line with the organization's information security policy, topic-specific policies and relevant procedures on information security, taking into consideration the organization's information to be protected and the information security controls that have been implemented to protect the

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

information.

Information security awareness, education and training should take place periodically. Initial awareness, education and training can apply to new personnel and to those who transfer to newpositions or roles with substantially different information security requirements.

Personnel's understanding should be assessed at the end of an awareness, education or training activityto test knowledge transfer and the effectiveness of the awareness, education and training programme.

Awareness
An information security awareness programme should aim to make personnel aware of their responsibilities for information security and the means by which those responsibilities are discharged.

The awareness programme should be planned taking into consideration the roles of personnel in the organization, including internal and external personnel (e.g. external consultants, supplier personnel). The activities in the awareness programme should be scheduled over time, preferably regularly, so that the activities are repeated and cover new personnel. It should also be built on lessons learnt from information security incidents.

The awareness programme should include a number of awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules and e-mails.

Information security awareness should cover general aspects such as:
a) management's commitment to information security throughout the organization;
b) familiarity and compliance needs concerning applicable information security rules and obligations, taking into account information security policy and topic-specific policies, standards, laws, statutes, regulations, contracts and agreements;
c) personal accountability for one's own actions and inactions, and general responsibilities towards securing or protecting information belonging to the organization and interested parties;
d) basic information security procedures [e.g. information security event reporting (6.8)] and baselinecontrols [e.g. password security (5.17)];
e) contact points and resources for additional information and advice on information security matters, including further information security awareness materials.

Education and training
The organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. Technical teams should have the skills for configuring and maintaining the required security level for devices, systems, applications and services. If there are missing skills, the organization should take action and acquire them.

The education and training programme should consider different forms [e.g. lectures or self-studies, being mentored by expert staff or consultants (on-the-job training), rotating staff members to follow different activities, recruiting already skilled people and hiring consultants]. It can use different means of delivery including classroom-based, distance learning, web-based, self-paced and others. Technical personnel should keep their knowledge up to date by subscribing to newsletters and magazines or by attending conferences and events aimed at technical and professional improvement.

Other information
When composing an awareness programme, it is important not only to focus on the 'what' and 'how', but also the 'why', when possible. It is important that personnel understand the aim of information security and the potential effect, positive and negative, on the organization of their own behaviour.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Information security awareness, education and training can be part of, or conducted in collaboration with, other activities, for example general information management, ICT, security, privacy or safety training.

6.4 Disciplinary process

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource _ security	#Governance_and_ Ecosystem

Control
A disciplinary process should be formalized and communicated to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

Purpose
To ensure personnel and other relevant interested parties understand the consequences of information security policy violation, to deter and appropriately deal with personnel and other relevant interested parties who committed the violation.

Guidance
The disciplinary process should not be initiated without prior verification that an information security policy violation has occurred (see 5.28).

The formal disciplinary process should provide for a graduated response that takes into consideration factors such as:
a) the nature (who, what, when, how) and gravity of the breach and its consequences;
b) whether the offence was intentional (malicious) or unintentional (accidental);
c) whether or not this is a first or repeated offence;
d) whether or not the violator was properly trained.

The response should take into consideration relevant legal, statutory, regulatory contractual and business requirements as well as other factors as required. The disciplinary process should also be used as a deterrent to prevent personnel and other relevant interested parties from violating the information security policy, topic-specific policies and procedures for information security. Deliberate information security policy violations can require immediate actions.

Other information
Where possible, the identity of individuals subject to disciplinary action should be protected in linewith applicable requirements.

When individuals demonstrate excellent behaviour with regard to information security, they can be rewarded to promote information security and encourage good behaviour.

6.5 Responsibilities after termination or change of employment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource _ security #Asset_managem ent	#Governance_and _ Ecosystem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Control
Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant personnel and other interested parties.

Purpose
To protect the organization's interests as part of the process of changing or terminating employment or contracts.

Guidance
The process for managing termination or change of employment should define which information security responsibilities and duties should remain valid after termination or change. This can include confidentiality of information, intellectual property and other knowledge obtained, as well as responsibilities contained within any other confidentiality agreement (see 6.6). Responsibilities and duties still valid after termination of employment or contract should be contained in the individual's terms and conditions of employment (see 6.2), contract or agreement. Other contracts or agreements that continue for a defined period after the end of the individual's employment can also contain information security responsibilities.
Changes of responsibility or employment should be managed as the termination of the current responsibility or employment combined with the initiation of the new responsibility or employment.

Information security roles and responsibilities held by any individual who leaves or changes job roles should be identified and transferred to another individual.

A process should be established for the communication of the changes and of operating procedures to personnel, other interested parties and relevant contact persons (e.g. to customers and suppliers).

The process for the termination or change of employment should also be applied to external personnel (i.e. suppliers) when a termination occurs of personnel, the contract or the job with the organization, or when there is a change of the job within the organization.

Other information
In many organizations, the human resources function is generally responsible for the overall termination process and works together with the supervising manager of the person transitioning to manage the information security aspects of the relevant procedures. In the case of personnel provided through an external party (e.g. through a supplier), this termination process is undertaken by the external party in accordance with the contract between the organization and the external party.

6.6 Confidentiality or non-disclosure agreements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem

Control
Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.

Purpose
To maintain confidentiality of information accessible by personnel or external parties.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance
Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. Confidentiality or non-disclosure agreements are applicable to interested parties and personnel of the organization. Based on an organization's information security requirements, the terms in the agreements should be determined by taking into consideration the type of information that will be handled, its classification level, its use and the permissible access by the other party. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);
b) the expected duration of an agreement, including cases where it can be necessary to maintain confidentiality indefinitely or until the information becomes publicly available;
c) the required actions when an agreement is terminated;
d) the responsibilities and actions of signatories to avoid unauthorized information disclosure;
e) the ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
f) the permitted use of confidential information and rights of the signatory to use the information;
g) the right to audit and monitor activities that involve confidential information for highly sensitive circumstances;
h) the process for notification and reporting of unauthorized disclosure or confidential information leakage;
i) the terms for information to be returned or destroyed at agreement termination;
j) the expected actions to be taken in the case of non-compliance with the agreement.

The organization should take into consideration the compliance with confidentiality and non-disclosure agreements for the jurisdiction to which they apply (see 5.31, 5.32, 5.33, 5.34).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other information
Confidentiality and non-disclosure agreements protect the organization's information and inform signatories of their responsibility to protect, use and disclose information in a responsible and authorized manner

6.7 Remote working

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protec-tion #Physical_security #System_and_net-work_security	#Protection

Control
Security measures should be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.

Purpose
To ensure the security of information when personnel are working remotely.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance

Remote working occurs whenever personnel of the organization work from a location outside of the organization's premises, accessing information whether in hardcopy or electronically via ICT equipment. Remote working environments include those referred to as "teleworking", "telecommuting", "flexible workplace", "virtual work environments" and "remote maintenance".

NOTE It is possible that not all the recommendations in this guidance can be applied due to local legislation and regulations in different jurisdictions.

Organizations allowing remote working activities should issue a topic-specific policy on remote working that defines the relevant conditions and restrictions. Where deemed applicable, the following matters should be considered:

a) the existing or proposed physical security of the remote working site, taking into account the physical security of the location and the local environment, including the different jurisdictions where personnel are located;
b) rules and security mechanisms for the remote physical environment such as lockable filing cabinets, secure transportation between locations and rules for remote access, clear desk, printing and disposal of information and other associated assets, and information security event reporting (see 6.8);
c) the expected physical remote working environments;
d) the communications security requirements, taking into account the need for remote access to the organization's systems, the sensitivity of the information to be accessed and passed over the communication link and the sensitivity of the systems and applications;
e) the use of remote access such as virtual desktop access that supports processing and storage of information on privately owned equipment;
f) the threat of unauthorized access to information or resources from other persons at the remote working site (e.g. family and friends);
g) the threat of unauthorized access to information or resources from other persons in public places;
h) the use of home networks and public networks, and requirements or restrictions on the configuration of wireless network services;
i) use of security measures, such as firewalls and protection against malware;
j) secure mechanisms for deploying and initializing systems remotely;
k) secure mechanisms for authentication and enablement of access privileges taking into consideration the vulnerability of single-factor authentication mechanisms where remote access to the organization's network is allowed.

The guidelines and measures to be considered should include:

a) the provision of suitable equipment and storage furniture for the remote working activities, where the use of privately-owned equipment that is not under the control of the organization is not allowed;
b) a definition of the work permitted, the classification of information that can be held and the internal systems and services that the remote worker is authorized to access;
c) the provision of training for those working remotely and those providing support. This should include how to conduct business in a secure manner while working remotely;
d) the provision of suitable communication equipment, including methods for securing remote access, such as requirements on device screen locks and inactivity timers; the enabling of device location tracking; installation of remote wipe capabilities;
e) physical security;
f) rules and guidance on family and visitor access to equipment and information;
g) the provision of hardware and software support and maintenance;
h) the provision of insurance;
i) the procedures for backup and business continuity;
j) audit and security monitoring;
k) revocation of authority and access rights and the return of equipment when the remote working activities are terminated.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Other information
No other information.

6.8 Information security event reporting

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence

Control
The organization should provide a mechanism for personnel to report observed or suspectedinformation security events through appropriate channels in a timely manner.

Purpose
To support timely, consistent and effective reporting of information security events that can be identified by personnel.

Guidance
All personnel and users should be made aware of their responsibility to report information security events as quickly as possible in order to prevent or minimize the effect of information security incidents.

They should also be aware of the procedure for reporting information security events and the point of contact to which the events should be reported. The reporting mechanism should be as easy, accessible and available as possible. Information security events include incidents, breaches and vulnerabilities.

Situations to be considered for information security event reporting include:
a) ineffective information security controls;
b) breach of information confidentiality, integrity or availability expectations;
c) human errors;
d) non-compliance with the information security policy, topic-specific policies or applicable standards;
e) breaches of physical security measures;
f) system changes that have not gone through the change management process;
g) malfunctions or other anomalous system behaviour of software or hardware;
h) access violations;
i) vulnerabilities;
j) suspected malware infection.

Personnel and users should be advised not to attempt to prove suspected information security vulnerabilities. Testing vulnerabilities can be interpreted as a potential misuse of the system and can also cause damage to the information system or service, and it can corrupt or obscure digital evidence. Ultimately, this can result in legal liability for the individual performing the testing.

Other information
See the ISO/IEC 27035 series for additional information.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7 Physical controls

7.1 Physical security perimeters

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control
Security perimeters should be defined and used to protect areas that contain information and other associated assets.

Purpose
To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets.

Guidance
The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) defining security perimeters and the siting and strength of each of the perimeters in accordance with the information security requirements related to the assets within the perimeter;
b) having physically sound perimeters for a building or site containing information processing facilities (i.e. there should be no gaps in the perimeter or areas where a break-in can easily occur). The exterior roofs, walls, ceilings and flooring of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms (e.g. bars, alarms, locks). Doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level; ventilation points should also be considered;
c) alarming, monitoring and testing all fire doors on a security perimeter in conjunction with the walls to establish the required level of resistance in accordance with suitable standards. They should operate in a failsafe manner.

Other information
Physical protection can be achieved by creating one or more physical barriers around the organization'spremises and information processing facilities.

A secure area can be a lockable office or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access can be necessary between areas with different security requirements inside the security perimeter. The organization should consider having physical security measures that can be strengthened during increased threat situations.

7.2 Pshysical entry

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Identity_and_Ac-cess_Management	#Protection

Control
Secure areas should be protected by appropriate entry controls and access points.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To ensure only authorized physical access to the organization's information and other associated assets occurs.

Guidance
General
Access points such as delivery and loading areas and other points where unauthorized persons can enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

The following guidelines should be considered:
a) restricting access to sites and buildings to authorized personnel only. The process for the management of access rights to physical areas should include the provision, periodical review, update and revocation of authorizations (see 5.18);
b) securely maintaining and monitoring a physical logbook or electronic audit trail of all access and protecting all logs (see 5.33) and sensitive authentication information;
c) establishing and implementing a process and technical mechanisms for the management of access to areas where information is processed or stored. Authentication mechanisms include the use of access cards, biometrics or two-factor authentication such as an access card and secret PIN. Double security doors should be considered for access to sensitive areas;
d) setting up a reception area monitored by personnel, or other means to control physical access tothe site or building;
e) inspecting and examining personal belongings of personnel and interested parties upon entry and exit;
NOTE Local legislation and regulations can exist regarding the possibility of inspecting personal belongings.
f) requiring all personnel and interested parties to wear some form of visible identification andto immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification. Easily distinguishable badges should be considered to better identify permanent employees, suppliers and visitors;
g) granting supplier personnel restricted access to secure areas or information processing facilities only when required. This access should be authorized and monitored;
h) giving special attention to physical access security in the case of buildings holding assets for multiple organizations;
i) designing physical security measures so that they can be strengthened when the likelihood of physical incidents increases;
j) securing other entry points such as emergency exits from unauthorized access;
k) setting up a key management process to ensure the management of the physical keys or authentication information (e.g. lock codes, combination locks to offices, rooms and facilities such as key cabinets) and to ensure a log book or annual key audit and that access to physicalkeys or authentication information is controlled (see 5.17 for further guidance on authentication information).

Visitors
The following guidelines should be considered:
a) authenticating the identity of visitors by an appropriate means;
b) recording the date and time of entry and departure of visitors;
c) only granting access for visitors for specific, authorized purposes and with instructions on thesecurity requirements of the area and on emergency procedures;
d) supervising all visitors, unless an explicit exception is granted.

Delivery and loading areas and incoming material
The following guidelines should be considered:
a) restricting access to delivery and loading areas from outside of the building to identified andauthorized personnel;
b) designing the delivery and loading areas so that deliveries can be loaded and

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

unloaded without delivery personnel gaining unauthorized access to other parts of the building;
c) securing the external doors of delivery and loading areas when doors to restricted areas are opened;
d) inspecting and examining incoming deliveries for explosives, chemicals or other hazardous materials before they are moved from delivery and loading areas;
e) registering incoming deliveries in accordance with asset management procedures (see 5.9 and 7.10) on entry to the site;
f) physically segregating incoming and outgoing shipments, where possible;
g) inspecting incoming deliveries for evidence of tampering on the way. If tampering is discovered, it should be immediately reported to security personnel.

Other information
No other information.

7.3 Securing offices, rooms and facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control
Physical security for offices, rooms and facilities should be designed and implemented.

Purpose
To prevent unauthorized physical access, damage and interference to the organization's information and other associated assets in offices, rooms and facilities.

Guidance
The following guidelines should be considered to secure offices, rooms and facilities:
a) siting critical facilities to avoid access by the public;
b) where applicable, ensuring buildings are unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities;
c) configuring facilities to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate;
d) not making directories, internal telephone books and online accessible maps identifying locations of confidential information processing facilities readily available to any unauthorized person.

Other information
No other information.

7.4 Physical security monitoring

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence

Control
Premises should be continuously monitored for unauthorized physical access.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To detect and deter unauthorized physical access.

Guidance
Physical premises should be monitored by surveillance systems, which can include guards, intruder alarms, video monitoring systems such as closed-circuit television and physical security information management software either managed internally or by a monitoring service provider.

Access to buildings that house critical systems should be continuously monitored to detect unauthorized access or suspicious behaviour by:

a) installing video monitoring systems such as closed-circuit television to view and record access to sensitive areas within and outside an organization's premises;
b) installing, according to relevant applicable standards, and periodically testing contact, sound or motion detectors to trigger an intruder alarm such as:
    1) installing contact detectors that trigger an alarm when a contact is made or broken in any place where a contact can be made or broken (such as windows and doors and underneath objects) to be used as a panic alarm;
    2) motion detectors based on infra-red technology which trigger an alarm when an object passes through their field of view;
    3) installing sensors sensitive to the sound of breaking glass which can be used to trigger an alarm to alert security personnel;
c) using those alarms to cover all external doors and accessible windows. Unoccupied areas should be alarmed at all times; cover should also be provided for other areas (e.g. computer or communications rooms).

The design of monitoring systems should be kept confidential because disclosure can facilitate undetected break-ins.

Monitoring systems should be protected from unauthorized access in order to prevent surveillance information, such as video feeds, from being accessed by unauthorized persons or systems being disabled remotely.

The alarm system control panel should be placed in an alarmed zone and, for safety alarms, in a place that allows an easy exit route for the person who sets the alarm. The control panel and the detectors should have tamperproof mechanisms. The system should regularly be tested to ensure that it is working as intended, particularly if its components are battery powered.

Any monitoring and recording mechanism should be used taking into consideration local laws and regulations including data protection and PII protection legislation, especially regarding the monitoring of personnel and recorded video retention periods.

Other information
No other information.

7.5 Protecting against physical and environmental threats

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control
Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure should be designed and

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

implemented.

Purpose
To prevent or reduce the consequences of events originating from physical and environmental threats.

Guidance
Risk assessments to identify the potential consequences of physical and environmental threats should be performed prior to beginning critical operations at a physical site, and at regular intervals. Necessary safeguards should be implemented and changes to threats should be monitored. Specialist advice should be obtained on how to manage risks arising from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

Physical premises location and construction should take account of:
a) local topography, such as appropriate elevation, bodies of water and tectonic fault lines;
b) urban threats, such as locations with a high profile for attracting political unrest, criminal activity or terrorist attacks.

Based on risk assessment results, relevant physical and environmental threats should be identified and appropriate controls considered in the following contexts as examples:
a) fire: installing and configuring systems able to detect fires at an early stage to send alarms or trigger fire suppression systems in order to prevent fire damage to storage media and to related information processing systems. Fire suppression should be performed using the most appropriate substance with regard to the surrounding environment (e.g. gas in confined spaces);
b) flooding: installing systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems. Water pumps or equivalent means should be readily made available in case flooding occurs;
c) electrical surges: adopting systems able to protect both server and client information systems against electrical surges or similar events to minimize the consequences of such events;
d) explosives and weapons: performing random inspections for the presence of explosives or weapons on personnel, vehicles or goods entering sensitive information processing facilities.

Other information
Safes or other forms of secure storage facilities can protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Organizations can consider the concepts of crime prevention through environmental design when designing the controls to secure their environment and reduce urban threats. For example, instead of using bollards, statues or water features can serve as both a feature and a physical barrier.

