RSNI3

Rancangan Standar Nasional Indonesia 3

RSNI3 ISO/IEC 27035-1:2023
(Ditetapkan oleh BSN tahun 2024)

Teknologi informasi – Manajemen insiden keamanan informasi – Bagian 1: Prinsip dan proses

Information technology – Information security incident management – Part 1: Principles and process

(ISO/IEC 27035-1:2023, IDT)

ICS 35.030

BADAN STANDARDISASI NASIONAL

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

Diterbitkan di Jakarta

Daftar isi

Prakata

SNI ISO/IEC 27035-1:2023, *Teknologi informasi – Manajemen insiden keamanan informasi – Bagian 1: Prinsip*, merupakan standar revisi dari SNI ISO/IEC 27035-1:2016, *Teknologi informasi – Teknik Keamanan – Manajemen insiden keamanan informasi – Bagian 1: Prinsip manajemen insiden*. Standar ini disusun dengan jalur adopsi tingkat keselarasan identik dari ISO/IEC 27035-1:2023*, Information technology – Information security incident management – Part 1: Principles and process*, dengan metode adopsi terjemahan dua bahasa dan ditetapkan oleh BSN Tahun 2024.

Standar ini merupakan bagian dari seri SNI ISO/IEC 27035, *Teknologi informasi – Manajemen insiden keamanan informasi*, yang terdiri dari beberapa bagian yaitu:

− Bagian 1: Prinsip dan proses;

− Bagian 2: Pedoman perencanaan dan persiapan respons insiden;

− Bagian 3: Pedoman untuk operasi tanggap insiden TIK.

Standar ini disusun oleh Komite Teknis 35-04, Keamanan Informasi, Keamanan Siber dan Perlindungan Privasi. Standar ini telah dibahas melalui rapat teknis dan disepakati dalam rapat konsensus pada tanggal 11 Oktober 2024 di Jakarta. Konsensus ini dihadiri oleh para pemangku kepentingan (*stakeholder*) terkait, yaitu perwakilan dari produsen, konsumen, pakar dan pemerintah. Standar ini telah melalui tahap jajak pendapat pada tanggal 31 Oktober 2024 sampai dengan 14 November 2024 dengan hasil akhir disetujui menjadi SNI.

Terdapat standar ISO/IEC yang digunakan sebagai acuan dalam standar ini telah diadopsi menjadi Standar Nasional Indonesia (SNI) sebagai berikut:

– ISO/IEC 27000*, Information technology — Security techniques — Information security management systems – Overview and vocabulary* telah diadopsi secara identik menjadi SNI ISO/IEC 27000:2018, *Teknologi informasi — Teknik keamanan — Sistem manajemen keamanan informasi — Gambaran umum dan kosakata*

Perlu diperhatikan bahwa kemungkinan beberapa unsur dari Standar ini dapat berupa hak kekayaan intelektual (HAKI). Namun selama proses perumusan SNI, Badan Standardisasi Nasional telah memperhatikan penyelesaian terhadap kemungkinan adanya HAKI terkait substansi SNI. Apabila setelah penetapan SNI masih terdapat permasalahan terkait HAKI, Badan Standardisasi Nasional tidak bertanggung jawab mengenai bukti, validitas, dan ruang lingkup dari HAKI tersebut.

Apabila pengguna menemukan keraguan dalam standar ini maka disarankan untuk melihat standar aslinya, yaitu ISO/IEC 27035-1:2023 (E) dan/atau dokumen terkait lain yang menyertainya.

Pendahuluan

Seri ISO/IEC 27035 menyediakan panduan tambahan untuk kontrol pada manajemen insiden dalam ISO/IEC 27002. Kontrol ini sebaiknya diimplementasikan berdasarkan risiko keamanan informasi yang dihadapi organisasi.

Kebijakan atau kontrol keamanan informasi sendiri tidak menjamin proteksi total atas informasi, sistem informasi, layanan atau jaringan. Setelah kontrol diimplementasikan, residu kerentanan bisa tetap ada yang mengurangi efektivitas keamanan informasi dan memfasilitasi kemunculan insiden keamanan informasi. Ini dapat berpotensi memberikan konsekuensi kerugian secara langsung dan tidak langsung pada operasi bisnis organisasi. Selain itu, tidak dapat dihindari bahwa kejadian baru dari ancaman yang sebelumnya tidak teridentifikasi menjadi penyebab insiden muncul. Persiapan tidak memadai oleh organisasi dalam menangani insiden membuat respons apa pun kurang efektif, dan memperamat tingkat potensi konsekuensi bisnis yang merugikan. Oleh karena itu, esensial bagi organisasi mana pun yang menginginkan program keamanan informasi yang kuat memiliki pendekatan terstruktur dan terencana untuk:

— merencanakan dan mempersiapkan manajemen insiden keamanan informasi, termasuk kebijakan, organisasi, rencana, dukungan teknis, kesadaran dan pelatihan keterampilan, dll.;

— mendeteksi, melaporkan dan menilai insiden dan kerentanan keamanan informasi yang terlibat dalam insiden;

— merespons insiden keamanan informasi, termasuk aktivasi kontrol yang tepat untuk mencegah, mengurangi, dan pulih dari dampak;

— mengurusi kerentanan keamanan informasi yang dilaporkan terlibat dalam insiden dengan tepat;

— belajar dari insiden keamanan informasi dan kerentanan yang terlibat dengan insiden, mengimplementasikan dan memverifikasi kontrol preventif, dan membuat peningkatan pada pendekatan untuk manajemen insiden keamanan informasi secara keseluruhan.

Seri ISO/IEC 27035 dimaksudkan untuk melengkapi standar dan dokumen lain yang memberikan panduan tentang investigasi atas, dan persiapan untuk menginvestigasi, insiden keamanan informasi. Seri ISO/IEC 27035 bukanlah panduan komprehensif, melainkan sebuah referensi bagi prinsip fundamental tertentu dan sebuah proses terdefinisi yang dimaksudkan untuk memastikan bahwa alat, teknik, dan metode dapat dipilih dengan tepat dan terbukti sesuai dengan tujuan jika diperlukan.

Sementara seri ISO/IEC 27035 meliputi manajemen dari insiden keamanan informasi, seri ini juga mencakup beberapa aspek dari kerentanan keamanan informasi. Panduan untuk pengungkapan kerentanan dan penanganan kerentanan oleh vendor juga disediakan masing-masing dalam ISO/IEC 29147 dan ISO/IEC 30111.

Seri ISO/IEC 27035 juga bertujuan memberi informasi kepada para pengambil keputusan ketika menentukan reliabilitas dari bukti digital yang disajikan kepada mereka. Seri ini dapat diterapkan pada organisasi yang perlu memproteksi, menganalisis dan menyajikan bukti digital potensial. Seri ini relevan bagi badan pembuat kebijakan yang membuat dan mengevaluasi prosedur terkait dengan bukti digital, sering kali sebagai bagian dari Kumpulan bukti yang lebih besar.

Informasi lebih lanjut tentang standar-standar investigatif tersedia di Lampiran A.

Teknologi informasi — Manajemen insiden keamanan informasi — Bagian 1: Prinsip dan proses

1 Ruang lingkup

Dokumen ini adalah fondasi dari seri ISO/IEC 27035. Dokumen ini menyajikan konsep, prinsip dan proses dasar dengan aktivitas utama dari manajemen insiden keamanan informasi, yang menyediakan pendekatan terstruktur untuk mempersiapkan, mendeteksi, melaporkan, menilai, dan merespons kepada insiden, dan menerapkan pembelajaran yang didapat.

Panduan tentang proses manajemen insiden keamanan informasi dan aktivitas utamanya dalam dokumen ini bersifat umum dan dimaksudkan untuk dapat diterapkan pada semua organisasi, terlepas dari tipe, ukuran atau sifatnya. Organisasi dapat menyesuaikan panduan sesuai dengan tipe, ukuran dan sifat bisnisnya sehubungan dengan situasi risiko keamanan informasi. Dokumen ini juga dapat diterapkan kepada organisasi eksternal yang menyediakan layanan manajemen insiden keamanan informasi.

2 Acuan normatif

Dokumen berikut dirujuk dalam teks sedemikian rupa sehingga beberapa atau semua isinya merupakan persyaratan dokumen ini. Untuk acuan tanggal, hanya edisi yang dikutip yang berlaku. Untuk acuan yang tidak bertanggal, berlaku edisi terakhir dari dokumen acuan tersebut (termasuk setiap amendemennya).