7.6 Working in secure areas

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Control
Security measures for working in secure areas should be designed and implemented.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To protect information and other associated assets in secure areas from damage and unauthorized interference by personnel working in these areas.

Guidance
The security measures for working in secure areas should apply to all personnel and cover all activities taking place in the secure area.

The following guidelines should be considered:
a) making personnel aware only of the existence of, or activities within, a secure area on a need-to-know basis;
b) avoiding unsupervised work in secure areas both for safety reasons and to reduce chances for malicious activities;
c) physically locking and periodically inspecting vacant secure areas;
d) not allowing photographic, video, audio or other recording equipment, such as cameras in user endpoint devices, unless authorized;
e) appropriately controlling the carrying and use of user endpoint devices in secure areas;
f) posting emergency procedures in a readily visible or accessible manner.

Other information
No other information.

7.7 Clear desk and clear screen

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection

Control
Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities should be defined and appropriately enforced.

Purpose
To reduce the risks of unauthorized access, loss of and damage to information on desks, screens and in other accessible locations during and outside normal working hours.

Guidance
The organization should establish and communicate a topic-specific policy on clear desk and clear screen to all relevant interested parties.
The following guidelines should be considered:
a) locking away sensitive or critical business information (e.g. on paper or on electronic storage media) (ideally in a safe, cabinet or other form of security furniture) when not required, especially when the office is vacated;
b) protecting user endpoint devices by key locks or other security means when not in use or unattended;
c) leaving user endpoint devices logged off or protected with a screen and keyboard locking mechanism controlled by a user authentication mechanism when unattended. All computers and systems should be configured with a timeout or automatic logout feature;
d) making the originator collect outputs from printers or multi-function devices immediately. The use of printers with an authentication function, so the originators are the only ones who can get their printouts and only when standing next to the printer;
e) securely storing documents and removable storage media containing sensitive information and, when no longer required, discarding them using secure disposal mechanisms;
f) establishing and communicating rules and guidance for the configuration of pop-ups on screens (e.g. turning off the new email and messaging pop-ups, if possible, during presentations, screen sharing or in a public area);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

g) clearing sensitive or critical information on whiteboards and other types of display when no longer required.

The organization should have procedures in place when vacating facilities including conducting a final sweep prior to leaving to ensure the organization's assets are not left behind (e.g. documents fallen behind drawers or furniture).

Other information
No other information.

7.8 Equipment siting and protection

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control
Equipment should be sited securely and protected.

Purpose
To reduce the risks from physical and environmental threats, and from unauthorized access and damage.

Guidance
The following guidelines should be considered to protect equipment:
a) siting equipment to minimize unnecessary access into work areas and to avoid unauthorized access;
b) carefully positioning information processing facilities handling sensitive data to reduce the risk of information being viewed by unauthorized persons during their use;
c) adopting controls to minimize the risk of potential physical and environmental threats [e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation and vandalism];
d) establishing guidelines for eating, drinking and smoking in proximity to information processing facilities;
e) monitoring environmental conditions, such as temperature and humidity, for conditions which can adversely affect the operation of information processing facilities;
f) applying lightning protection to all buildings and fitting lightning protection filters to all incoming power and communications lines;
g) considering the use of special protection methods, such as keyboard membranes, for equipment in industrial environments;
h) protecting equipment processing confidential information to minimize the risk of information leakage due to electromagnetic emanation;
i) physically separating information processing facilities managed by the organization from those not managed by the organization.

Other information
No other information.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7.9 Security of assets off-premises

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control
Off-site assets should be protected.

Purpose
To prevent loss, damage, theft or compromise of off-site devices and interruption to the organization's operations.

Guidance
Any device used outside the organization's premises which stores or processes information (e.g. mobile device), including devices owned by the organization and devices owned privately and used on behalf of the organization [bring your own device (BYOD)] needs protection. The use of these devices should be authorized by management.

The following guidelines should be considered for the protection of devices which store or process

information outside the organization's premises:
a) not leaving equipment and storage media taken off premises unattended in public and unsecured places;
b) observing manufacturers' instructions for protecting equipment at all times (e.g. protection against exposure to strong electromagnetic fields, water, heat, humidity, dust);
c) when off-premises equipment is transferred among different individuals or interested parties, maintaining a log that defines the chain of custody for the equipment including at least names and organizations of those who are responsible for the equipment. Information that does not need to betransferred with the asset should be securely deleted before the transfer;
d) where necessary and practical, requiring authorization for equipment and media to be removed from the organization's premises and keeping a record of such removals in order to maintain an audit trail (see 5.14);
e) protecting against viewing information on a device (e.g. mobile or laptop) on public transport, and the risks associated with shoulder surfing;
f) implementing location tracking and ability for remote wiping of devices.

Permanent installation of equipment outside the organization's premises [such as antennas and automated teller machines (ATMs)] can be subject to higher risk of damage, theft or eavesdropping. These risks can vary considerably between locations and should be taken into account in determining the most appropriate measures. The following guidelines should be considered when siting this equipment outside of the organization's premises:
a) physical security monitoring (see 7.4);
b) protecting against physical and environmental threats (see 7.5);
c) physical access and tamper proofing controls;
d) logical access controls.

Other information
More information about other aspects of protecting information storing and processing equipment and user endpoint devices can be found in 8.1 and 6.7.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

7.10 Storage media

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Control
Storage media should be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.

Purpose
To ensure only authorized disclosure, modification, removal or destruction of information on storage media.

Guidance
Removable storage media
The following guidelines for the management of removable storage media should be considered:

a) establishing a topic-specific policy on the management of removable storage media and communicating such topic- specific policy to anyone who uses or handles removable storage media;
b) where necessary and practical, requiring authorization for storage media to be removed from the organization and keeping a record of such removals in order to maintain an audit trail;
c) storing all storage media in a safe, secure environment according to their information classification and protecting them against environmental threats (such as heat, moisture, humidity, electronic field or ageing), in accordance with manufacturers' specifications;
d) if information confidentiality or integrity are important considerations, using cryptographic techniques to protect information on removable storage media;
e) to mitigate the risk of storage media degrading while stored information is still needed, transferringthe information to fresh storage media before becoming unreadable;
f) storing multiple copies of valuable information on separate storage media to further reduce therisk of coincidental information damage or loss;
g) considering the registration of removable storage media to limit the chance for information loss;
h) only enabling removable storage media ports [e.g. secure digital (SD) card slots and universal serialbus (USB) ports] if there is an organizational reason for their use;
i) where there is a need to use removable storage media, monitoring the transfer of information to such storage media;
j) information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending storage media via the postal service or via courier.

In this control, media includes paper documents. When transferring physical storage media, applysecurity measures in 5.14.

Secure reuse or disposal
Procedures for the secure reuse or disposal of storage media should be established to minimize therisk of confidential information leakage to unauthorized persons. The procedures for secure reuse or disposal of storage media containing confidential information should be proportional to the sensitivity of that information. The following items should be considered:

a) if storage media containing confidential information need to be reused within the organization,securely deleting data or formatting the storage media before reuse (see 8.10);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) disposing of storage media containing confidential information securely when not needed anymore (e.g. by destroying, shredding or securely deleting the content);
c) having procedures in place to identify the items that can require secure disposal;
d) many organizations offer collection and disposal services for storage media. Care should be takenin selecting a suitable external party supplier with adequate controls and experience;
e) logging the disposal of sensitive items in order to maintain an audit trail;
f) when accumulating storage media for disposal, giving consideration to the aggregation effect, which can cause a large quantity of non-sensitive information to become sensitive.

A risk assessment should be performed on damaged devices containing sensitive data to determine whether the items should be physically destroyed rather than sent for repair or discarded (see 7.14).

Other information
When confidential information on storage media is not encrypted, additional physical protection of the storage media should be considered.

7.11 Supporting utilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection

Control
Information processing facilities should be protected from power failures and other disruptions caused by failures in supporting utilities.

Purpose
To prevent loss, damage or compromise of information and other associated assets, or interruption to the organization's operations due to failure and disruption of supporting utilities.

Guidance
Organizations depend on utilities (e.g. electricity, telecommunications, water supply, gas, sewage, ventilation and air conditioning) to support their information processing facilities. Therefore, the organization should:
a) ensure equipment supporting the utilities is configured, operated and maintained in accordance with the relevant manufacturer's specifications;
b) ensure utilities are appraised regularly for their capacity to meet business growth and interactions with other supporting utilities;
c) ensure equipment supporting the utilities is inspected and tested regularly to ensure their proper functioning;
d) if necessary, raise alarms to detect utilities malfunctions;
e) if necessary, ensure utilities have multiple feeds with diverse physical routing;
f) ensure equipment supporting the utilities is on a separate network from the information processing facilities if connected to a network;
g) ensure equipment supporting the utilities is connected to the internet only when needed and only in a secure manner.

Emergency lighting and communications should be provided. Emergency switches and valves to cut off power, water, gas or other utilities should be located near emergency exits or equipment rooms. Emergency contact details should be recorded and available to personnel in the event of an outage.

Other information
Additional redundancy for network connectivity can be obtained by means of multiple

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

routes frommore than one utility provider.

7.12 Cabling security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection

Control
Cables carrying power, data or supporting information services should be protected from interception, interference or damage.

Purpose
To prevent loss, damage, theft or compromise of information and other associated assets and interruption to the organization's operations related to power and communications cabling.

Guidance
The following guidelines for cabling security should be considered:
a) power and telecommunications lines into information processing facilities being underground where possible, or subject to adequate alternative protection, such as floor cable protector and utility pole; if cables are underground, protecting them from accidental cuts (e.g. with armoured conduits or signals of presence);
b) segregating power cables from communications cables to prevent interference;
c) for sensitive or critical systems, further controls to consider include:
    1) installation of armoured conduit and locked rooms or boxes and alarms at inspection andtermination points;
    2) use of electromagnetic shielding to protect the cables;
    3) periodical technical sweeps and physical inspections to detect unauthorized devices beingattached to the cables;
    4) controlled access to patch panels and cable rooms (e.g. with mechanical keys or PINs);
    5) use of fibre-optic cables;
d) labelling cables at each end with sufficient source and destination details to enable the physical identification and inspection of the cable.

Specialist advice should be sought on how to manage risks arising from cabling incidents ormalfunctions.

Other information
Sometimes power and telecommunications cabling are shared resources for more than one organization occupying co-located premises.

7.13 Equipment maintenance

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

Control
Equipment should be maintained correctly to ensure availability, integrity and confidentiality of information.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To prevent loss, damage, theft or compromise of information and other associated assets andinterruption to the organization's operations caused by lack of maintenance.

Guidance
The following guidelines for equipment maintenance should be considered:
a) maintaining equipment in accordance with the supplier's recommended service frequency and specifications;
b) implementing and monitoring of a maintenance programme by the organization;
c) only authorized maintenance personnel carrying out repairs and maintenance on equipment;
d) keeping records of all suspected or actual faults, and of all preventive and corrective maintenance;
e) implementing appropriate controls when equipment is scheduled for maintenance, taking intoaccount whether this maintenance is performed by personnel on site or external to the organization; subjecting the maintenance personnel to a suitable confidentiality agreement;
f) supervising maintenance personnel when carrying out maintenance on site;
g) authorizing and controlling access for remote maintenance;
h) applying security measures for assets off-premises (see 7.9) if equipment containing information istaken off premises for maintenance;
i) complying with all maintenance requirements imposed by insurance;
j) before putting equipment back into operation after maintenance, inspecting it to ensure that theequipment has not been tampered with and is functioning properly;
k) applying measures for secure disposal or re-use of equipment (see 7.14) if it is determined that equipment is to be disposed of.

Other information
Equipment includes technical components of information processing facilities, uninterruptible power supply (UPS) and batteries, power generators, power alternators and converters, physical intrusion detection systems and alarms, smoke detectors, fire extinguishers, air conditioning and lifts.

7.14 Secure disposal or re-use of equipment

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection

Control
Items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Purpose
To prevent leakage of information from equipment to be disposed or re-used.

Guidance
Equipment should be verified to ensure whether or not storage media is contained prior to disposal or re-use.

Storage media containing confidential or copyrighted information should be physically destroyed orthe information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete function. See 7.10 for detailed guidance on secure disposal of storage media and 8.10 for guidance on

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

information deletion.

Labels and markings identifying the organization or indicating the classification, owner, system or network, should be removed prior to disposal, including reselling or donating to charity.

The organization should consider the removal of security controls such as access controls or surveillance equipment at the end of lease or when moving out of premises. This depends on factors such as:
a) its lease agreement to return the facility to original condition;
b) minimizing the risk of leaving systems with sensitive information on them for the next tenant (e.g. user access lists, video or image files);
c) the ability to reuse the controls at the next facility.

Other information
Damaged equipment containing storage media can require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded. Information can be compromised through careless disposal or re-use of equipment.

In addition to secure disk deletion, full-disk encryption reduces the risk of disclosure of confidential information when equipment is disposed of or redeployed, provided that:
a) the encryption process is sufficiently strong and covers the entire disk (including slack space, swap files);
b) the cryptographic keys are long enough to resist brute force attacks;
c) the cryptographic keys are themselves kept confidential (e.g. never stored on the same disk). For further advice on cryptography, see 8.24.

Techniques for securely overwriting storage media differ according to the storage media technology and the classification level of the information on the storage media. Overwriting tools should be reviewed to make sure that they are applicable to the technology of the storage media.

See ISO/IEC 27040 for detail on methods for sanitizing storage media.

8 Technological controls

8.1 User endpoint devices

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection

Control
Information stored on, processed by or accessible via user endpoint devices should be protected.

Purpose
To protect information against the risks introduced by using user endpoint devices.

Guidance
General
The organization should establish a topic-specific policy on secure configuration and handling of user endpoint devices. The topic-specific policy should be communicated to all relevant personnel and consider the following:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) the type of information and the classification level that the user endpoint devices can handle, process, store or support;
b) registration of user endpoint devices;
c) requirements for physical protection;
d) restriction of software installation (e.g. remotely controlled by system administrators);
e) requirements for user endpoint device software (including software versions) and for applying updates (e.g. active automatic updating);
f) rules for connection to information services, public networks or any other network off premises (e.g. requiring the use of personal firewall);
g) access controls;
h) storage device encryption;
i) protection against malware;
j) remote disabling, deletion or lockout;
k) backups;
l) usage of web services and web applications;
m) end user behaviour analytics (see 8.16);
n) the use of removable devices, including removable memory devices, and the possibility of disabling physical ports (e.g. USB ports);
o) the use of partitioning capabilities, if supported by the user endpoint device, which can securely separate the organization's information and other associated assets (e.g. software) from other information and other associated assets on the device.

Consideration should be given as to whether certain information is so sensitive that it can only be accessed via user endpoint devices, but not stored on such devices. In such cases, additional technical safeguards can be required on the device. For example, ensuring that downloading files for offline working is disabled and that local storage such as SD card is disabled.

As far as possible, the recommendations on this control should be enforced through configuration management (see 8.9) or automated tools.

User responsibility

All users should be made aware of the security requirements and procedures for protecting user endpoint devices, as well as of their responsibilities for implementing such security measures. Users should be advised to:

a) log-off active sessions and terminate services when no longer needed;
b) protect user endpoint devices from unauthorized use with a physical control (e.g. key lock or special locks) and logical control (e.g. password access) when not in use; not leave devices carrying important, sensitive or critical business information unattended;
c) use devices with special care in public places, open offices, meeting places and other unprotected areas (e.g. avoid reading confidential information if people can read from the back, use privacy screen filters);
d) physically protect user endpoint devices against theft (e.g. in cars and other forms of transport, hotel rooms, conference centres and meeting places).

A specific procedure taking into account legal, statutory, regulatory, contractual (including insurance) and other security requirements of the organization should be established for cases of theft or loss of user endpoint devices.

Use of personal devices

Where the organization allows the use of personal devices (sometimes known as BYOD), in addition to the guidance given in this control, the following should be considered:

a) separation of personal and business use of the devices, including using software to support such separation and protect business data on a private device;
b) providing access to business information only after users have acknowledged their duties (physical protection, software updating, etc.), waiving ownership of business data, allowing remote wiping of data by the organization in case of theft or loss of the device or when no longer authorized to use the service. In such cases, PII protection legislation

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

should be considered;
c) topic-specific policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;
d) access to privately owned equipment (to verify the security of the machine or during an investigation), which can be prevented by legislation;
e) software licensing agreements that are such that organizations can become liable for licensing for client software on user endpoint devices owned privately by personnel or external party users.

Wireless connections
The organization should establish procedures for:
a) the configuration of wireless connections on devices (e.g. disabling vulnerable protocols);
b) using wireless or wired connections with appropriate bandwidth in accordance with relevant topic-specific policies (e.g. because backups or software updates are needed).

Other information
Controls to protect information on user endpoint devices depend on whether the user endpoint device is used only inside of the organization's secured premises and network connections, or whether it is exposed to increased physical and network related threats outside of the organization.

The wireless connections for user endpoint devices are similar to other types of network connections but have important differences that should be considered when identifying controls. In particular, back-up of information stored on user endpoint devices can sometimes fail because of limited network bandwidth or because user endpoint devices are not connected at the times when backups are scheduled.

For some USB ports, such as USB-C, disabling the USB port is not possible because it is used for other purposes (e.g. power delivery and display output).

8.2 Privileged access rights

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
The allocation and use of privileged access rights should be restricted and managed.

Purpose
To ensure only authorized users, software components and services are provided with privileged access rights.