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Istilah, definisi dan singkatan

3.1 Istilah singkatan

Untuk tujuan dokumen ini, berlaku istilah dan definisi yang tersedia dalam ISO/IEC 27000 dan istilah-istilah berikut ini 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
tim manajemen insiden (*incident management team*)
IMT

tim yang terdiri dari anggota yang cukup terampil dan tepercaya dari organisasi yang bertanggung jawab untuk memimpin semua aktivitas manajemen insiden keamanan informasi, dalam koordinasi dengan pihak lain baik internal dan eksternal, sepanjang siklus hidup insiden

Catatan 1 untuk entri: Ketua dari tim ini dapat disebut manajer insiden yang ditunjuk oleh manajemen puncak untuk merespons semua tipe insiden secara memadai.

3.1.2
tim tanggap insiden (*incident response team*)
IRT

tim yang terdiri dari anggota yang cukup terampil dan tepercaya dari organisasi yang merespons dan menyelesaikan insiden secara terkoordinasi

Catatan 1 untuk entri: Bisa terdapat beberapa tim, satu untuk setiap aspek insiden.

Catatan 2 untuk entri: Tim Tanggap Darurat Komputer (*Computer Emergency Response Team*/CERT [1]) dan Tim Tanggap Insiden Keamanan Komputer (*Computer Security Incident Response Team*/CSIRT) adalah contoh spesifik dari IRT dalam organisasi dan entitas sektoral, regional, dan nasional yang ingin mengoordinasikan respons mereka ke insiden TIK dan keamanan siber skala besar.

3.1.3
koordinator insiden

orang yang bertanggung jawab memimpin semua aktivitas tanggap insiden (3.1.9) dan mengoordinasikan *tim tanggap insiden* (3.1.2) tersebut

Catatan 1 untuk entri: Suatu organisasi dapat memutuskan menggunakan istilah lain bagi koordinator insiden.

3.1.4
peristiwa keamanan informasi

kejadian yang mengindikasikan kemungkinan pelanggaran keamanan informasi atau kegagalan kontrol

3.1.5
insiden keamanan informasi

peristiwa keamanan informasi (3.1.4) terkait dan teridentifikasi yang dapat membahayakan aset organisasi atau membobol pengoperasiannya

3.1.6
manajemen insiden keamanan informasi

aktivitas kolaborasi untuk menangani *insiden keamanan informasi* (3.1.5) dalam cara yang konsisten dan efektif

3.1.7
investigasi keamanan informasi

penerapan eksaminasi, analisis dan interpretasi untuk membantu pemahaman atas suatu *insiden keamanan informasi* (3.1.5)

[SUMBER: ISO/IEC 27042:2015, 3.10, dimodifikasi — “keamanan informasi” ditambahkan pada istilah dan frasa “suatu insiden: diganti dengan “suatu insiden keamanan informasi” dalam definisi.]

[1] CERT adalah contoh dari suatu produk yang cocok tersedia secara komersial. Informasi ini diberikan demi kenyamanan pengguna dokumen ini dan bukan merupakan suatu dukungan oleh ISO atau IEC terhadap produk ini.

3.1.8
penanganan insiden

tindakan mendeteksi, melaporkan, menilai, merespons, menangani, dan belajar dari *insiden keamanan informasi* (3.1.5)

3.1.9
tanggap insiden

tindakan yang diambil untuk memitigasi atau menyelesaikan suatu *insiden keamanan informasi* (3.1.5), termasuk yang diambil untuk memproteksi dan mengembalikan kondisi operasional normal dari suatu sistem informasi dan informasi yang disimpan di dalamnya

3.1.10
titik kontak (*point of contact*)
PoC

fungsi atau peran organisasional yang ditetapkan sebagai koordinator atau titik fokus informasi perihal aktivitas manajemen insiden

Catatan 1 untuk entri: PoC yang paling jelas adalah peran yang kepada siapa peristiwa keamanan informasi disampaikan.

3.2 Singkatan

BCP	perencanaan kontinuitas bisnis *(business continuity planning*)
CERT	tim tanggap darurat komputer *(computer emergency response team*)
CSIRT	tim tanggap insiden keamanan komputer *(computer security incident response team*)
DRP	perencanaan pemulihan bencana *(disaster recovery planning*)
TIK	teknologi informasi dan komunikasi *(information and communications technology*)
IMT	tim manajemen insiden *(incident management team*)
IRT	tim tanggap insiden *(incident response team*)
SMKI	sistem manajemen keamanan informasi *(information security management system*)
PoC	titik kontak *(point of contact*)
RPO	sasaran titik pemulihan *(recovery point objective*)
RTO	sasaran waktu pemulihan (recovery time objective)

4 Gambaran umum

4.1 Konsep dasar

Peristiwa dan insiden keamanan informasi dapat terjadi karena beberapa alasan:

— kerentanan teknis/teknologi, organisasi atau fisik, sebagian karena implementasi yang

tidak lengkap atas kontrol yang sudah diputuskan, besar kemungkinan untuk dieksploitasi, sebab penghapusan eksposur atau risiko sepenuhnya tidak mungkin terjadi;

— manusia dapat melakukan kesalahan;

— teknologi bisa gagal;

— asesmen risiko tidak lengkap dan risikonya diabaikan;

— perlakuan risiko tidak mencakup risiko secara memadai;

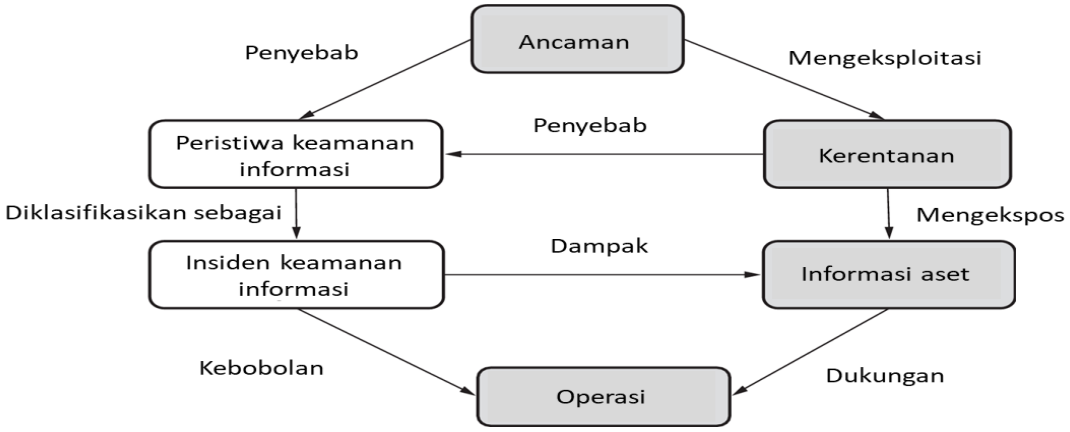
— perubahan di dalam konteks (internal dan/atau eksternal) sehingga muncul risiko baru atau risiko yang telah diperlakukan sudah tidak lagi tercakup secara memadai.

Terjadinya peristiwa keamanan informasi belum tentu berarti sebuah serangan telah berhasil atau bahwa terdapat implikasi pada konfidensialitas, integritas atau availabilitas, dengan kata lain tidak semua peristiwa keamanan informasi diklasifikasikan sebagai insiden keamanan informasi.

Insiden keamanan informasi bisa disengaja (misalnya disebabkan oleh perangkat lunak perusak (*malware*) atau pelanggaran disiplin), tidak disengaja (misalnya disebabkan oleh kesalahan manusia yang tidak disengaja) atau lingkungan (misalnya disebabkan oleh kebakaran atau banjir) dan dapat disebabkan oleh sarana teknis (misalnya virus komputer) atau nonteknis (misalnya kehilangan atau pencurian dokumen salinan cetak). Insiden dapat termasuk pengungkapan yang tidak sah, modifikasi, penghancuran, atau ketidaktersediaan informasi, atau kerusakan atau pencurian aset organisasi yang berisi informasi.

Lampiran B menyediakan deskripsi contoh terpilih dari insiden keamanan informasi dan penyebabnya untuk tujuan informatif saja. Penting untuk dicatat bahwa contoh-contoh ini tidaklah lengkap.

Suatu ancaman mengeksploitasi kerentanan (kelemahan) dalam sistem, layanan, atau jaringan informasi, menyebabkan terjadinya peristiwa keamanan informasi dan dengan demikian berpotensi menyebabkan insiden pada asset yang sudah terekspos kerentanan. Gambar 1 menunjukkan hubungan objek dalam insiden keamanan informasi.



CATATAN Objek berbayang adalah yang sudah ada sebelumnya, terdampak oleh objek takberbayang sehingga mengakibatkan suatu insiden keamanan informasi.