Guidance
The allocation of privileged access rights should be controlled through an authorization process in accordance with the relevant topic-specific policy on access control (see 5.15). The following should be considered:
a) identifying users who need privileged access rights for each system or process (e.g. operating systems, database management systems and applications);
b) allocating privileged access rights to users as needed and on an event-by-event basis in line with the topic-specific policy on access control (see 5.15) (i.e. only to individuals with the necessary competence to carry out activities that require privileged access and based on the minimum requirement for their functional roles);
c) maintaining an authorization process (i.e. determining who can approve privileged

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

access rights, or not granting privileged access rights until the authorization process is complete) and a record of all privileges allocated;
d) defining and implementing requirements for expiry of privileged access rights;
e) taking measures to ensure that users are aware of their privileged access rights and when they are in privileged access mode. Possible measures include using specific user identities, user interface settings or even specific equipment;
f) authentication requirements for privileged access rights can be higher than the requirements for normal access rights. Re-authentication or authentication step-up can be necessary before doing work with privileged access rights;
g) regularly, and after any organizational change, reviewing users working with privileged access rights in order to verify if their duties, roles, responsibilities and competence still qualify them for working with privileged access rights (see 5.18);
h) establishing specific rules in order to avoid the use of generic administration user IDs (such as “root”), depending on systems’ configuration capabilities. Managing and protecting authentication information of such identities (see 5.17);
i) granting temporary privileged access just for the time window necessary to implement approved changes or activities (e.g. for maintenance activities or some critical changes), rather than permanently granting privileged access rights. This is often referred as break glass procedure, and often automated by privilege access management technologies;
j) logging all privileged access to systems for audit purposes;
k) not sharing or linking identities with privileged access rights to multiple persons, assigning each person a separate identity which allows assigning specific privileged access rights. Identities can be grouped (e.g. by defining an administrator group) in order to simplify the management of privileged access rights;
l) only using identities with privileged access rights for undertaking administrative tasks and not for day-to-day general tasks [i.e. checking email, accessing the web (users should have a separate normal network identity for these activities)].

Other information
Privileged access rights are access rights provided to an identity, a role or a process that allows the performance of activities that typical users or processes cannot perform. System administrator roles typically require privileged access rights.

Inappropriate use of system administrator privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

More information related to access management and the secure management of access to information and information and communications technologies resources can be found in ISO/IEC 29146.

8.3 Information access restriction

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.

Purpose
To ensure only authorized access and to prevent unauthorized access to information and other associated assets.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance
Access to information and other associated assets should be restricted in accordance with the established topic-specific policies. The following should be considered in order to support access restriction requirements:
a) not allowing access to sensitive information by unknown user identities or anonymously. Publicor anonymous access should only be granted to storage locations that do not contain any sensitive information;
b) providing configuration mechanisms to control access to information in systems, applications and services;
c) controlling which data can be accessed by a particular user;
d) controlling which identities or group of identities have which access, such as read, write, delete and execute;
e) providing physical or logical access controls for the isolation of sensitive applications, application data, or systems.

Further, dynamic access management techniques and processes to protect sensitive information that has high value to the organization should be considered when the organization:
a) needs granular control over who can access such information during what period and in what way;
b) wants to share such information with people outside the organization and maintain control over who can access it;
c) wants to dynamically manage, in real-time, the use and distribution of such information;
d) wants to protect such information against unauthorized changes, copying and distribution (including printing);
e) wants to monitor the use of the information;
f) wants to record any changes to such information that take place in case a future investigation is required.

Dynamic access management techniques should protect information throughout its life cycle (i.e. creation, processing, storage, transmission and disposal), including:
a) establishing rules on the management of dynamic access based on specific use cases considering:
    1) granting access permissions based on identity, device, location or application;
    2) leveraging the classification scheme in order to determine what information needs to beprotected with dynamic access management techniques;
b) establishing operational, monitoring and reporting processes and supporting technical infrastructure.

Dynamic access management systems should protect information by:
a) requiring authentication, appropriate credentials or a certificate to access information;
b) restricting access, for example to a specified time frame (e.g. after a given date or until a particular date);
c) using encryption to protect information;
d) defining the printing permissions for the information;
e) recording who accesses the information and how the information is used;
f) raising alerts if attempts to misuse the information are detected.

Other information
Dynamic access management techniques and other dynamic information protection technologies can support the protection of information even when data is shared beyond the originating organization, where traditional access controls cannot be enforced. It can be applied to documents, emails or other files containing information to limit who can access the content and in what way. It can be at a granular level and be adapted over the life cycle of the information.

Dynamic access management techniques do not replace classical access management [e.g. using access control lists (ACLs)], but can add more factors for conditionality, real-time

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

evaluation, just-in-time data reduction and other enhancements that can be useful for the most sensitive information. It offers a way to control access outside the organization's environment. Incident response can be supported by dynamic access management techniques as permissions can be modified or revoked at any time.

Additional information on a framework for access management is provided in ISO/IEC 29146.

8.4 Access to source code

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management #Application_security #Secure_configuration	#Protection

Control
Read and write access to source code, development tools and software libraries should be appropriately managed.

Purpose
To prevent the introduction of unauthorized functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property.

Guidance
Access to source code and associated items (such as designs, specifications, verification plans and validation plans) and development tools (e.g. compilers, builders, integration tools, test platforms and environments) should be strictly controlled.

For source code, this can be achieved by controlling central storage of such code, preferably in source code management system.

Read access and write access to source code can differ based on the personnel's role. For example, read access to source code can be broadly provided inside the organization, but write access to source code is only made available to privileged personnel or designated owners. Where code components are used by several developers within an organization, read access to a centralized code repository should be implemented. Furthermore, if open-source code or third-party code components are used inside an organization, read access to such external code repositories can be broadly provided. However, write access should still be restricted.

The following guidelines should be considered to control access to program source libraries in order to reduce the potential for corruption of computer programs:

a) managing the access to program source code and the program source libraries according to established procedures;
b) granting read and write access to source code based on business needs and managed to address risks of alteration or misuse and according to established procedures;
c) updating of source code and associated items and granting of access to source code in accordance with change control procedures (see 8.32) and only performing it after appropriate authorization has been received;
d) not granting developers direct access to the source code repository, but through developer tools that control activities and authorizations on the source code;
e) holding program listings in a secure environment, where read and write access should be appropriately managed and assigned;
f) maintaining an audit log of all accesses and of all changes to source code.

If the program source code is intended to be published, additional controls to provide

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

assurance on its integrity (e.g. digital signature) should be considered.

Other information
If access to source code is not properly controlled, source code can be modified or some data in the development environment (e.g. copies of production data, configuration details) can be retrieved by unauthorized persons.

8.5 Secure authentication

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection

Control
Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.

Purpose
To ensure a user or an entity is securely authenticated, when access to systems, applications and services is granted.

Guidance
A suitable authentication technique should be chosen to substantiate the claimed identity of a user, software, messages and other entities.

The strength of authentication should be appropriate for the classification of the information to be accessed. Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as digital certificates, smart cards, tokens or biometric means, should be used.

Authentication information should be accompanied by additional authentication factors for accessing critical information systems (also known as multi-factor authentication). Using a combination of multiple authentication factors, such as what you know, what you have and what you are, reduces the possibilities for unauthorized accesses. Multi-factor authentication can be combined with other techniques to require additional factors under specific circumstances, based on predefined rules and patterns, such as access from an unusual location, from an unusual device or at an unusual time.

Biometric authentication information should be invalidated if it is ever compromised. Biometric authentication can be unavailable depending on the conditions of use (e.g. moisture or aging). Toprepare for these issues, biometric authentication should be accompanied with at least one alternative authentication technique.

The procedure for logging into a system or application should be designed to minimize the risk of unauthorized access. Log-on procedures and technologies should be implemented considering the following:

a) not displaying sensitive system or application information until the log-on process has been successfully completed in order to avoid providing an unauthorized user with any unnecessary assistance;
b) displaying a general notice warning that the system or the application or the service should only be accessed by authorized users;
c) not providing help messages during the log-on procedure that would aid an unauthorized user (e.g. if an error condition arises, the system should not indicate which part of the data is correct or incorrect);
d) validating the log-on information only on completion of all input data;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

e) protecting against brute force log-on attempts on usernames and passwords [e.g. using completely automated public Turing test to tell computers and humans apart (CAPTCHA), requiring password reset after a predefined number of failed attempts or blocking the user after a maximum number of errors];
f) logging unsuccessful and successful attempts;
g) raising a security event if a potential attempted or successful breach of log-on controls is detected (e.g. sending an alert to the user and the organization's system administrators when a certain number of wrong password attempts has been reached);
h) displaying or sending the following information on a separate channel on completion of a successful Slog-on:
   1) date and time of the previous successful log-on;
   2) details of any unsuccessful log-on attempts since the last successful log-on;
i) not displaying a password in clear text when it is being entered; in some cases, it can be required to de-activate this functionality in order to facilitate user log-on (e.g. for accessibility reasons or to avoid blocking users because of repeated errors);
j) not transmitting passwords in clear text over a network to avoid being captured by a network "sniffer" program;
k) terminating inactive sessions after a defined period of inactivity, especially in high risk locations such as public or external areas outside the organization's security management or on user endpoint devices;
l) restricting connection duration times to provide additional security for high-risk applications and reduce the window of opportunity for unauthorized access.

Other information
Additional information on entity authentication assurance can be found is ISO/IEC 29115.

8.6 Capacity management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Integrity #Availability	#Identify #Protect #Detect	#Continuity	#Governance_and_ Ecosystem #Protec-tion

Control
The use of resources should be monitored and adjusted in line with current and expected capacity requirements.

Purpose
To ensure the required capacity of information processing facilities, human resources, offices and other facilities.

Guidance
Capacity requirements for information processing facilities, human resources, offices and other facilities should be identified, taking into account the business criticality of the concerned systems and processes.

System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems.

The organization should perform stress-tests of systems and services to confirm that sufficient system capacity is available to meet peak performance requirements.

Detective controls should be put in place to indicate problems in due time.

Projections of future capacity requirements should take account of new business and system

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

requirements and current and projected trends in the organization's information processing capabilities.

Particular attention should be paid to any resources with long procurement lead times or high costs. Therefore, managers, service or product owners should monitor the utilization of key system resources.

Managers should use capacity information to identify and avoid potential resource limitations and dependency on key personnel which can present a threat to system security or services and plan appropriate action.

Providing sufficient capacity can be achieved by increasing capacity or by reducing demand. The following should be considered to increase capacity:

a) hiring new personnel;
b) obtaining new facilities or space;
c) acquiring more powerful processing systems, memory and storage;
d) making use of cloud computing, which has inherent characteristics that directly address issues of capacity. Cloud computing has elasticity and scalability which enable on-demand rapid expansion and reduction in resources available to particular applications and services.

The following should be considered to reduce demand on the organization's resources:

a) deletion of obsolete data (disk space);
b) disposal of hardcopy records that have met their retention period (free up shelving space);
c) decommissioning of applications, systems, databases or environments;
d) optimizing batch processes and schedules;
e) optimizing application code or database queries;
f) denying or restricting bandwidth for resource-consuming services if these are not critical (e.g. video streaming).

A documented capacity management plan should be considered for mission critical systems.

Other information

For more detail on the elasticity and scalability of cloud computing, see ISO/IEC TS 23167.

8.7 Protection against malware

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

Control

Protection against malware should be implemented and supported by appropriate user awareness.

Purpose

To ensure information and other associated assets are protected against malware.

Guidance

Protection against malware should be based on malware detection and repair software, information security awareness, appropriate system access and change management controls. Use of malware detection and repair software alone is not usually adequate. The following guidance should be considered:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) implementing rules and controls that prevent or detect the use of unauthorized software [e.g. application allowlisting (i.e. using a list providing allowed applications)] (see 8.19 and 8.32);
b) implementing controls that prevent or detect the use of known or suspected malicious websites (e.g. blocklisting);
c) reducing vulnerabilities that can be exploited by malware [e.g. through technical vulnerability management (see 8.8 and 8.19)];
d) conducting regular automated validation of the software and data content of systems, especially for systems supporting critical business processes; investigating the presence of any unapproved files or unauthorized amendments;
e) establishing protective measures against risks associated with obtaining files and software either from or via external networks or on any other medium;
f) installing and regularly updating malware detection and repair software to scan computers and electronic storage media. Carrying out regular scans that include:
    1) scanning any data received over networks or via any form of electronic storage media, for malware before use;
    2) scanning email and instant messaging attachments and downloads for malware before use. Carrying out this scan at different places (e.g. at email servers, desktop computers) and when entering the network of the organization;
    3) scanning webpages for malware when accessed;
g) determining the placement and configuration of malware detection and repair tools based on risk assessment outcomes and considering:
    1) defence in depth principles where they would be most effective. For example, this can lead to malware detection in a network gateway (in various application protocols such as email, file transfer and web) as well as user endpoint devices and servers;
    2) the evasive techniques of attackers (e.g. the use of encrypted files) to deliver malware or the use of encryption protocols to transmit malware;
h) taking care to protect against the introduction of malware during maintenance and emergency procedures, which can bypass normal controls against malware;
i) implementing a process to authorize temporarily or permanently disable some or all measures against malware, including exception approval authorities, documented justification and review date. This can be necessary when the protection against malware causes disruption to normal operations;
j) preparing appropriate business continuity plans for recovering from malware attacks, including all necessary data and software backup (including both online and offline backup) and recovery measures (see 8.13);
k) isolating environments where catastrophic consequences can occur;
l) defining procedures and responsibilities to deal with protection against malware on systems, including training in their use, reporting and recovering from malware attacks;
m) providing awareness or training (see 6.3) to all users on how to identify and potentially mitigate the receipt, sending or installation of malware infected emails, files or programs [the information collected in n) and o) can be used to ensure awareness and training are kept up-to-date];
n) implementing procedures to regularly collect information about new malware, such as subscribing to mailing lists or reviewing relevant websites;
o) verifying that information relating to malware, such as warning bulletins, comes from qualified and reputable sources (e.g. reliable internet sites or suppliers of malware detection software) and is accurate and informative.

Other information

It is not always possible to install software that protects against malware on some systems (e.g. some industrial control systems). Some forms of malware infect computer operating systems and computer firmware such that common malware controls cannot clean the system and a full reimaging of the operating system software and sometimes the computer firmware is necessary to return to a secure state.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.8 Management of technical vulnerabilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_and _Ecosystem #Protection #Defence

Control
Information about technical vulnerabilities of information systems in use should be obtained, the organization's exposure to such vulnerabilities should be evaluated and appropriate measures shouldbe taken.

Purpose
To prevent exploitation of technical vulnerabilities.

Guidance
Identifying technical vulnerabilities
The organization should have an accurate inventory of assets (see 5.9 to 5.14) as a prerequisite for effective technical vulnerability management; the inventory should include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

To identify technical vulnerabilities, the organization should consider:
a) defining and establishing the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, updating, asset tracking and any coordination responsibilities required;
b) for software and other technologies (based on the asset inventory list, see 5.9), identifying information resources that will be used for identifying relevant technical vulnerabilities and maintaining awareness about them. Updating the list of information resources based on changes in the inventory or when other new or useful resources are found;
c) requiring suppliers of information system (including their components) to ensure vulnerability reporting, handling and disclosure, including the requirements in applicable contracts (see 5.20);
d) using vulnerability scanning tools suitable for the technologies in use to identify vulnerabilities and to verify whether the patching of vulnerabilities was successful;
e) conducting planned, documented and repeatable penetration tests or vulnerability assessments by competent and authorized persons to support the identification of vulnerabilities. Exercising caution as such activities can lead to a compromise of the security of the system;
f) tracking the usage of third-party libraries and source code for vulnerabilities. This should be
included in secure coding (see 8.28).

The organization should develop procedures and capabilities to:
a) detect the existence of vulnerabilities in its products and services including any external component used in these;
b) receive vulnerability reports from internal or external sources.

The organization should provide a public point of contact as part of a topic-specific policy on vulnerability disclosure so that researchers and others are able to report issues. The organization should establish vulnerability reporting procedures, online reporting forms and making use of appropriate threat intelligence or information sharing forums. The organization should also consider bug bounty programs where rewards are offered as an incentive to assist organizations in identifying vulnerabilities in order to appropriately remediate them. The

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

organization should also share information with competent industry bodies or other interested parties.

Evaluating technical vulnerabilities

To evaluate identified technical vulnerabilities, the following guidance should be considered:

a) analyse and verify reports to determine what response and remediation activity is needed;
b) once a potential technical vulnerability has been identified, identifying the associated risks and the actions to be taken. Such actions can involve updating vulnerable systems or applying other controls.

Taking appropriate measures to address technical vulnerabilities

A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software. If changes are necessary, the original software should be retained and the changes applied to a designated copy. All changes should be fully tested and documented, so that they can be reapplied, if necessary, to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

The following guidance should be considered to address technical vulnerabilities:

a) taking appropriate and timely action in response to the identification of potential technical vulnerabilities; defining a timeline to react to notifications of potentially relevant technical vulnerabilities;
b) depending on how urgently a technical vulnerability needs to be addressed, carrying out the action according to the controls related to change management (see 8.32) or by following information security incident response procedures (see 5.26);
c) only using updates from legitimate sources (which can be internal or external to the organization);
d) testing and evaluating updates before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated [i.e. if an update is available, assessing the risks associated with installing the update (the risks posed by the vulnerability should be compared with the risk of installing the update)];
e) addressing systems at high risk first;
f) develop remediation (typically software updates or patches);
g) test to confirm if the remediation or mitigation is effective;
h) provide mechanisms to verify the authenticity of remediation;
i) if no update is available or the update cannot be installed, considering other controls, such as:
    1) applying any workaround suggested by the software vendor or other relevant sources;
    2) turning off services or capabilities related to the vulnerability;
    3) adapting or adding access controls (e.g. firewalls) at network borders (see 8.20 to 8.22);
    4) shielding vulnerable systems, devices or applications from attack through deployment of suitable traffic filters (sometimes called virtual patching);
    5) increasing monitoring to detect actual attacks;
    6) raising awareness of the vulnerability.

For acquired software, if the vendors regularly release information about security updates for their software and provide a facility to install such updates automatically, the organization should decide whether to use the automatic update or not.

Other considerations

An audit log should be kept for all steps undertaken in technical vulnerability management. The technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

An effective technical vulnerability management process should be aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out in case an incident occurs.

Where the organization uses a cloud service supplied by a third-party cloud service provider, technical vulnerability management of cloud service provider resources should be ensured by the cloud service provider. The cloud service provider's responsibilities for technical vulnerability management should be part of the cloud service agreement and this should include processes for reporting the cloud service provider's actions relating to technical vulnerabilities (see 5.23). For some cloud services, there are respective responsibilities for the cloud service provider and the cloud service customer. For example, the cloud service customer is responsible for vulnerability management of its own assets used for the cloud services.

Other information
STechnical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 8.32).

There is a possibility that an update does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling an update cannot be easily achieved once the update has been applied.