Gambar 1 — Hubungan objek dalam insiden keamanan informasi

Koordinasi merupakan aspek penting dalam manajemen insiden keamanan informasi. Banyak insiden lintas organisasi dan tidak bisa dengan mudah diselesaikan oleh satu organisasi atau, satu bagian dari organisasi di mana insiden terdeteksi. Organisasi sebaiknya berkomitmen kepada seluruh sasaran manajemen insiden. Koordinasi manajemen insiden diperlukan di sepanjang proses manajemen insiden bagi banyak organisasi bekerja sama dalam menangani insiden keamanan informasi. Ini sebagai contoh peran dari CERT dan CSIRT. Berbagi informasi diperlukan untuk koordinasi manajemen insiden, di mana organisasi yang berbeda berbagi informasi ancaman, serangan, dan kerentanan satu sama lain sehingga pengetahuan masing-masing organisasi bermanfaat bagi yang lain. Organisasi sebaiknya memproteksi informasi sensitif pada saat berbagi informasi dan berkomunikasi. Lihat ISO/IEC 27010 untuk detail lebih lanjut.

Hal ini penting untuk menunjukkan bahwa menyelesaikan insiden keamanan informasi sebaiknya dilakukan dalam jangka waktu yang telah ditentukan untuk menghindari kerusakan yang tidak dapat diterima atau yang mengakibatkan bencana yang hebat dan mendadak (*catastrophe*). Penundaan penyelesaian ini tidaklah sebegitu penting dalam hal terjadi peristiwa, kerentanan atau ketidaksesuaian.

4.2 Sasaran manajemen insiden

Sebagai bagian utama dari seluruh strategi keamanan informasi organisasi, organisasi sebaiknya menaruh kontrol termasuk prosedur yang ada untuk memungkinkan pendekatan terstruktur yang terencana terhadap manajemen insiden keamanan informasi. Dari perspektif organisasi, sasaran utama ialah menghindari atau membendung dampak dari insiden keamanan informasi untuk meminimalkan kerusakan langsung dan tidak langsung terhadap pengoperasian akibat insiden. Karena kerusakan pada aset informasi dapat memiliki konsekuensi negatif pada operasinya, perspektif bisnis dan operasional sebaiknya memiliki pengaruh besar dalam menentukan sasaran yang lebih spesifik untuk manajemen insiden keamanan informasi.

Sasaran yang lebih spesifik dari pendekatan terstruktur yang terencana terhadap manajemen insiden sebaiknya termasuk yang berikut ini:

a) peristiwa keamanan informasi dideteksi dan ditangani dengan efisien, secara khusus dalam memutuskan apakah sebaiknya diklasifikasikan sebagai insiden keamanan informasi;

b) insiden keamanan informasi yang teridentifikasi dinilai dan ditanggapi dengan cara yang paling tepat dan efisien dan dalam jangka waktu yang telah ditentukan;

c) dampak kerugian dari insiden keamanan informasi pada organisasi dan pihak-pihak yang terlibat dan operasinya diminimalkan dengan kontrol yang tepat sebagai bagian dari tanggap insiden;