If adequate testing of the updates is not possible (e.g. because of costs or lack of resources) a delay in updating can be considered to evaluate the associated risks, based on the experience reported by other users. The use of ISO/IEC 27031 can be beneficial.

Where software patches or updates are produced, the organization can consider providing an automated update process where these updates are installed on affected systems or products without the need for intervention by the customer or the user. If an automated update process is offered, it can allow the customer or user to choose an option to turn off the automatic update or control the timing of the installation of the update.

Where the vendor provides an automated update process and the updates can be installed on affected systems or products without the need for intervention, the organization determines if it applies the automated process or not. One reason for not electing for automated update is to retain control over when the update is performed. For example, a software used for a business operation cannot be updateduntil the operation has completed.

A weakness with vulnerability scanning is that it is possible it does not fully account for defence in depth: two countermeasures that are always invoked in sequence can have vulnerabilities that are masked by strengths in the other. The composite countermeasure is not vulnerable, whereas a vulnerability scanner can report that both components are vulnerable. The organization should therefore take care in reviewing and acting on vulnerability reports.

Many organizations supply software, systems, products and services not only within the organization but also to interested parties such as customers, partners or other users. These software, systems, products and services can have information security vulnerabilities that affect the security of users.

Organizations can release remediation and disclose information about vulnerabilities to users (typically through a public advisory) and provide appropriate information for software vulnerability database services.

For more information relating to the management of technical vulnerabilities when using cloud computing, see the ISO/IEC 19086 series and ISO/IEC 27017.

ISO/IEC 29147 provides detailed information on receiving vulnerability reports and publishing

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

vulnerability advisories. ISO/IEC 30111 provides detailed information about handling and resolving reported vulnerabilities.

8.9 Configuration management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control
Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Purpose
To ensure hardware, software, services and networks function correctly with required security settings, and configuration is not altered by unauthorized or incorrect changes.

Guidance
General
The organization should define and implement processes and tools to enforce the defined configurations (including security configurations) for hardware, software, services (e.g. cloud services) and networks, for newly installed systems as well as for operational systems over their lifetime.

Roles, responsibilities and procedures should be in place to ensure satisfactory control of all configuration changes.

Standard templates
Standard templates for the secure configuration of hardware, software, services and networks should be defined:
a) using publicly available guidance (e.g. pre-defined templates from vendors and from independent security organizations);
b) considering the level of protection needed in order to determine a sufficient level of security;
c) supporting the organization's information security policy, topic-specific policies, standards and other security requirements;
d) considering the feasibility and applicability of security configurations in the organization's context.

The templates should be reviewed periodically and updated when new threats or vulnerabilities need to be addressed, or when new software or hardware versions are introduced.

The following should be considered for establishing standard templates for the secure configuration of hardware, software, services and networks:
a) minimizing the number of identities with privileged or administrator level access rights;
b) disabling unnecessary, unused or insecure identities;
c) disabling or restricting unnecessary functions and services;
d) restricting access to powerful utility programs and host parameter settings;
e) synchronizing clocks;
f) changing vendor default authentication information such as default passwords immediately after installation and reviewing other important default security-related parameters;
g) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

h) verifying that licence requirements have been met (see 5.32).

Managing configurations
Established configurations of hardware, software, services and networks should be recorded and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

Configuration records can contain as relevant:

a) up-to-date owner or point of contact information for the asset;
b) date of the last change of configuration;
c) version of configuration template;
d) relation to configurations of other assets.

Monitoring configurations
Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Other information
Documentation for systems often records details about the configuration of both hardware and software.

System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling. Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).
Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

8.10 Information deletion

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection

Control
Information stored in information systems, devices or in any other storage media should be deleted when no longer required.

Purpose
To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory and contractual requirements for information deletion.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance

General

Sensitive information should not be kept for longer than it is required to reduce the risk of undesirable disclosure.

When deleting information on systems, applications and services, the following should be considered:

a) selecting a deletion method (e.g. electronic overwriting or cryptographic erasure) in accordancewith business requirements and taking into consideration relevant laws and regulations;
b) recording the results of deletion as evidence;
c) when using service suppliers of information deletion, obtaining evidence of information deletion from them.

Where third parties store the organization's information on its behalf, the organization should consider the inclusion of requirements on information deletion into the third-party agreements to enforce it during and upon termination of such services.

Deletion methods

In accordance with the organization's topic-specific policy on data retention and taking into consideration relevant legislation and regulations, sensitive information should be deleted when no longer required, by:

a) configuring systems to securely destroy information when no longer required (e.g. after a definedperiod subject to the topic-specific policy on data retention or by subject access request);
b) deleting obsolete versions, copies and temporary files wherever they are located;
c) using approved, secure deletion software to permanently delete information to help ensureinformation cannot be recovered by using specialist recovery or forensic tools;
d) using approved, certified providers of secure disposal services;
e) using disposal mechanisms appropriate for the type of storage media being disposed of (e.g.degaussing hard disk drives and other magnetic storage media).

Where cloud services are used, the organization should verify if the deletion method provided by the cloud service provider is acceptable, and if it is the case, the organization should use it, or request that the cloud service provider delete the information. These deletion processes should be automated in accordance with topic-specific policies, when available and applicable. Depending on the sensitivity of information deleted, logs can track or verify that these deletion processes have happened.

To avoid the unintentional exposure of sensitive information when equipment is being sent back to vendors, sensitive information should be protected by removing auxiliary storages (e.g. hard disk drives) and memory before equipment leaves the organization's premises.

Considering that the secure deletion of some devices (e.g. smartphones) can only be achieved through destruction or using the functions embedded in these devices (e.g. "restore factory settings"), the organization should choose the appropriate method according to the classification of information handled by such devices.

Control measures described in 7.14 should be applied to physically destroy the storage device and simultaneously delete the information it contains.

An official record of information deletion is useful when analysing the cause of a possible information leakage event.

Other information

Information on user data deletion in cloud services can be found in ISO/IEC 27017.

Information on deletion of PII can be found in ISO/IEC 27555.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.11 Data masking

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection

Control
Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.

Purpose
To limit the exposure of sensitive data including PII, and to comply with legal, statutory, regulatory and contractual requirements.

Guidance
Where the protection of sensitive data (e.g. PII) is a concern, the organization should consider hiding such data by using techniques such as data masking, pseudonymization or anonymization.

Pseudonymization or anonymization techniques can hide PII, disguise the true identity of PII principals or other sensitive information, and disconnect the link between PII and the identity of the PII principal or the link between other sensitive information.

When using pseudonymization or anonymization techniques, it should be verified that data has been adequately pseudonymized or anonymized. Data anonymization should consider all the elements of the sensitive information to be effective. As an example, if not considered properly, a person can be identified even if the data that can directly identify that person is anonymised, by the presence of further data which allows the person to be identified indirectly.

Additional techniques for data masking include:
a) encryption (requiring authorized users to have a key);
b) nulling or deleting characters (preventing unauthorized users from seeing full messages);
c) varying numbers and dates;
d) substitution (changing one value for another to hide sensitive data);
e) replacing values with their hash.

The following should be considered when implementing data masking techniques:
a) not granting all users access to all data, therefore designing queries and masks in order to show only the minimum required data to the user;
b) there are cases where some data should not be visible to the user for some records out of a set of data; in this case, designing and implementing a mechanism for obfuscation of data (e.g. if a patient does not want hospital staff to be able to see all of their records, even in case of emergency, then the hospital staff are presented with partially obfuscated data and data can only be accessed by staff with specific roles if it contains useful information for appropriate treatment);
c) when data are obfuscated, giving the PII principal the possibility to require that users cannot see if the data are obfuscated (obfuscation of the obfuscation; this is used in health facilities, for example if the patient does not want personnel to see that sensitive information such as pregnancies or results of blood exams has been obfuscated);
d) any legal or regulatory requirements (e.g. requiring the masking of payment cards' information during processing or storage).

The following should be considered when using data masking, pseudonymization or anonymization:
a) level of strength of data masking, pseudonymization or anonymization according to the

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

usage ofthe processed data;
b) access controls to the processed data;
c) agreements or restrictions on usage of the processed data;
d) prohibiting collating the processed data with other information in order to identify the PII principal;
e) keeping track of providing and receiving the processed data.

Other information
Anonymization irreversibly alters PII in such a way that the PII principal can no longer be identified directly or indirectly.

Pseudonymization replaces the identifying information with an alias. Knowledge of the algorithm (sometimes referred to as the "additional information") used to perform the pseudonymization allows for at least some form of identification of the PII principal. Such "additional information" should therefore be kept separate and protected.

While pseudonymization is therefore weaker than anonymization, pseudonymized datasets can bemore useful in statistical research.

Data masking is a set of techniques to conceal, substitute or obfuscate sensitive data items. Data masking can be static (when data items are masked in the original database), dynamic (using automation and rules to secure data in real-time) or on-the-fly (with data masked in an application's memory).

Hash functions can be used in order to anonymize PII. In order to prevent enumeration attacks, they should always be combined with a salt function.

PII in resource identifiers and their attributes [e.g. file names, uniform resource locators (URLs)] shouldbe either avoided or appropriately anonymized.

Additional controls concerning the protection of PII in public clouds are given in ISO/IEC 27018.

Additional information on de-identification techniques is available in ISO/IEC 20889.

8.12 Data leakage prevention

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence

Control
Data leakage prevention measures should be applied to systems, networks and any other devices that process, store or transmit sensitive information.

Purpose
To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

Guidance
The organization should consider the following to reduce the risk of data leakage:
a) identifying and classifying information to protect against leakage (e.g. personal information, pricing models and product designs);
b) monitoring channels of data leakage (e.g. email, file transfers, mobile devices and portable storage devices);
c) acting to prevent information from leaking (e.g. quarantine emails containing sensitive information).

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Data leakage prevention tools should be used to:
a) identify and monitor sensitive information at risk of unauthorized disclosure (e.g. in unstructured data on a user's system);
b) detect the disclosure of sensitive information (e.g. when information is uploaded to untrustedthird-party cloud services or sent via email);
c) block user actions or network transmissions that expose sensitive information (e.g. preventing the copying of database entries into a spreadsheet).

The organization should determine if it is necessary to restrict a user's ability to copy and paste or upload data to services, devices and storage media outside of the organization. If that is the case, the organization should implement technology such as data leakage prevention tools or the configuration of existing tools that allow users to view and manipulate data held remotely but prevent copy and paste outside of the organization's control.

If data export is required, the data owner should be allowed to approve the export and hold users accountable for their actions.

Taking screenshots or photographs of the screen should be addressed through terms and conditions of use, training and auditing.

Where data is backed up, care should be taken to ensure sensitive information is protected using measures such as encryption, access control and physical protection of the storage media holding the backup.

Data leakage prevention should also be considered to protect against the intelligence actions of an adversary from obtaining confidential or secret information (geopolitical, human, financial, commercial,scientific or any other) which can be of interest for espionage or can be critical for the community. The data leakage prevention actions should be oriented to confuse the adversary's decisions for example by replacing authentic information with false information, either as an independent action or as response to the adversary's intelligence actions. Examples of these kinds of actions are reverse social engineering or the use of honeypots to attract attackers.

Other information
Data leakage prevention tools are designed to identify data, monitor data usage and movement, andtake actions to prevent data from leaking (e.g. alerting users to their risky behaviour and blocking the transfer of data to portable storage devices).

Data leakage prevention inherently involves monitoring personnel's communications and online activities, and by extension external party messages, which raises legal concerns that should be considered prior to deploying data leakage prevention tools. There is a variety of legislation relating to privacy, data protection, employment, interception of data and telecommunications that is applicable to monitoring and data processing in the context of data leakage prevention.

Data leakage prevention can be supported by standard security controls, such as topic-specific policies on access control and secure document management (see 5.12 and 5.15).

8.13 Information backup

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection

Control
Backup copies of information, software and systems should be maintained and regularly tested

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

in accordance with the agreed topic-specific policy on backup.

Purpose
To enable recovery from loss of data or systems.

Guidance
A topic-specific policy on backup should be established to address the organization's data retention and information security requirements.

Adequate backup facilities should be provided to ensure that all essential information and software can be recovered following an incident or failure or loss of storage media.

Plans should be developed and implemented for how the organization will back up information, software and systems, to address the topic-specific policy on backup.

When designing a backup plan, the following items should be taken into consideration:
a) producing accurate and complete records of the backup copies and documented restoration procedures;
b) reflecting the business requirements of the organization (e.g. the recovery point objective, see 5.30), the security requirements of the information involved and the criticality of the information to the continued operation of the organization in the extent (e.g. full or differential backup) and frequency of backups;
c) storing the backups in a safe and secure remote location, at a sufficient distance to escape any damage from a disaster at the main site;
d) giving backup information an appropriate level of physical and environmental protection (see Clause 7 and 8.1) consistent with the standards applied at the main site;
e) regularly testing backup media to ensure that they can be relied on for emergency use when necessary. Testing the ability to restore backed-up data onto a test system, not by overwriting the original storage media in case the backup or restoration process fails and causes irreparable data damage or loss;
f) protecting backups by means of encryption according to the identified risks (e.g. in situations where confidentiality is of importance);
g) taking care to ensure that inadvertent data loss is detected before backup is taken.

Operational procedures should monitor the execution of backups and address failures of scheduled backups to ensure completeness of backups according to the topic-specific policy on backups.

Backup measures for individual systems and services should be regularly tested to ensure that they meet the objectives of incident response and business continuity plans (see 5.30). This should be combined with a test of the restoration procedures and checked against the restoration time required by the business continuity plan. In the case of critical systems and services, backup measures should cover all systems information, applications and data necessary to recover the complete system in the event of a disaster.

When the organization uses a cloud service, backup copies of the organization's information, applications and systems in the cloud service environment should be taken. The organization should determine if and how requirements for backup are fulfilled when using the information backup service provided as part of the cloud service.

The retention period for essential business information should be determined, taking into account any requirement for retention of archive copies. The organization should consider the deletion of information (see 8.10) in storage media used for backup once the information's retention period expires and should take into consideration legislation and regulations.

Other information
For further information on storage security including retention consideration, see ISO/IEC 27040.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.14 Redundancy of information processing facilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience

Control
Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Purpose
To ensure the continuous operation of information processing facilities.

Guidance
The organization should identify requirements for the availability of business services and information systems. The organization should design and implement systems architecture with appropriate redundancy to meet these requirements.

Redundancy can be introduced by duplicating information processing facilities in part or in their entirety (i.e. spare components or having two of everything). The organization should plan and implement procedures for the activation of the redundant components and processing facilities. The procedures should establish if the redundant components and processing activities are always

activated, or in case of emergency, automatically or manually activated. The redundant components and information processing facilities should ensure the same security level as the primary ones.

Mechanisms should be in place to alert the organization to any failure in the information processing facilities, enable executing the planned procedure and allow continued availability while the information processing facilities are repaired or replaced.

The organization should consider the following when implementing redundant systems:
a) contracting with two or more suppliers of network and critical information processing facilities such as internet service providers;
b) using redundant networks;
c) using two geographically separate data centres with mirrored systems;
d) using physically redundant power supplies or sources;
e) using multiple parallel instances of software components, with automatic load balancing between them (between instances in the same data centre or in different data centres);
f) having duplicated components in systems (e.g. CPU, hard disks, memories) or in networks (e.g. firewalls, routers, switches).

Where applicable, preferably in production mode, redundant information systems should be tested to ensure the failover from one component to another component works as intended.

Other information
There is a strong relationship between redundancy and ICT readiness for business continuity (see 5.30) especially if short recovery times are required. Many of the redundancy measures can be part of the ICT continuity strategies and solutions.

The implementation of redundancies can introduce risks to the integrity (e.g. processes of copying data to duplicated components can introduce errors) or confidentiality (e.g. weak security control of duplicated components can lead to compromise) of information and information systems, which needto be considered when designing information systems.

Redundancy in information processing facilities does not usually address application

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

unavailability due to faults within an application.

With the use of public cloud computing, it is possible to have multiple live versions of information processing facilities, existing in multiple separate physical locations with automatic failover and load balancing between them.

Some of the technologies and techniques for providing redundancy and automatic fail-over in thecontext of cloud services are discussed in ISO/IEC TS 23167.

8.15 Logging

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence

Control
Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.

Purpose
To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, identify information security events that can lead to an information security incident and to support investigations.

Guidance
General
The organization should determine the purpose for which logs are created, what data is collected and logged, and any log-specific requirements for protecting and handling the log data. This should be documented in a topic-specific policy on logging.

Event logs should include for each event, as applicable:
a) user IDs;
b) system activities;
c) dates, times and details of relevant events (e.g. log-on and log-off);
d) device identity, system identifier and location;
e) network addresses and protocols.

The following events should be considered for logging:
a) successful and rejected system access attempts;
b) successful and rejected data and other resource access attempts;
c) changes to system configuration;
d) use of privileges;
e) use of utility programs and applications;
f) files accessed and the type of access, including deletion of important data files;
g) alarms raised by the access control system;
h) activation and de-activation of security systems, such as anti-virus systems and intrusion detection systems;
i) creation, modification or deletion of identities;
j) transactions executed by users in applications. In some cases, the applications are a service or product provided or run by a third party.

It is important for all systems to have synchronized time sources (see 8.17) as this allows for correlation of logs between systems for analysis, alerting and investigation of an incident.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Protection of logs
Users, including those with privileged access rights, should not have permission to delete or de-activate logs of their own activities. They can potentially manipulate the logs on information processing facilities under their direct control. Therefore, it is necessary to protect and review the logs to maintain accountability for the privileged users.

Controls should aim to protect against unauthorized changes to log information and operational problems with the logging facility including:
a) alterations to the message types that are recorded;
b) log files being edited or deleted;
c) failure to record events or over-writing of past recorded events if the storage media holding a log file is exceeded.

For protection of logs, the use of the following techniques should be considered: cryptographic hashing, recording in an append-only and read-only file, recording in a public transparency file. Some audit logs can be required to be archived because of requirements on data retention or requirements to collect and retain evidence (see 5.28).

Where the organization needs to send system or application logs to a vendor to assist with debugging ortroubleshooting errors, logs should be de-identified where possible using data masking techniques (see 8.11) for information such as usernames, internet protocol (IP) addresses, hostnames or organization name, before sending to the vendor.

Event logs can contain sensitive data and personally identifiable information. Appropriate privacy protection measures should be taken (see 5.34).

Log analysis
Log analysis should cover the analysis and interpretation of information security events, to help identify unusual activity or anomalous behaviour, which can represent indicators of compromise.

Analysis of events should be performed by taking into account:
a) the necessary skills for the experts performing the analysis;
b) determining the procedure of log analysis;
c) the required attributes of each security-related event;
d) exceptions identified through the use of predetermined rules [e.g. security information and event management (SIEM) or firewall rules, and intrusion detection systems (IDSs) or malware signatures];
e) known behaviour patterns and standard network traffic compared to anomalous activity and behaviour [user and entity behaviour analytics (UEBA)];
f) results of trend or pattern analysis (e.g. as a result of using data analytics, big data techniques and specialized analysis tools);
g) available threat intelligence.

Log analysis should be supported by specific monitoring activities to help identify and analyse anomalous behaviour, which includes:
a) reviewing successful and unsuccessful attempts to access protected resources [e.g. domain name system (DNS) servers, web portals and file shares];
b) checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers;
c) examining usage reports from service providers (e.g. invoices or service reports) for unusual activity within systems and networks (e.g. by reviewing patterns of activity);
d) including event logs of physical monitoring such as entrance and exit to ensure more accurate detection and incident analysis;
e) correlating logs to enable efficient and highly accurate analysis.

Suspected and actual information security incidents should be identified (e.g. malware infection or probing of firewalls) and be subject to further investigation (e.g. as part of an

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

information security incident management process, see 5.25).

Other information
System logs often contain a large volume of information, much of which is extraneous to information security monitoring. To help identify significant events for information security monitoring purposes, the use of suitable utility programs or audit tools to perform file interrogation can be considered.

Event logging sets the foundation for automated monitoring systems (see 8.16) which are capable of generating consolidated reports and alerts on system security.

A SIEM tool or equivalent service can be used to store, correlate, normalize and analyse log information**,**and to generate alerts. SIEMs tend to require careful configuration to optimize their benefits. Configurations to consider include identification and selection of appropriate log sources, tuning and testing of rules and development of use cases.

Public transparency files for the recording of logs are used, for example, in certificate transparency systems. Such files can provide an additional detection mechanism useful for guarding against log tampering.

In cloud environments, log management responsibilities can be shared between the cloud service customer and the cloud service provider. Responsibilities vary depending on the type of cloud service being used. Further guidance can be found in ISO/IEC 27017.

8.16 Monitoring activities

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence

Control
Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.

Purpose
To detect anomalous behaviour and potential information security incidents.

Guidance
The monitoring scope and level should be determined in accordance with business and information security requirements and taking into consideration relevant laws and regulations. Monitoring records should be maintained for defined retention periods.

The following should be considered for inclusion within the monitoring system:
a) outbound and inbound network, system and application traffic;
b) access to systems, servers, networking equipment, monitoring system, critical applications, etc.;
c) critical or admin level system and network configuration files;
d) logs from security tools [e.g. antivirus, IDS, intrusion prevention system (IPS), web filters, firewalls, data leakage prevention];
e) event logs relating to system and network activity;
f) checking that the code being executed is authorized to run in the system and that it has not been tampered with (e.g. by recompilation to add additional unwanted code);
g) use of the resources (e.g. CPU, hard disks, memory, bandwidth) and their performance.

The organization should establish a baseline of normal behaviour and monitor against this baseline for anomalies. When establishing a baseline, the following should be considered:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) reviewing utilization of systems at normal and peak periods;
b) usual time of access, location of access, frequency of access for each user or group of users.

The monitoring system should be configured against the established baseline to identify anomalous behaviour, such as:
a) unplanned termination of processes or applications;
b) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g. those associated with botnet command and control servers);
c) known attack characteristics (e.g. denial of service and buffer overflows);
d) unusual system behaviour (e.g. keystroke logging, process injection and deviations in use of standard protocols);
e) bottlenecks and overloads (e.g. network queuing, latency levels and network jitter)
f) unauthorized access (actual or attempted) to systems or information;
g) unauthorized scanning of business applications, systems and networks;
h) successful and unsuccessful attempts to access protected resources (e.g. DNS servers, web portals and file systems);
i) unusual user and system behaviour in relation to expected behaviour.

Continuous monitoring via a monitoring tool should be used. Monitoring should be done in real time or in periodic intervals, subject to organizational need and capabilities. Monitoring tools should include the ability to handle large amounts of data, adapt to a constantly changing threat landscape, and allow for real-time notification. The tools should also be able to recognize specific signatures and data or network or application behaviour patterns.

Automated monitoring software should be configured to generate alerts (e.g. via management consoles, email messages or instant messaging systems) based on predefined thresholds. The alerting system should be tuned and trained on the organization's baseline to minimize false positives. Personnel shouldbe dedicated to respond to alerts and should be properly trained to accurately interpret potential incidents. There should be redundant systems and processes in place to receive and respond to alert notifications.

Abnormal events should be communicated to relevant parties in order to improve the following activities: auditing, security evaluation, vulnerability scanning and monitoring (see 5.25). Procedures should be in place to respond to positive indicators from the monitoring system in a timely manner, in order to minimize the effect of adverse events (see 5.26) on information security. Procedures should also be established to identify and address false positives including tuning the monitoring software to reduce the number of future false positives.

Other information
Security monitoring can be enhanced by:
a) leveraging threat intelligence systems (see 5.7);
b) leveraging machine learning and artificial intelligence capabilities;
c) using blocklists or allowlists;
d) undertaking a range of technical security assessments (e.g. vulnerability assessments, penetration testing, cyber-attack simulations and cyber response exercises), and using the results of these assessments to help determine baselines or acceptable behaviour;
e) using performance monitoring systems to help establish and detect anomalous behaviour;
f) leveraging logs in combination with monitoring systems.

Monitoring activities are often conducted using specialist software, such as intrusion detection systems. These can be configured to a baseline of normal, acceptable and expected system and network activities.

Monitoring for anomalous communications helps in the identification of botnets (i.e. set of devicesunder the malicious control of the botnet owner, usually used for mounting distributed

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

denial of service attacks on other computers of other organizations). If the computer is being controlled by an external device, there is a communication between the infected device and the controller. The organization should therefore employ technologies to monitor for anomalous communications and take such action as necessary.

8.17 Clock synchronization

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Control
The clocks of information processing systems used by the organization should be synchronized to approved time sources.

Purpose
To enable the correlation and analysis of security-related events and other recorded data, and to support investigations into information security incidents.

Guidance
External and internal requirements for time representation, reliable synchronization and accuracy should be documented and implemented. Such requirements can be from legal, statutory, regulatory, contractual, standards and internal monitoring needs. A standard reference time for use within the organization should be defined and considered for all systems, including building management systems, entry and exit systems and others that can be used to aid investigations.

A clock linked to a radio time broadcast from a national atomic clock or global positioning system (GPS) should be used as the reference clock for logging systems; a consistent, trusted date and time source to ensure accurate time-stamps. Protocols such as network time protocol (NTP) or precision time protocol (PTP) should be used to keep all networked systems in synchronization with a reference clock.

The organization can use two external time sources at the same time in order to improve the reliability of external clocks, and appropriately manage any variance.

Clock synchronization can be difficult when using multiple cloud services or when using both cloud and on-premises services. In this case, the clock of each service should be monitored and the difference recorded in order to mitigate risks arising from discrepancies.

Other information
The correct setting of computer clocks is important to ensure the accuracy of event logs, which can be required for investigations or as evidence in legal and disciplinary cases. Inaccurate audit logs can hinder such investigations and damage the credibility of such evidence.

8.18 Use of privileged utility programs

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Control
The use of utility programs that can be capable of overriding system and application controls should be restricted and tightly controlled.

Purpose
To ensure the use of utility programs does not harm system and application controls for information security.

Guidance
The following guidelines for the use of utility programs that can be capable of overriding system and application controls should be considered:
a) limitation of the use of utility programs to the minimum practical number of trusted, authorized users (see 8.2);
b) use of identification, authentication and authorization procedures for utility programs, including unique identification of the person who uses the utility program;
c) defining and documenting of authorization levels for utility programs;
d) authorization for ad hoc use of utility programs;
e) not making utility programs available to users who have access to applications on systems where segregation of duties is required;
f) removing or disabling all unnecessary utility programs;
g) at a minimum, logical segregation of utility programs from application software. Where practical, segregating network communications for such programs from application traffic;
h) limitation of the availability of utility programs (e.g. for the duration of an authorized change);
i) logging of all use of utility programs.

Other information
Most information systems have one or more utility programs that can be capable of overriding system and application controls, for example diagnostics, patching, antivirus, disk defragmenters, debuggers, backup and network tools.

8.19 Installation of software on operational systems

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection

Control
Procedures and measures should be implemented to securely manage software installation on operational systems.

Purpose
To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities.

Guidance
The following guidelines should be considered to securely manage changes and installation of software on operational systems:
a) performing updates of operational software only by trained administrators upon appropriate management authorization (see 8.5);
b) ensuring that only approved executable code and no development code or compilers is installed on operational systems;
c) only installing and updating software after extensive and successful testing (see 8.29 and 8.31);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) updating all corresponding program source libraries;
e) using a configuration control system to keep control of all operational software as well as the system documentation;
f) defining a rollback strategy before changes are implemented;
g) maintaining an audit log of all updates to operational software;
h) archiving old versions of software, together with all required information and parameters, procedures, configuration details and supporting software as a contingency measure, and for as long as the software is required to read or process archived data.

Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release (e.g. the introduction of new information security functionality or the number and severity of information security vulnerabilities affecting the current version). Software patches should be applied when they can help to remove or reduce information security vulnerabilities (see 8.8 and 8.19).

Computer software can rely on externally supplied software and packages (e.g. software programs using modules which are hosted on external sites), which should be monitored and controlled to avoid unauthorized changes, because they can introduce information security vulnerabilities.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software. Open source software used in operational systems should be maintained to the latest appropriate release of the software. Over time, open source code can cease to be maintained but is still available in an open source software repository. The organization should also consider the risks of relying on unmaintained open source software when used in operational systems.

When suppliers are involved in installing or updating software, physical or logical access should only be given when necessary and with appropriate authorization. The supplier's activities should be monitored (see 5.22).

The organization should define and enforce strict rules on which types of software users can install.

The principle of least privilege should be applied to software installation on operational systems. The organization should identify what types of software installations are permitted (e.g. updates and security patches to existing software) and what types of installations are prohibited (e.g. software that is only for personal use and software whose pedigree with regard to being potentially malicious is unknown or suspect). These privileges should be granted based on the roles of the users concerned.

Other information
No other information.

8.20 Networks security

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection

Control
Networks and network devices should be secured, managed and controlled to protect information in systems and applications.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To protect information in networks and its supporting information processing facilities from compromise via the network.

Guidance
Controls should be implemented to ensure the security of information in networks and to protect connected services from unauthorized access. In particular, the following items should be considered:

a) the type and classification level of information that the network can support;
b) establishing responsibilities and procedures for the management of networking equipment and devices;
c) maintaining up to date documentation including network diagrams and configuration files of devices (e.g. routers, switches);
d) separating operational responsibility for networks from ICT system operations where appropriate (see 5.3);
e) establishing controls to safeguard the confidentiality and integrity of data passing over public networks, third-party networks or over wireless networks and to protect the connected systems and applications (see 5.22, 8.24, 5.14 and 6.6). Additional controls can also be required to maintain the availability of the network services and computers connected to the network;
f) appropriately logging and monitoring to enable recording and detection of actions that can affect, or are relevant to, information security (see 8.16 and 8.15);
g) closely coordinating network management activities both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure;
h) authenticating systems on the network;
i) restricting and filtering systems connection to the network (e.g. using firewalls);
j) detecting, restricting and authenticating the connection of equipment and devices to the network;
k) hardening of network devices;
l) segregating network administration channels from other network traffic;
m) temporarily isolating critical subnetworks (e.g. with drawbridges) if the network is under attack;
n) disabling vulnerable network protocols.

The organization should ensure that appropriate security controls are applied to the use of virtualized networks. Virtualized networks also cover software-defined networking (SDN, SD-WAN). Virtualized networks can be desirable from a security viewpoint, since they can permit logical separation of communication taking place over physical networks, particularly for systems and applications that are implemented using distributed computing.

Other information
Additional information on network security can be found in the ISO/IEC 27033 series. More information concerning virtualized networks can be found in ISO/IEC TS 23167.

8.21 Security of network services

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control
Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To ensure security in the use of network services.

Guidance
The security measures necessary for particular services, such as security features, service levels and service requirements, should be identified and implemented (by internal or external network service providers). The organization should ensure that network service providers implement these measures.

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored. The right to audit should be agreed between the organization and the provider. The organization should also consider third-party attestations provided by service providers to demonstrate they maintain appropriate security measures.

Rules on the use of networks and network services should be formulated and implemented to cover:
a) the networks and network services which are allowed to be accessed;
b) authentication requirements for accessing various network services;
c) authorization procedures for determining who is allowed to access which networks and networked services;
d) network management and technological controls and procedures to protect access to network connections and network services;
e) the means used to access networks and network services [e.g. use of virtual private network (VPN) or wireless network];
f) time, location and other attributes of the user at the time of the access;
g) monitoring of the use of network services.

The following security features of network services should be considered:
a) technology applied for security of network services, such as authentication, encryption and network connection controls;
b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;
c) caching (e.g. in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements;
d) procedures for the network service usage to restrict access to network services or applications, where necessary.

Other information
Network services include the provision of connections, private network services and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

More guidance on a framework for access management is given in ISO/IEC 29146.

8.22 Segregation of networks

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control
Groups of information services, users and information systems should be segregated in the organization's networks.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Purpose
To split the network in security boundaries and to control traffic between them based on business needs.

Guidance
The organization should consider managing the security of large networks by dividing them into separate network domains and separating them from the public network (i.e. internet). The domains can be chosen based on levels of trust, criticality and sensitivity (e.g. public access domain, desktop domain, server domain, low- and high-risk systems), along organizational units (e.g. human resources, finance, marketing) or some combination (e.g. server domain connecting to multiple organizational units). The segregation can be done using either physically different networks or by using different logical networks.

The perimeter of each domain should be well-defined. If access between network domains is allowed, it should be controlled at the perimeter using a gateway (e.g. firewall, filtering router). The criteria for segregation of networks into domains, and the access allowed through the gateways, should be based on an assessment of the security requirements of each domain. The assessment should be in accordance with the topic-specific policy on access control (see 5.15), access requirements, value and classification of information processed and take account of the relative cost and performance impact of incorporating suitable gateway technology.

Wireless networks require special treatment due to the poorly-defined network perimeter. Radio coverage adjustment should be considered for segregation of wireless networks. For sensitive environments, consideration should be made to treat all wireless access as external connections and to segregate this access from internal networks until the access has passed through a gateway in accordance with network controls (see 8.20) before granting access to internal systems. Wireless access network for guests should be segregated from those for personnel if personnel only use controlled user endpoint devices compliant to the organization's topic-specific policies. WiFi for guests should have at least the same restrictions as WiFi for personnel, in order to discourage the use of guest WiFi by personnel.

Other information
Networks often extend beyond organizational boundaries, as business partnerships are formed that require the interconnection or sharing of information processing and networking facilities. Such extensions can increase the risk of unauthorized access to the organization's information systems that use the network, some of which require protection from other network users because of their sensitivity or criticality.

8.23 Web filtering

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection

Control
Access to external websites should be managed to reduce exposure to malicious content.

Purpose
To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

Guidance
The organization should reduce the risks of its personnel accessing websites that contain illegal information or are known to contain viruses or phishing material. A technique for achieving this works by blocking the IP address or domain of the website(s) concerned. Some

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

browsers and anti-malware technologies do this automatically or can be configured to do so.

The organization should identify the types of websites to which personnel should or should not have access. The organization should consider blocking access to the following types of websites:

a) websites that have an information upload function unless permitted for valid business reasons;
b) known or suspected malicious websites (e.g. those distributing malware or phishing contents);
c) command and control servers;
d) malicious website acquired from threat intelligence (see 5.7);
e) websites sharing illegal content.

Prior to deploying this control, the organization should establish rules for safe and appropriate use of online resources, including any restriction to undesirable or inappropriate websites and web-based applications. The rules should be kept up-to-date.

Training should be given to personnel on the secure and appropriate use of online resources including access to the web. The training should include the organization's rules, contact point for raising securityconcerns, and exception process when restricted web resources need to be accessed for legitimate business reasons. Training should also be given to personnel to ensure that they do not overrule any browser advisory that reports that a website is not secure but allows the user to proceed.

Other information

Web filtering can include a range of techniques including signatures, heuristics, list of acceptable websites or domains, list of prohibited websites or domains and bespoke configuration to help prevent malicious software and other malicious activity from attacking the organization's network and systems.

8.24 Use of cryptography

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

Rules for the effective use of cryptography, including cryptographic key management, should be definedand implemented.

Purpose

To ensure proper and effective use of cryptography to protect the confidentiality, authenticity or integrity of information according to business and information security requirements, and taking into consideration legal, statutory, regulatory and contractual requirements related to cryptography.

Guidance

General

When using cryptography, the following should be considered:

a) the topic-specific policy on cryptography defined by the organization, including the general principles for the protection of information. A topic-specific policy on the use of cryptography is necessary to maximize the benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use;
b) identifying the required level of protection and the classification of the information and consequently establishing the type, strength and quality of the cryptographic algorithms

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

required;
c) the use of cryptography for protection of information held on mobile user endpoint devices or storage media and transmitted over networks to such devices or storage media;
d) the approach to key management, including methods to deal with the generation and protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;
e) roles and responsibilities for:
   1) the implementation of the rules for the effective use of cryptography;
   2) the key management, including key generation (see 8.24);
f) the standards to be adopted, as well as cryptographic algorithms, cipher strength, cryptographic solutions and usage practices that are approved or required for use in the organization;
g) the impact of using encrypted information on controls that rely on content inspection (e.g. malware detection or content filtering).

When implementing the organization's rules for effective use of cryptography, the regulations and national restrictions that can apply to the use of cryptographic techniques in different parts of the world should be taken into consideration as well as the issues of trans-border flow of encrypted information (see 5.31).