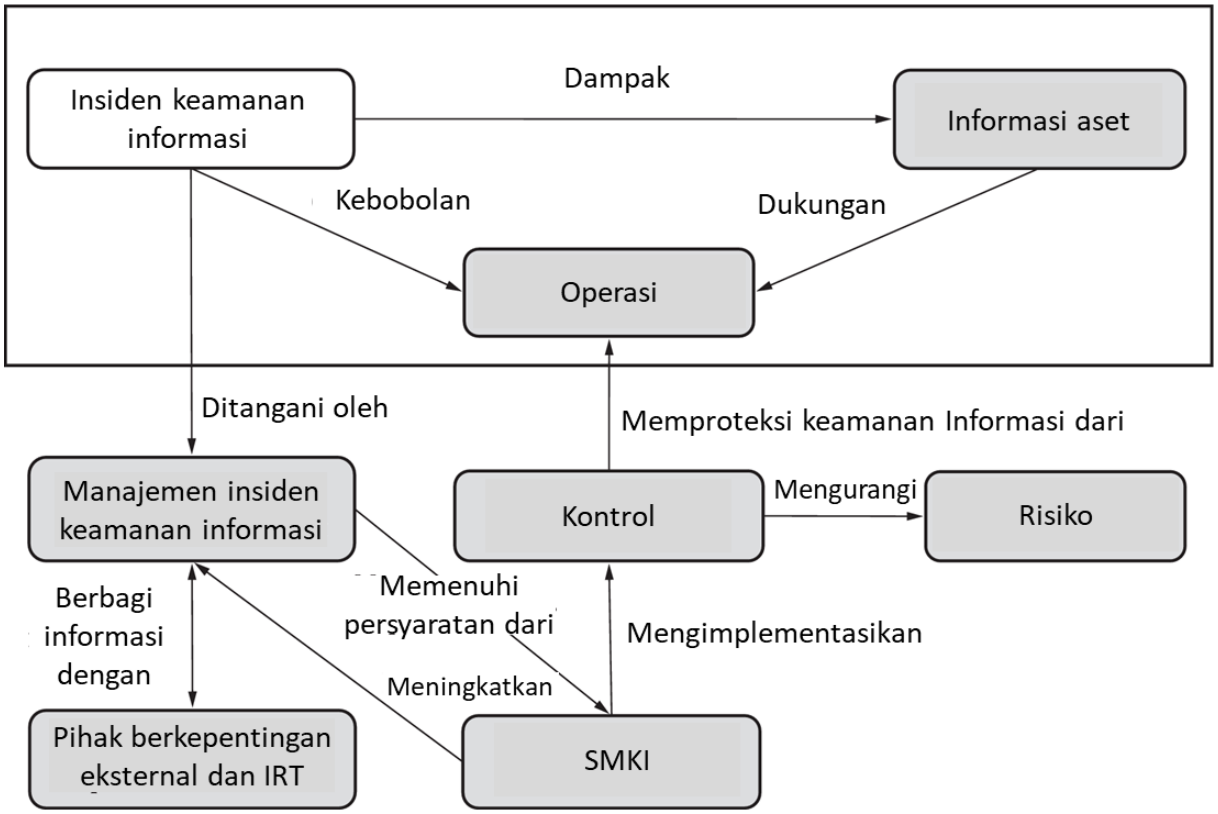
d) sebuah tautan dengan elemen yang relevan dari manajemen krisis dan manajemen kontinuitas bisnis melalui proses eskalasi yang telah ditetapkan. Diperlukan suatu transfer tanggung jawab dan tindakan yang cepat dari manajemen insiden kepada manajemen krisis ketika situasi membutuhkan, serta urutan ini dibalik setelah krisis teratasi untuk memungkinkan penyelesaian insiden secara menyeluruh;

e) kerentanan keamanan informasi yang termasuk dalam atau ditemukan saat insiden agar dinilai dan ditangani dengan tepat untuk mencegah atau mengurangi insiden. Asesmen ini dapat dilakukan baik oleh tim tanggap insiden (IRT) atau tim lain dalam organisasi dan pihak yang terlibat, tergantung dari distribusi tugas;

f) Pelajaran yang didapat dipelajari dengan cepat dari insiden keamanan informasi, kerentanan yang terkait dan manajemennya. Mekanisme umpan balik ini dimaksudkan untuk menaikkan peluang mencegah terjadinya insiden keamanan informasi di masa depan, meningkatkan implementasi dan penggunaan kontrol keamanan informasi, dan meningkatkan rencana manajemen insiden keamanan informasi secara keseluruhan.

Untuk membantu mencapai sasaran tersebut, organisasi sebaiknya memastikan insiden keamanan informasi didokumentasikan secara konsisten, menggunakan standar atau prosedur yang tepat untuk kategorisasi insiden, klasifikasi, prioritisasi dan berbagi informasi, sehingga diperoleh metrik dari data agregat selama periode waktu tertentu. Ini menyediakan informasi berharga untuk membantu proses pengambilan keputusan strategis ketika berinvestasi dalam kontrol keamanan informasi. Sistem manajemen insiden keamanan informasi sebaiknya dapat membagikan informasi dengan pihak internal dan eksternal yang terkait.

Sasaran lainnya yang terasosiasi dengan dokumen ini yaitu untuk menyediakan panduan bagi organisasi yang bermaksud memenuhi persyaratan sistem manajemen keamanan informasi (SMKI) yang dispesifikasikan dalam ISO/IEC 27001 yang didukung dengan panduan dari ISO/IEC 27002. ISO/IEC 27001 mencakup persyaratan yang terkait manajemen insiden keamanan informasi. Tabel C.1 menyediakan referensi silang tentang pasal-pasal manajemen insiden keamanan informasi dari ISO/IEC 27001 dan pasal-pasal dalam dokumen ini. Hubungan SMKI juga dijelaskan dalam Gambar 2. Dokumen ini juga dapat mendukung persyaratan dari sistem manajemen keamanan informasi yang tidak mengikuti ISO/IEC 27001.