The contents of service level agreements or contracts with external suppliers of cryptographic services (e.g. with a certification authority) should cover issues of liability, reliability of services and response times for the provision of services (see 5.22).

Key management
Appropriate key management requires secure processes for generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys.

A key management system should be based on an agreed set of standards, procedures and secure methods for:
a) generating keys for different cryptographic systems and different applications;
b) issuing and obtaining public key certificates;
c) distributing keys to intended entities, including how to activate keys when received;
d) storing keys, including how authorized users obtain access to keys;
e) changing or updating keys including rules on when to change keys and how this will be done;
f) dealing with compromised keys;
g) revoking keys including how to withdraw or deactivate keys [e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived)];
h) recovering keys that are lost or corrupted;
i) backing up or archiving keys;
j) destroying keys;
k) logging and auditing of key management related activities;
l) setting activation and deactivation dates for keys so that the keys can only be used for the period of time according to the organization's rules on key management;
m) handling legal requests for access to cryptographic keys (e.g. encrypted information can be required to be made available in an unencrypted form as evidence in a court case).

All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorized use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

In addition to integrity, for many use cases, the authenticity of public keys should also be considered.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Other information
The authenticity of public keys is usually addressed by public key management processes using certificate authorities and public key certificates, but it is also possible to address it by using technologies such as applying manual processes for small number keys.

Cryptography can be used to achieve different information security objectives, for example:
a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
b) integrity or authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information. Using algorithms for the purpose of file integrity checking;
c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non- occurrence of an event or action;
d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

The ISO/IEC 11770 series provides further information on key management.

8.25 Secure development life cycle

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net-work_security	#Protection

Control
Rules for the secure development of software and systems should be established and applied.

Purpose
To ensure information security is designed and implemented within the secure development life cycle of software and systems.

Guidance
Secure development is a requirement to build up a secure service, architecture, software and system. To achieve this, the following aspects should be considered:
a) separation of development, test and production environments (see 8.31);
b) guidance on the security in the software development life cycle:
   1) security in the software development methodology (see 8.28 and 8.27);
   2) secure coding guidelines for each programming language used (see 8.28);
c) security requirements in the specification and design phase (see 5.8);
d) security checkpoints in projects (see 5.8);
e) system and security testing, such as regression testing, code scan and penetration tests (see 8.29);
f) secure repositories for source code and configuration (see 8.4 and 8.9);
g) security in the version control (see 8.32);
h) required application security knowledge and training (see 8.28);
i) developers' capability for preventing, finding and fixing vulnerabilities (see 8.28);
j) licensing requirements and alternatives to ensure cost-effective solutions while avoiding future licensing issues (See 5.32).

If development is outsourced, the organization should obtain assurance that the supplier complies with the organization's rules for secure development (see 8.30).

Other information
Development can also take place inside applications, such as office applications, scripting, browsers anddatabases.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.26 Application security requirements

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence

Control
Information security requirements should be identified, specified and approved when developing or acquiring applications.

Purpose
To ensure all information security requirements are identified and addressed when developing or acquiring applications.

Guidance
General
Application security requirements should be identified and specified. These requirements are usually determined through a risk assessment. The requirements should be developed with the support of information security specialists.

Application security requirements can cover a wide range of topics, depending on the purpose of the application.

Application security requirements should include, as applicable:
a) level of trust in identity of entities [e.g. through authentication (see 5.17, 8.2 and 8.5)];
b) identifying the type of information and classification level to be processed by the application;
c) need for segregation of access and level of access to data and functions in the application;
d) resilience against malicious attacks or unintentional disruptions [e.g. protection against buffer overflow or structured query language (SQL) injections];
e) legal, statutory and regulatory requirements in the jurisdiction where the transaction is generated, processed, completed or stored;
f) need for privacy associated with all parties involved;
g) the protection requirements of any confidential information;
h) protection of data while being processed, in transit and at rest;
i) need to securely encrypt communications between all involved parties;
j) input controls, including integrity checks and input validation;
k) automated controls (e.g. approval limits or dual approvals);
l) output controls, also considering who can access outputs and its authorization;
m) restrictions around content of "free-text" fields, as these can lead to uncontrolled storage of confidential data (e.g. personal data);
n) requirements derived from the business process, such as transaction logging and monitoring, nonrepudiation requirements;
o) requirements mandated by other security controls (e.g. interfaces to logging and monitoring or data leakage detection systems);
p) error message handling.

Transactional services
Additionally, for applications offering transactional services between the organization and a partner, the following should be considered when identifying information security requirements:
a) the level of trust each party requires in each other's claimed identity;
b) the level of trust required in the integrity of information exchanged or processed and the mechanisms for identification of lack of integrity (e.g. cyclic redundancy check, hashing,

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

digital signatures);
c) authorization processes associated with who can approve contents of, issue or sign key transactional documents;
d) confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation (e.g. contracts associated with tendering and contract processes);
e) the confidentiality and integrity of any transactions (e.g. orders, delivery address details and confirmation of receipts);
f) requirements on how long to maintain a transaction confidential;
g) insurance and other contractual requirements.

Electronic ordering and payment applications
Additionally, for applications involving electronic ordering and payment, the following should be considered:
a) requirements for maintaining the confidentiality and integrity of order information;
b) the degree of verification appropriate to verify payment information supplied by a customer;
c) avoidance of loss or duplication of transaction information;
d) storing transaction details outside of any publicly accessible environment (e.g. on a storage platform existing on the organizational intranet, and not retained and exposed on electronic storage media directly accessible from the internet);
e) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures or digital certificates) security is integrated and embedded throughout the entire end- to-end certificate or signature management process.

Several of the above considerations can be addressed by the application of cryptography (see 8.24), taking into consideration legal requirements (see 5.31 to 5.36, especially see 5.31 for cryptography legislation).

Other information
Applications accessible via networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public; incomplete transmission, mis- routing, unauthorized message alteration, duplication or replay. Therefore, detailed risk assessments and careful determination of controls are indispensable. Controls required often include cryptographic methods for authentication and securing data transfer.

Further information on application security can be found in the ISO/IEC 27034 series.

8.27 Secure system architecture and engineering principles

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_net-work_security	#Protection

Control
Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.

Purpose
To ensure information systems are securely designed, implemented and operated within the development life cycle.

Guidance
Security engineering principles should be established, documented and applied to information system engineering activities. Security should be designed into all architecture layers (business, data, applications and technology). New technology should be analysed for

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

security risks and the design should be reviewed against known attack patterns.

Secure engineering principles provide guidance on user authentication techniques, secure session control and data validation and sanitisation.

Secure system engineering principles should include analysis of:
a) the full range of security controls required to protect information and systems against identified threats;
b) the capabilities of security controls to prevent, detect or respond to security events;
c) specific security controls required by particular business processes (e.g. encryption of sensitive information, integrity checking and digitally signing information);
d) where and how security controls are to be applied (e.g. by integrating with a security architecture and the technical infrastructure);
e) how individual security controls (manual and automated) work together to produce an integrated set of controls.

Security engineering principles should take account of:
a) the need to integrate with a security architecture;
b) technical security infrastructure [e.g. public key infrastructure (PKI), identity and access management (IAM), data leakage prevention and dynamic access management];
c) capability of the organization to develop and support the chosen technology;
d) cost, time and complexity of meeting security requirements;
e) current good practices.

Secure system engineering should involve:
a) the use of security architecture principles, such as “security by design”, “defence in depth”, “security by default”, “default deny”, “fail securely”, “distrust input from external applications”, “security in deployment”, “assume breach”, "least privilege", “usability and manageability” and“least functionality”;
b) a security-oriented design review to help identify information security vulnerabilities, ensure security controls are specified and meet security requirements;
c) documentation and formal acknowledgement of security controls that do not fully meet requirements (e.g. due to overriding safety requirements);
d) hardening of systems.

The organization should consider "zero trust" principles such as:
a) assuming the organization’s information systems are already breached and thus not be reliant on network perimeter security alone;
b) employing a “never trust and always verify” approach for access to information systems;
c) ensuring that requests to information systems are encrypted end-to-end;
d) verifying each request to an information system as if it originated from an open, external network, even if these requests originated internal to the organization (i.e. not automatically trusting anything inside or outside its perimeters);
e) using "least privilege" and dynamic access control techniques (see 5.15, 5.18 and 8.2). This includesauthenticating and authorizing requests for information or to systems based on contextual information such as authentication information (see 5.17), user identities (see 5.16), data about the user endpoint device, and data classification (see 5.12);
f) always authenticating requesters and always validating authorization requests to information systems based on information including authentication information (see 5.17) and user identities (5.16), data about the user endpoint device, and data classification (see 5.12), for example enforcingstrong authentication (e.g. multi-factor, see 8.5).

The established security engineering principles should be applied, where applicable, to outsourced development of information systems through the contracts and other binding agreements between the organization and the supplier to whom the organization outsources. The organization should ensure that suppliers’ security engineering practices align with the organization’s needs.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

The security engineering principles and the established engineering procedures should be regularly reviewed to ensure that they are effectively contributing to enhanced standards of security within the engineering process. They should also be regularly reviewed to ensure that they remain up-to- date in terms of combatting any new potential threats and in remaining applicable to advances in the technologies and solutions being applied.

Other information
Secure engineering principles can be applied to the design or configuration of a range of techniques, such as:
— fault tolerance and other resilience techniques;
— segregation (e.g.through virtualization or containerization);
— tamper resistance.

Secure virtualization techniques can be used to prevent interference between applications running on the same physical device. If a virtual instance of an application is compromised by an attacker, only that instance is affected. The attack has no effect on any other application or data.

Tamper resistance techniques can be used to detect tampering of information containers, whether physical (e.g. a burglar alarm) or logical (e.g. a data file). A characteristic of such techniques is that there is a record of the attempt to tamper with the container. In addition, the control can prevent the successful extraction of data through its destruction (e.g device memory can be deleted).

8.28 Secure coding

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control
Secure coding principles should be applied to software development.

Purpose
To ensure software is written securely thereby reducing the number of potential information security vulnerabilities in the software.

Guidance
General
The organization should establish organization-wide processes to provide good governance for secure coding. A minimum secure baseline should be established and applied. Additionally, such processes and governance should be extended to cover software components from third parties and open source software.

The organization should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the organization's secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape.

Planning and before coding
Secure coding principles should be used both for new developments and in reuse scenarios. These principles should be applied to development activities both within the organization and for products and services supplied by the organization to others. Planning and prerequisites before coding should include:

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

a) organization-specific expectations and approved principles for secure coding to be used for both in-house and outsourced code developments;
b) common and historical coding practices and defects that lead to information security vulnerabilities;
c) configuring development tools, such as integrated development environments (IDE), to help enforce the creation of secure code;
d) following guidance issued by the providers of development tools and execution environments as applicable;
e) maintenance and use of updated development tools (e.g. compilers);
f) qualification of developers in writing secure code;
g) secure design and architecture, including threat modelling;
h) secure coding standards and where relevant mandating their use;
i) use of controlled environments for development.

During coding

Considerations during coding should include:
a) secure coding practices specific to the programming languages and techniques being used;
b) using secure programming techniques, such as pair programming, refactoring, peer review, security iterations and test-driven development;
c) using structured programming techniques;
d) documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;
e) prohibiting the use of insecure design techniques (e.g. the use of hard-coded passwords, unapproved code samples and unauthenticated web services).

Testing should be conducted during and after development (see 8.29). Static application security testing (SAST) processes can identify security vulnerabilities in software.

Before software is made operational, the following should be evaluated:
a) attack surface and the principle of least privilege;
b) conducting an analysis of the most common programming errors and documenting that these have been mitigated.

Review and maintenance

After code has been made operational:
a) updates should be securely packaged and deployed;
b) reported information security vulnerabilities should be handled (see 8.8);
c) errors and suspected attacks should be logged and logs regularly reviewed to make adjustments to the code as necessary;
d) source code should be protected against unauthorized access and tampering (e.g. by using configuration management tools, which typically provide features such as access control and version control).

If using external tools and libraries, the organization should consider:
a) ensuring that external libraries are managed (e.g. by maintaining an inventory of libraries used and their versions) and regularly updated with release cycles;
b) selection, authorization and reuse of well-vetted components, particularly authentication and cryptographic components;
c) the licence, security and history of external components;
d) ensuring that software is maintainable, tracked and originates from proven, reputable sources;
e) sufficiently long-term availability of development resources and artefacts.

Where a software package needs to be modified the following points should be considered:
a) the risk of built-in controls and integrity processes being compromised;
b) whether to obtain the consent of the vendor;

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

c) the possibility of obtaining the required changes from the vendor as standard program updates;
d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes;
e) compatibility with other software in use.

Other information
A guiding principle is to ensure security-relevant code is invoked when necessary and is tamper-resistant. Programs installed from compiled binary code also have these properties but only for data held within the application. For interpreted languages, the concept only works when the code is executed on a server that is otherwise inaccessible by the users and processes that use it, and that its data is held in a similarly protected database. For example, the interpreted code can be run on a cloud service where access to the code itself requires administrator privileges. Such administrator access should be protected by security mechanisms such as just-in-time administration principles and strong authentication. If the application owner can access scripts by direct remote access to the server, so in principle can an attacker. Webservers should be configured to prevent directory browsing in such cases.

Application code is best designed on the assumption that it is always subject to attack, through error or malicious action. In addition, critical applications can be designed to be tolerant of internal faults. For example, the output from a complex algorithm can be checked to ensure that it lies within safe bounds before the data is used in an application such as a safety or financial critical application. The code that performs the boundary checks is simple and therefore much easier to prove correctness.

Some web applications are susceptible to a variety of vulnerabilities that are introduced by poor design and coding, such as database injection and cross-site scripting attacks. In these attacks, requests can be manipulated to abuse the webserver functionality.

More information on ICT security evaluation can be found in the ISO/IEC 15408 series.

8.29 Security testing in development and acceptance

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection

Control
Security testing processes should be defined and implemented in the development life cycle.

Purpose
To validate if information security requirements are met when applications or code are deployed to the production environment.

Guidance
New information systems, upgrades and new versions should be thoroughly tested and verified during the development processes. Security testing should be an integral part of the testing for systems or components.

Security testing should be conducted against a set of requirements, which can be expressed as functional or non-functional. Security testing should include testing of:
a) security functions [e.g. user authentication (see 8.5), access restriction (see 8.3) and use ofcryptography (see 8.24)];

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

b) secure coding (see 8.28);
c) secure configurations (see 8.9, 8.20 and 8.22) including that of operating systems, firewalls and other security components.

Test plans should be determined using a set of criteria. The extent of testing should be in proportion to the importance, nature of the system and the potential impact of the change being introduced. The test plan should include:
a) detailed schedule of activities and tests;
b) inputs and expected outputs under a range of conditions;
c) criteria to evaluate the results;
d) decision for further actions as necessary.

The organization can leverage automated tools, such as code analysis tools or vulnerability scanners, and should verify the remediation of security related defects.

For in-house developments, such tests should initially be performed by the development team. Independent acceptance testing should then be undertaken to ensure that the system works as expected and only as expected (see 5.8). The following should be considered:
a) performing code review activities as a relevant element for testing for security flaws, including un-anticipated inputs and conditions;
b) performing vulnerability scanning to identify insecure configurations and system vulnerabilities;
c) performing penetration testing to identify insecure code and design.

For outsourced development and purchasing components, an acquisition process should be followed. Contracts with the supplier should address the identified security requirements (see 5.20). Products and services should be evaluated against these criteria before acquisition.

Testing should be performed in a test environment that matches the target production environment as closely as possible to ensure that the system does not introduce vulnerabilities to the organization's environment and that the tests are reliable (see 8.31).

Other information
Multiple test environments can be established, which can be used for different kinds of testing (e.g. functional and performance testing). These different environments can be virtual, with individual configurations to simulate a variety of operating environments.

Testing and monitoring of test environments, tools and technologies also needs to be considered to ensure effective testing. The same considerations apply to monitoring of the monitoring systems deployed in development, test and production settings. Judgement is needed, guided by the sensitivity of the systems and data, to determine how many layers of meta-testing are useful.

8.30 Outsourced development

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #Detect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection

Control
The organization should direct, monitor and review the activities related to outsourced

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

system development.

Purpose
To ensure information security measures required by the organization are implemented in outsourced system development.

Guidance
Where system development is outsourced, the organization should communicate and agree requirements and expectations, and continually monitor and review whether the delivery of outsourcedwork meets these expectations. The following points should be considered across the organization's entire external supply chain:

a) licensing agreements, code ownership and intellectual property rights related to the outsourced content (see 5.32);
b) contractual requirements for secure design, coding and testing practices (see 8.25 to 8.29);
c) provision of the threat model to consider by external developers;
d) acceptance testing for the quality and accuracy of the deliverables (see 8.29);
e) provision of evidence that minimum acceptable levels of security and privacy capabilities are established (e.g. assurance reports);
f) provision of evidence that sufficient testing has been applied to guard against the presence ofmalicious content (both intentional and unintentional) upon delivery;
g) provision of evidence that sufficient testing has been applied to guard against the presence ofknown vulnerabilities;
h) escrow agreements for the software source code (e.g. if the supplier goes out of business);
i) contractual right to audit development processes and controls;
j) security requirements for the development environment (see 8.31);
k) taking consideration of applicable legislation (e.g. on protection of personal data).

Other information
Further information on supplier relationships can be found in the ISO/IEC 27036 series.

8.31 Separation of development, test and production environments

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control
Development, testing and production environments should be separated and secured.

Purpose
To protect the production environment and data from compromise by development and test activities.

Guidance
The level of separation between production, testing and development environments that is necessary to prevent production problems should be identified and implemented.
The following items should be considered:

a) adequately separating development and production systems and operating them in different domains (e.g. in separate virtual or physical environments);
b) defining, documenting and implementing rules and authorization for the deployment of software from development to production status;
c) testing changes to production systems and applications in a testing or staging environment prior to being applied to production systems (see 8.29);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) not testing in production environments except in circumstances that have been defined and approved;
e) compilers, editors and other development tools or utility programs not being accessible from production systems when not required;
f) displaying appropriate environment identification labels in menus to reduce the risk of error;
g) not copying sensitive information into the development and testing system environments unless equivalent controls are provided for the development and testing systems.

In all cases, development and testing environments should be protected considering:
a) patching and updating of all the development, integration and testing tools (including builders, integrators, compilers, configuration systems and libraries);
b) secure configuration of systems and software;
c) control of access to the environments;
d) monitoring of change to the environment and code stored therein;
e) secure monitoring of the environments;
f) taking backups of the environments.

A single person should not have the ability to make changes to both development and production without prior review and approval. This can be achieved for example through segregation of access rights or through rules that are monitored. In exceptional situations, additional measures such as detailed logging and real-time monitoring should be implemented in order to detect and act on unauthorized changes.

Other information
Without adequate measures and procedures, developers and testers having access to production systems can introduce significant risks (e.g. unwanted modification of files or system environment, system failure, running unauthorized and untested code in production systems, disclosure of confidential data, data integrity and availability issues). There is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access to the production environment.

Measures and procedures include carefully designed roles in conjunction with implementing segregation of duty requirements and having adequate monitoring processes in place.

Development and testing personnel also pose a threat to the confidentiality of production information. Development and testing activities can cause unintended changes to software or information if they share the same computing environment. Separating development, testing and production environments is therefore desirable to reduce the risk of accidental change or unauthorized access to production software and business data (see 8.33 for the protection of test information).

In some cases, the distinction between development, test and production environments can be deliberately blurred and testing can be carried out in a development environment or through controlled rollouts to live users or servers (e.g. small population of pilot users). In some cases, product testing can occur through live use of the product inside the organization. Furthermore, to reduce downtime of live deployments, two identical production environments can be supported where only one is live at any one time.

Supporting processes for the use of production data in development and testing environments (8.33) are necessary.

Organizations can also consider the guidance provided in this section for training environments when conducting end user training.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

8.32 Change management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection

Control
Changes to information processing facilities and information systems should be subject to change management procedures.

Purpose
To preserve information security when executing changes.

Guidance
Introduction of new systems and major changes to existing systems should follow agreed rules and a formal process of documentation, specification, testing, quality control and managed implementation. Management responsibilities and procedures should be in place to ensure satisfactory control of all changes.

Change control procedures should be documented and enforced to ensure the confidentiality, integrity and availability of information in information processing facilities and information systems, for the entire system development life cycle from the early design stages through all subsequent maintenance efforts.

Wherever practicable, change control procedures for ICT infrastructure and software should be integrated.

The change control procedures should include:
a) planning and assessing the potential impact of changes considering all dependencies;
b) authorization of changes;
c) communicating changes to relevant interested parties;
d) tests and acceptance of tests for the changes (see 8.29);
e) implementation of changes including deployment plans;
f) emergency and contingency considerations including fall-back procedures;
g) maintaining records of changes that include all of the above;
h) ensuring that operating documentation (see 5.37) and user procedures are changed as necessary to remain appropriate;
i) ensuring that ICT continuity plans and response and recovery procedures (see 5.30) are changed as necessary to remain appropriate.

Other information
Inadequate control of changes to information processing facilities and information systems is a common cause of system or security failures. Changes to the production environment, especially when transferring software from development to operational environment, can impact on the integrity and availability of applications.

Changing software can impact the production environment and vice versa.

Good practice includes the testing of ICT components in an environment segregated from both the production and development environments (see 8.31). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs and other updates.

Production environment includes operating systems, databases and middleware platforms.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

The control should be applied for changes of applications and infrastructures.

8.33 Test information

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

Control
Test information should be appropriately selected, protected and managed.

Purpose
To ensure relevance of testing and protection of operational information used for testing.

Guidance
Test information should be selected to ensure the reliability of tests results and the confidentiality of the relevant operational information. Sensitive information (including personally identifiable information) should not be copied into the development and testing environments (see 8.31).

The following guidelines should be applied to protect the copies of operational information, when used for testing purposes, whether the test environment is built in-house or on a cloud service:

a) applying the same access control procedures to test environments as those applied to operational environments;
b) having a separate authorization each time operational information is copied to a test environment;
c) logging the copying and use of operational information to provide an audit trail;
d) protecting sensitive information by removal or masking (see 8.11) if used for testing;
e) properly deleting (see 8.10) operational information from a test environment immediately after thetesting is complete to prevent unauthorized use of test information.

Test information should be securely stored (to prevent tampering, which can otherwise lead to invalid results) and only used for testing purposes.

Other information
System and acceptance testing can require substantial volumes of test information that are as close as possible to operational information.

8.34 Protection of information systems during audit testing

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protec-tion

Control
Audit tests and other assurance activities involving assessment of operational systems should be planned and agreed between the tester and appropriate management.

Purpose
To minimize the impact of audit and other assurance activities on operational systems and business processes.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Guidance

The following guidelines should be observed:

a) agreeing audit requests for access to systems and data with appropriate management;
b) agreeing and controlling the scope of technical audit tests;
c) limiting audit tests to read-only access to software and data. If read-only access is not available to obtain the necessary information, executing the test by an experienced administrator who has the necessary access rights on behalf of the auditor;
d) if access is granted, establishing and verifying the security requirements (e.g. antivirus and patching) of the devices used for accessing the systems (e.g. laptops or tablets) before allowing the access;
e) only allowing access other than read-only for isolated copies of system files, deleting them when the audit is completed, or giving them appropriate protection if there is an obligation to keep such files under audit documentation requirements;
f) identifying and agreeing on requests for special or additional processing, such as running audit tools;
g) running audit tests that can affect system availability outside business hours;
h) monitoring and logging all access for audit and test purposes.

Other information

Audit tests and other assurance activities can also happen on development and test systems, where such tests can impact for example the integrity of code or lead to disclosure of any sensitive information held in such environments.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Annex A
(informative)
Using attributes

A.1 General

This annex provides a table to demonstrate the use of attributes as a way of creating different views of the controls. The five examples of attributes are (see 4.2):

a) Control types (#Preventive, #Detective, #Corrective)
b) Information security properties (#Confidentiality, #Integrity, #Availability)
c) Cybersecurity concepts (#Identify, #Protect, #Detect, #Respond, #Recover)
d) Operational capabilities (#Governance, #Asset_management, #Information_protection, #Human_ resource_security, #Physical_security, #System_and_network_security, #Application_security, #Secure_configuration, #Identity_and_access_management, #Threat_and_vulnerability_ management, #Continuity, #Supplier_relationships_security, #Legal_and_compliance, #Information_security_event_management, #Information_security_assurance)
e) Security domains (#Governance_and_Ecosystem, #Protection, #Defence, #Resilience) Table A.1 contains a matrix of all controls in this document with their given attribute values.

The filtering or sorting of the matrix can be achieved by using a tool such as a simple spreadsheet or a database, which can include more information like control text, guidance, organization-specific guidance or attributes (see A.2).

Table A.1 — Matrix of controls and attribute values

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
5.2	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
5.3	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_access_management	#Governance_and_Ecosystem
5.4	Management responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contact with special interest groups	#Preventive #Corrective	#Confidential- ity #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Threat intelligence	#Preventive #Detective #Corrective	#Confidential- ity #Integrity #Availability	#Identify #De tect #Respond	#Threat_and _ vulnerability_ management	#Defence #Resilience
5.8	Information security in project management	#Preventive	#Confidential- ity #Integrity #Availability	#Identify #Protect	#Governance	#Governance _and_Ecosyst em #Protec- tion
5.9	Inventory of information and other associated assets	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Asset_man- agement	#Governance _and_Ecosyst em #Protection
5.10	Acceptable use of information and other associated assets	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement #Information _protection	#Governance _and_Ecosyst em #Protection
5.11	Return of assets	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Asset_man- agement	#Protection
5.12	Classification of information	#Preventive	#Confidential- ity #Integrity #Availability	#Identify	#Information _protection	#Protection #Defence
5.13	Labelling of information	#Preventive	#Confidential- ity #Integrity #Availability	#Protect	#Information _protection	#Defence #Protection

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.14	Information transfer	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
5.15	Access control	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.16	Identity management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.17	Authentication information	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.18	Access rights	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
5.19	Information security in supplier relationships	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
5.20	Addressing information security within supplier agreements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
5.21	Managing information security in the ICT supply chain	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
5.22	Monitoring, review and change management of supplier services	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Supplier_relationships_security #Information_security_assurance	#Governance_and_Ecosystem #Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.23	Information security for use of cloud services	#Preventive	#Confidential - ity #Integrity #Availability	#Protect	#Supplier_relationships_security	#Governance_and_Ecosystem #Protection
5.24	Information security inci- dent manage- ment planning and prepara- tion	#Corrective	#Confidential - ity #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.25	Assessment and decision on informa- tion security events	#Detective	#Confidential - ity #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
5.26	Response to information security inci- dents	#Corrective	#Confidential - ity #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence
5.27	Learning from information security inci- dents	#Preventive	#Confidential - ity #Integrity #Availability	#Identify #Protect	#Information_security_event_management	#Defence
5.28	Collection of evidence	#Corrective	#Confidential - ity #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
5.29	Information security dur- ing disruption	#Preventive #Corrective	#Confidential - ity #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.31	Legal, statutory, regulatory and contractual requirements	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem #Protection
5.32	Intellectual property rights	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Legal_and_compliance	#Governance_and_Ecosystem
5.33	Protection of **records**	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Asset_management #Information_protection	#Defence
5.34	Privacy and protection of PII	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_protection #Legal_and_compliance	#Protection
5.35	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosystem
5.36	Compliance with policies, rules and standards for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Legal_and_compliance #Information_security_assurance	#Governance_and_Ecosystem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.37	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
6.1	Screening	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.2	Terms and conditions of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.3	Information security awareness, education and training	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security	#Governance_and_Ecosystem
6.4	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosystem

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
6.5	Responsibilities after termination or change of employment	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Human_resource_security #Asset_management	#Governance_and_Ecosystem
6.6	Confidentiality or non-disclosure agreements	#Preventive	#Confidentiality	#Protect	#Human_resource_security #Information_protection #Supplier_relationships	#Governance_and_Ecosystem
6.7	Remote working	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection #Physical_security #System_and_network_security	#Protection
6.8	Information security event reporting	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Defence
7.1	Physical security perimeters	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
7.2	Physical entry	#Preventive	#Confidentiaity #Integrity #Availability	#Protect	#Physical_security #Identity_and_Access_Management	#Protection
7.3	Securing offices, rooms and facilities	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
7.4	Physical security monitoring	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#Physical_security	#Protection #Defence
7.5	Protecting against physical and environmental threats	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
7.6	Working in secure areas	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection
7.7	Clear desk and clear screen	#Preventive	#Confidentiality	#Protect	#Physical_security	#Protection
7.8	Equipment siting and protection	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
7.9	Security of assets off premises	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
7.10	Storage media	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection
7.11	Supporting utilities	#Preventive #Detective	#Integrity #Availability	#Protect #Detect	#Physical_security	#Protection
7.12	Cabling security	#Preventive	#Confidentiality #Availability	#Protect	#Physical_security	#Protection
7.13	Equipment maintenance	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security #Asset_management	#Protection #Resilience

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
7.14	Secure disposal or reuse of equipment	#Preventive	#Confidentiality	#Protect	#Physical_security #Asset_management	#Protection
8.1	User endpoint devices	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Asset_management #Information_protection	#Protection
8.2	Privileged access rights	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
8.3	Information access restriction	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_ access_man-agement	#Protection
8.4	Access to source code	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_ and_access_ management #Application_ security #Secure_configuration	#Protection
8.5	Secure authentication	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Identity_and_access_management	#Protection
8.6	Capacity management	#Preventive #Detective	#Integrity #Availability	#Identify #Protect #De- tect	#Continuity	#Governance_and_Ecosystem #Protection
8.7	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #De- tect	#System_and_network_security #Information_protection	#Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.8	Management of technical vulnerabilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_vulnerability_management	#Governance_and_Ecosystem #Protection #Defence
8.9	Configuration management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
8.10	Information deletion	#Preventive	#Confidentiality	#Protect	#Information_protection #Legal_and_compliance	#Protection
8.11	Data masking	#Preventive	#Confidentiality	#Protect	#Information_protection	#Protection
8.12	Data leakage prevention	#Preventive #Detective	#Confidentiality	#Protect #Detect	#Information_protection	#Protection #Defence
8.13	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.14	Redundancy of information processing facilities	#Preventive	#Availability	#Protect	#Continuity #Asset_management	#Protection #Resilience
8.15	Logging	#Detective	#Confidentiality #Integrity #Availability	#Detect	#Information_security_event_management	#Protection #Defence
8.16	Monitoring activities	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
8.17	Clock synchro-nization	#Detective	#Integrity	#Protect #Detect	#Information_security_event_management	#Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.18	Use of privileged utility programs	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Secure_configuration #Application_security	#Protection
8.19	Installation of software on operational systems	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration #Application_security	#Protection
8.20	Networks security	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security	#Protection
8.21	Security of network services	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.22	Segregation of networks	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.23	Web filtering	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security	#Protection
8.24	Use of cryptography	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection
8.25	Secure development life cycle	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.26	Application security requirements	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.27	Secure system architecture and engineeriing principles	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.28	Secure coding	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.29	Security testing in development and acceptance	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Application_security #Information_security_assurance #System_and_network_security	#Protection
8.30	Outsourced development	#Preventive #Detective	#Confidentiality #Integrity #Availability	#Identify #Protect #De-tect	#System_and_network_security #Application_security #Supplier_relationships_security	#Governance_and_Ecosystem #Protection
8.31	Separation of development, test and production environments	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.32	Change management	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Application_security #System_and_network_security	#Protection
8.33	Test information	#Preventive	#Confidentiality #Integrity	#Protect	#Information_protection	#Protection

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.1 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.34	Protection of information systems during audit testing	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#System_and_network_security #Information_protection	#Governance_and_Ecosystem #Protection

Table A.2 shows an example of how to create a view by filtering by a particular attribute value, in this case #Corrective.

Table A.2 — View of #Corrective controls

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.5	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience
5.6	Contact with special interest groups	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond #Recover	#Governance	#Defence
5.7	Threat intelligence	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_vulnerability_management	#Defence #Resilience
5.24	Information security incident management planning and preparation	#Corrective	#Confidentiality #Integrity #Availability	#Respond #Recover	#Governance #Information_security_event_management	#Defence
5.26	Response to information security incidents	#Corrective	#Confidentiallity #Integrity #Availability	#Respond #Recover	#Information_security_event_management	#Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table A.2 *(continued)*

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.28	Collection of evidence	#Corrective	#Confidentiality #Integrity #Availability	#Detect #Respond	#Information_security_event_management	#Defence
5.29	Information security during disruption	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Continuity	#Protection #Resilience
5.30	ICT readiness for business continuity	#Corrective	#Availability	#Respond	#Continuity	#Resilience
5.35	Independent review of information security	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect	#Information_security_assurance	#Governance_and_Ecosytem
5.37	Documented operating procedures	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Recover	#Asset_management #Physical_security #System_and_network_security #Application_security #Secure_configuration #Identity_and_access_management #Threat_and_vulnerability management #Continuity #Information_security_event_management	#Governance_and_Ecosystem #Protection #Defence
6.4	Disciplinary process	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Protect #Respond	#Human_resource_security	#Governance_and_Ecosytem
8.7	Protection against malware	#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Protect #Detect	#System_and_network_security #Information_protection	#Protection #Defence

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

ISO/ IEC 27002 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
8.13	Information backup	#Corrective	#Integrity #Availability	#Recover	#Continuity	#Protection
8.16	Monitoring activities	#Detective #Corrective	#Confidentiality #Integrity #Availability	#Detect #Re-spond	#Information_security_event_management	#Defence

A.2 Organizational views

Since attributes are used to create different views of controls, organizations can discard the examples of attributes proposed in this document and create their own attributes with different values to address specific needs in the organization. In addition, the values assigned to each attribute can differ between organizations since organizations can have different views on the use or applicability of the control or of the values associated to the attribute (when the values are specific to the context of the organization). The first step is to understand why an organizational-specific attribute is desirable. For example, if an organization has constructed its risk treatment plans [see ISO/IEC 27001:2013, 6.1.3 e)] based on events, it can wish to associate a risk scenario attribute to each control in this document.

The benefit of such an attribute is to speed up the process of fulfilment of ISO/IEC 27001 requirement related to risk treatment, which is to compare the controls determined through the process of risk treatment (referred to as “necessary” controls), with those in ISO/IEC 27001:2013, Annex A (which are issued from in this document) to ensure that no necessary control has been overlooked.

Once the purpose and benefits are known, the next step is to determine the attribute values. For example, the organization might identify 9 events:

1) loss or theft of mobile device;
2) loss or theft from organization’s premises;
3) force majeure, vandalism and terrorism;
4) failure of software, hardware, power, internet and communications;
5) fraud;
6) hacking;
7) disclosure;
8) breach of the law;
9) social engineering.

The second step can therefore be accomplished by assigning identifiers to each event (e.g. E1, E2, ..., E9).

The third step is to copy the control identifiers and control names from this document into a spreadsheet or database and associate the attribute values with each control, remembering that each control can have more than one attribute value.

The final step is to sort the spreadsheet or query the database to extract the required information. Other examples of organizational attributes (and possible values) include:

a) maturity (values from the ISO/IEC 33000 series or other maturity models);
b) implementation state (to do, in progress, partially implemented, fully implemented);
c) priority (1, 2, 3, etc.);

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

d) organizational areas involved (security, ICT, human resources, top management, etc.);
e) events;
f) assets involved;
g) build and run, to differentiate controls used in the different steps of the service life cycle;
h) other frameworks the organization works with or can be transitioning from.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Annex B
(informative)
Correspondence of ISO/IEC 27002:2022 (this document) withISO/IEC 27002:2013

The purpose of this annex is to provide backwards compatibility with ISO/IEC 27002:2013 for organizations that are currently using that standard and now wish to transition to this edition.

Table B.1 provides the correspondence of the controls specified in Clauses 5 to 8 with those in ISO/IEC 27002:2013.

Table B.1 — Correspondence between controls in this document and controls in ISO/IEC 27002:2013

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.1	05.1.1, 05.1.2	Policies for information security
5.2	06.1.1	Information security roles and responsibilities
5.3	06.1.2	Segregation of duties
5.4	07.2.1	Management responsibilities
5.5	06.1.3	Contact with authorities
5.6	06.1.4	Contact with special interest groups
5.7	New	Threat intelligence
5.8	06.1.5, 14.1.1	Information security in project management
5.9	08.1.1, 08.1.2	Inventory of information and other associated assets
5.10	08.1.3, 08.2.3	Acceptable use of information and other associated assets
5.11	08.1.4	Return of assets
5.12	08.2.1	Classification of information
5.13	08.2.2	Labelling of information
5.14	13.2.1, 13.2.2, 13.2.3	Information transfer
5.15	09.1.1, 09.1.2	Access control
5.16	09.2.1	Identity management
5.17	09.2.4, 09.3.1, 09.4.3	Authentication information
5.18	09.2.2, 09.2.5, 09.2.6	Access rights
5.19	15.1.1	Information security in supplier relationships
5.20	15.1.2	Addressing information security within supplier agreements
5.21	15.1.3	Managing information security in the ICT supply chain

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.1 *(continued)*

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
5.22	15.2.1, 15.2.2	Monitoring, review and change management of supplier services
5.23	New	Information security for use of cloud services
5.24	16.1.1	Information security incident management planning and preparation
5.25	16.1.4	Assessment and decision on information security events
5.26	16.1.5	Response to information security incidents
5.27	16.1.6	Learning from information security incidents
5.28	16.1.7	Collection of evidence
5.29	17.1.1, 17.1.2, 17.1.3	Information security during disruption
5.30	New	ICT readiness for business continuity
5.31	18.1.1, 18.1.5	Legal, statutory, regulatory and contractual requirements
5.32	18.1.2	Intellectual property rights
5.33	18.1.3	Protection of records
5.34	18.1.4	Privacy and protection of PII
5.35	18.2.1	Independent review of information security
5.36	18.2.2, 18.2.3	Compliance with policies, rules and standards for information security
5.37	12.1.1	Documented operating procedures
6.1	07.1.1	Screening
6.2	07.1.2	Terms and conditions of employment
6.3	07.2.2	Information security awareness, education and training
6.4	07.2.3	Disciplinary process
6.5	07.3.1	Responsibilities after termination or change of employment
6.6	13.2.4	Confidentiality or non-disclosure agreements
6.7	06.2.2	Remote working
6.8	16.1.2, 16.1.3	Information security event reporting
7.1	11.1.1	Physical security perimeters
7.2	11.1.2, 11.1.6	Physical entry
7.3	11.1.3	Securing offices, rooms and facilities
7.4	New	Physical security monitoring
7.5	11.1.4	Protecting against physical and environmental threats
7.6	11.1.5	Working in secure areas
7.7	11.2.9	Clear desk and clear screen
7.8	11.2.1	Equipment siting and protection
7.9	11.2.6	Security of assets off-premises
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Storage media
7.11	11.2.2	Supporting utilities

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.1 *(continued)*

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2022 control identifier	Control name
7.12	11.2.311.2.3	Cabling security
7.13	11.2.411.2.4	Equipment maintenance
7.14	11.2.711.2.7	Secure disposal or re-use of equipment
8.1	06.2.1, 11.2.8	User endpoint devices
8.2	09.2.3	Privileged access rights
8.3	09.4.1	Information access restriction
8.4	09.4.5	Access to source code
8.5	09.4.2	Secure authentication
8.6	12.1.3	Capacity management
8.7	12.2.1	Protection against malware
8.8	12.6.1, 18.2.3	Management of technical vulnerabilities
8.9	New	Configuration management
8.10	New	Information deletion
8.11	New	Data masking
8.12	New	Data leakage prevention
8.13	12.3.1	Information backup
8.14	17.2.1	Redundancy of information processing facilities
8.15	12.4.1, 12.4.2, 12.4.3	Logging
8.16	New	Monitoring activities
8.17	12.4.4	Clock synchronization
8.18	09.4.4	Use of privileged utility programs
8.19	12.5.1, 12.6.2	Installation of software on operational systems
8.20	13.1.1	Networks security
8.21	13.1.2	Security of network services
8.22	13.1.3	Segregation of networks
8.23	New	Web filtering
8.24	10.1.1, 10.1.2	Use of cryptography
8.25	14.2.1	Secure development life cycle
8.26	14.1.2, 14.1.3	Application security requirements
8.27	14.2.5	Secure system architecture and engineering principles
8.28	New	Secure coding
8.29	14.2.8, 14.2.9	Security testing in development and acceptance
8.30	14.2.7	Outsourced development
8.31	12.1.4, 14.2.6	Separation of development, test and production environments

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.1 *(continued)*

ISO/IEC 27002:2022 control identifier	ISO/IEC 27002:2013 control identifier	Control name
8.32	12.1.2, 14.2.2, **14.2.3, 14.2.4**	Change management
8.33	14.3	Test information
8.34	12.7.1	Protection of information systems during audit testing

Table B.2 provides the correspondence of controls specified in ISO/IEC 27002:2013 with those in this document.

Table B.2 — Correspondence between controls in ISO/IEC 27002:2013 and controls in thisdocument

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 ontrol identifier	Control name according to ISO/IEC 27002:2013
5		Information security policies
5.1		Management direction for information security
5.1.1	5.1	Policies for information security
5.1.2	5.1	Review of the policies for information security
6		Organization of information security
6.1		Internal organization
6.1.1	5.2	Information security roles and responsibilities
6.1.2	5.3	Segregation of duties
6.1.3	5.5	Contact with authorities
6.1.4	5.6	Contact with special interest groups
6.1.5	5.8	Information security in project management
6.2		Mobile devices and teleworking
6.2.1	8.1	Mobile device policy
6.2.2	6.7	Teleworking
7		Human resource security
7.1		Prior to employment
7.1.1	6.1	Screening
7.1.2	6.2	Terms and conditions of employment
7.2		During employment
7.2.1	5.4	Management responsibilities
7.2.2	6.3	Information security awareness, education and training
7.2.3	6.4	Disciplinary process
7.3		Termination and change of employment
7.3.1	6.5	Termination or change of employment responsibilities

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.2 *(continued)*

ISO/IEC 27002:2013 control identifier	ISO/IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
8		Asset management
8.1		Responsibility for assets
8.1.1	5.9	Inventory of assets
8.1.2	5.9	Ownership of assets
8.1.3	5.1	Acceptable use of assets
8.1.4	5.11	Return of assets
8.2		Information classification
8.2.1	5.12	Classification of information
8.2.2	5.13	Labelling of information
8.2.3	5.1	Handling of assets
8.3		Media handling
8.3.1	7.1	Management of removable media
8.3.2	7.1	Disposal of media
8.3.3	7.1	Physical media transfer
9		Access control
9.1		Business requirements of access control
9.1.1	5.15	Access control policy
9.1.2	5.15	Access to networks and network services
9.2		User access management
9.2.1	5.16	User registration and de-registration
9.2.2	5.18	User access provisioning
9.2.3	8.2	Management of privileged access rights
9.2.4	5.17	Management of secret authentication information of users
9.2.5	5.18	Review of user access rights
9.2.6	5.18	Removal or adjustment of access rights
9.3		User responsibilities
9.3.1	5.17	Use of secret authentication information
9.4		System and application access control
9.4.1	8.3	Information access restriction
9.4.2	8.5	Secure log-on procedures
9.4.3	5.17	Password management system
9.4.4	8.18	Use of privileged utility programs
9.4.5	8.4	Access control to program source code
10		Cryptography
10.1		Cryptographic controls
10.1.1	8.24	Policy on the use of cryptographic controls
10.1.2	8.24	Key management
11		Physical and environmental security
11.1		Secure areas

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.2 *(continued)*

ISO/IEC 27002:2013 Control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
11.1.1	7.1	Physical security perimeter
11.1.2	7.2	Physical entry controls
11.1.3	7.3	Securing offices, rooms and facilities
11.1.4	7.5	Protecting against external and environmental threats
11.1.5	7.6	Working in secure areas
11.1.6	7.2	Delivery and loading areas
11.2		Equipment
11.2.1	7.8	Equipment siting and protection
11.2.2	7.11	Supporting utilities
11.2.3	7.12	Cabling security
11.2.4	7.13	Equipment maintenance
11.2.5	7.1	Removal of assets
11.2.6	7.9	Security of equipment and assets off-premises
11.2.7	7.14	Secure disposal or reuse of equipment
11.2.8	8.1	Unattended user equipment
11.2.9	7.7	Clear desk and clear screen policy
12		Operations security
12.1		Operational procedures and responsibilities
12.1.1	5.37	Documented operating procedures
12.1.2	8.32	Change management
12.1.3	8.6	Capacity management
12.1.4	8.31	Separation of development, testing and operational environments
12.2		Protection from malware
12.2.1	8.7	Controls against malware
12.3		Backup
12.3.1	8.13	Information backup
12.4		Logging and monitoring
12.4.1	8.15	Event logging
12.4.2	8.15	Protection of log information
12.4.3	8.15	Administrator and operator logs
12.4.4	8.17	Clock synchronization
12.5		Control of operational software
12.5.1	8.19	Installation of software on operational systems
12.6		Technical vulnerability management
12.6.1	8.8	Management of technical vulnerabilities
12.6.2	8.19	Restrictions on software installation
12.7		Information systems audit considerations
12.7.1	8.34	Information systems audit controls
13		Communications security
13.1		Network security management facilities.

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.2 *(continued)*

ISO/IEC 27002:2013 control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
13.1.1	8.2	Network controls
13.1.2	8.21	Security of network services
13.1.3	8.22	Segregation in networks
13.2		Information transfer
13.2.1	5.14	Information transfer policies and procedures
13.2.2	5.14	Agreements on information transfer
13.2.3	5.14	Electronic messaging
13.2.4	6.6	Confidentiality or nondisclosure agreements
14		System acquisition, development and maintenance
14.1		Security requirements of information systems
14.1.1	5.8	Information security requirements analysis and specification
14.1.2	8.26	Securing application services on public networks
14.1.3	8.26	Protecting application services transactions
14.2		Security in development and support processes
14.2.1	8.25	Secure development policy
14.2.2	8.32	System change control procedures
14.2.3	8.32	Technical review of applications after operating platform changes
14.2.4	8.32	Restrictions on changes to software packages
14.2.5	8.27	Secure system engineering principles
14.2.6	8.31	Secure development environment
14.2.7	8.3	Outsourced development
14.2.8	8.29	System security testing
14.2.9	8.29	System acceptance testing
14.3		Test data
14.3.1	8.33	Protection of test data
15		Supplier relationships
15.1		Information security in supplier relationships
15.1.1	5.19	Information security policy for supplier relationships
15.1.2	5.2	Addressing security within supplier agreements
15.1.3	5.21	Information and communication technology supply chain
15.2		Supplier service delivery management
15.2.1	5.22	Monitoring and review of supplier services
15.2.2	5.22	Managing changes to supplier services
16		Information security incident management
16.1		Management of information security incidents and improvements
16.1.1	5.24	Responsibilities and procedures
16.1.2	6.8	Reporting information security events
16.1.3	6.8	Reporting information security weaknesses

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Table B.2 *(continued)*

ISO/IEC 27002:2013 control identifier	ISO/ IEC 27002:2022 control identifier	Control name according to ISO/IEC 27002:2013
16.1.4	5.25	Assessment of and decision on information security events
16.1.5	5.26	Response to information security incidents
16.1.6	5.27	Learning from information security incidents
16.1.7	5.28	Collection of evidence
17		Information security aspects of business continuity management
17.1		Information security continuity
17.1.1	5.29	Planning information security continuity
17.1.2	5.29	Implementing information security continuity
17.1.3	5.29	Verify, review and evaluate information security continuity
17.2		Redundancies
17.2.1	8.14	Availability of information processing facilities
18		Compliance
18.1		Compliance with legal and contractual requirements
18.1.1	5.31	Identification of applicable legislation and contractual requirements
18.1.2	5.32	Intellectual property rights
18.1.3	5.33	Protection of records
18.1.4	5.34	Privacy and protection of personally identifiable information
18.1.5	5.31	Regulation of cryptographic controls
18.2		Information security reviews
18.2.1	5.35	Independent review of information security
18.2.2	5.36	Compliance with security policies and standards
18.2.3	5.36, 8.8	Technical compliance review

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
[2] ISO 55001, *Asset management — Management systems — Requirements*
[3] ISO/IEC 11770 (all parts), *Information security — Key management*
[4] ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*
[5] ISO 15489 (all parts), *Information and documentation — Records management*
[6] ISO/IEC 17788, *Information technology — Cloud computing — Overview and vocabulary*
[7] ISO/IEC 17789, *Information technology — Cloud computing — Reference architecture*
[8] ISO/IEC 19086 (all parts), *Cloud computing — Service level agreement (SLA) framework*
[9] ISO/IEC 19770 (all parts), *Information technology — IT asset management*
[10] ISO/IEC 19941, *Information technology — Cloud computing — Interoperability and portability*
[11] ISO/IEC 20889, *Privacy enhancing data de-identification terminology and classification of techniques*
[12] ISO 21500, *Project, programme and portfolio management — Context and concepts*
[13] ISO 21502, *Project, programme and portfolio management — Guidance on project management*
[14] ISO 22301, *Security and resilience — Business continuity management systems — Requirements*
[15] ISO 22313, *Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301*
[16] ISO/TS 22317, *Societal security — Business continuity management systems — Guidelines for business impact analysis (BIA)*
[17] ISO 22396, *Security and resilience — Community resilience — Guidelines for information exchange between organizations*
[18] ISO/IEC TS 23167, *Information technology — Cloud computing — Common technologies and techniques*
[19] ISO/IEC 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
[20] ISO/IEC 24760 (all parts), *IT Security and Privacy — A framework for identity management*
[21] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*
[22] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
[23] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
[24] ISO/IEC TS 27008, *Information technology — Security techniques — Guidelines for the assessment of information security controls*
[25] ISO/IEC 27011, *Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*
[26] ISO/IEC TR 27016, *Information technology — Security techniques — Information security management — Organizational economics*
[27] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
[28] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
[29] ISO/IEC 27019, *Information technology — Security techniques — Information security controls for the energy utility industry*
[30] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for*

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

information andcommunication technology readiness for business continuity
[31] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*
[32] ISO/IEC 27034 (all parts), *Information technology — Application security*
[33] ISO/IEC 27035 (all parts), *Information technology — Security techniques — Information securityincident management*
[34] ISO/IEC 27036 (all parts), *Information technology — Security techniques — Information securityfor supplier relationships*
[35] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*
[36] ISO/IEC 27040, *Information technology — Security techniques — Storage security*
[37] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*
[38] ISO/IEC TS 27110, *Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines*
[39] ISO/IEC 27701, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacyinformation management — Requirements and guidelines*
[40] ISO 27799, *Health informatics — Information security management in health using ISO/IEC 27002*
[41] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*
[42] ISO/IEC 29115, *Information technology — Security techniques — Entity authentication assurance framework*
[43] ISO/IEC 29134, *Information technology — Security techniques — Guidelines for privacy impactassessment*
[44] ISO/IEC 29146, *Information technology — Security techniques — A framework for access management*
[45] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*
[46] ISO 30000, *Ships and marine technology — Ship recycling management systems — Specifications for management systems for safe and environmentally sound ship recycling facilities*
[47] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*
[48] ISO 31000:2018, *Risk management — Guidelines*
[49] IEC 31010, *Risk management — Risk assessment techniques*
[50] ISO/IEC 22123 (all parts), *Information technology — Cloud computing*
[51] ISO/IEC 27555, *Information security, cybersecurity and privacy protection — Guidelines on personally identifiable information deletion*
[52] INFORMATION SECURITY FORUM (ISF). The ISF Standard of Good Practice for Information Security 2020, August 2018. Available at https: /www.securityforum.org/tool/standard-of-good-practice-for-information-security-2020/
[53] ITIL® Foundation, ITIL 4 edition, AXELOS, February 2019, ISBN: 9780113316076
[54] NATIONAL INSTITUTE OF STANDARDS and TECHNOLOGY (NIST), SP 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, Revision 2. December 2018 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-37r2
[55] Open Web APPLICATION SECURITY PROJECT (OWASP). OWASP Top Ten - 2017, The Ten MostCritical Web Application Security Risks, 2017 [viewed 2020-07-31]. Available at https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/
[56] Open Web APPLICATION SECURITY PROJECT (OWASP). OWASP Developer Guide, [online] [viewed 2020-10-22]. Available at https://github.com/OWASP/DevGuide
[57] NATIONAL INSTITUTE OF STANDARDS and TECHNOLOGY (NIST), SP 800-63B, Digital Identity Guidelines; Authentication and Lifecycle Management. February 2020 [viewed 2020-07-31]. Available at https://doi.org/10.6028/NIST.SP.800-63b
[58] OASIS, Structured Threat Information Expression. Available at https://www.oasis-open.org/standards#stix2.0
[59] OASIS, Trusted Automated Exchange of Indicator Information. Available at https://www.oasis-open.org/standards#taxii2.0

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Informasi pendukung terkait perumus standar

1. Komite teknis perumus SNI

Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

2. Susunan keanggotaan komite teknis perumus SNI

Ketua : Soetedjo Joewono
Sekretaris : Agus Prasetyo
Anggota :
1. Pinuji Prasetyaningtyas
2. Hilman Pradana
3. Baga Gusdiana
4. Zaenal Arifin
5. Chandra Yulistia
6. Bisyron Wahyudi
7. Wisnoe Prasetyo Pribadi
8. Sarwono Sutikno
9. Satriyo Wibowo

3. Konseptor SNI

Gugus Kerja 1 Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

Ketua : Chandra Yulistia
Wakil Ketua : Zaenal Arifin
Sekretaris : Mahendra Yudhistira
Anggota :
1. Obrina Chandra Brlyant
2. Satriyo Wibowo
3. Harun Al-Rasyid
4. Magdalena Christine

4. Sekretariat pengelola komite teknis perumus SNI

Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

Hak cipta Badan Standardisasi Nasional. Salinan standar ini dibuat oleh BSN untuk PT SCCI | PT Surveyor Carbon Consulting Indonesia | prapanca@scci.co.id

BADAN STANDARDISASI NASIONAL - BSN
e-mail: bsn@bsn.go.id
www.bsn.go.id