CATATAN Lihat juga Gambar 1.

Gambar 2 — Manajemen insiden keamanan informasi dalam hubungannya dengan SMKI dan kontrol yang diterapkan

4.3 Manfaat dari pendekatan terstruktur

Menggunakan pendekatan terstruktur pada manajemen insiden keamanan informasi dapat menghasilkan manfaat yang signifikan, yang dapat dikelompokkan dalam topik berikut.

a) Meningkatkan keamanan informasi secara keseluruhan

Untuk memastikan identifikasi yang memadai dan tanggapan kepada peristiwa dan insiden keamanan informasi, merupakan suatu prasyarat untuk adanya proses terstruktur atas perencanaan dan persiapan, deteksi, pelaporan dan asesmen, dan pengambilan keputusan yang relevan. Hal ini meningkatkan keamanan secara menyeluruh dengan membantu untuk mengidentifikasikan dan mengimplementasikan solusi yang konsisten dengan cepat, dan dengan demikian menyediakan cara untuk mencegah insiden keamanan informasi serupa di masa depan. Selain itu, manfaat juga didapatkan melalui metrik, pembagian dan agregasi. Kredibilitas organisasi dapat ditingkatkan melalui demonstrasi implementasi praktik terbaiknya yang terkait dengan manajemen insiden keamanan informasi.

b) Mengurangi konsekuensi bisnis yang merugikan

Pendekatan terstruktur pada manajemen insiden keamanan informasi dapat membantu mengurangi level potensi konsekuensi bisnis yang merugikan yang terasosiasi dengan insiden keamanan informasi. Konsekuensi ini dapat termasuk kerugian finansial langsung dan kerugian jangka panjang yang timbul dari reputasi dan kredibilitas yang rusak. Untuk panduan lebih lanjut terkait asesmen konsekuensi, lihat ISO/IEC 27005. Untuk panduan pada kesiapan teknologi informasi dan komunikasi untuk kontinuitas bisnis, lihat ISO/IEC 27031.

c) Memperkuat fokus pada pencegahan insiden keamanan informasi

Menggunakan pendekatan terstruktur pada manajemen insiden keamanan informasi membantu untuk membuat fokus yang lebih baik pada pencegahan insiden dalam organisasi, termasuk pengembangan metode untuk mengidentifikasi ancaman dan kerentanan baru. Analisis data terkait insiden memungkinkan identifikasi dari pola dan tren, sehingga memfasilitasi fokus yang lebih akurat pada pencegahan insiden dan identifikasi tindakan dan kontrol yang tepat untuk mencegah kejadian lebih lanjut.

d) Meningkatkan prioritisasi

Pendekatan terstruktur pada manajemen insiden keamanan informasi menyediakan basis yang solid untuk prioritisasi ketika melakukan investigasi insiden keamanan informasi, termasuk penggunaan skala kategorisasi dan klasifikasi yang efektif. Jika tidak ada prosedur yang jelas, maka ada risiko aktivitas investigasi mungkin dilakukan dalam mode yang terlalu reaktif, menanggapi insiden ketika terjadi dan mengabaikan aktivitas yang sebaiknya ditangani dengan prioritas yang lebih tinggi.

e) Mendukung pengumpulan bukti dan investigasi

Jika dan ketika diperlukan, prosedur investigasi insiden yang jelas membantu untuk memastikan bahwa pengumpulan data dan penanganan terbukti sah dan dapat diterima secara hukum. Ini adalah pertimbangan penting jika diikuti penuntutan hukum atau tindakan disipliner. Untuk informasi lebih lanjut pada bukti digital dan investigasi, lihat standar investigatif dalam Lampiran A.

f) Berkontribusi pada justifikasi anggaran dan sumber daya

Pendekatan yang terdefinisi dengan baik dan terstruktur pada manajemen insiden keamanan

informasi membantu untuk menjustifikasi dan menyederhanakan alokasi anggaran dan sumber daya bagi unit organisasional yang terlibat. Selain itu, manfaat diperoleh untuk rencana manajemen insiden keamanan informasi itu sendiri, dengan kemampuan untuk merencanakan yang lebih baik bagi alokasi staf dan sumber daya.

Satu contoh cara untuk mengontrol dan mengoptimalkan anggaran dan sumber daya adalah dengan menambah penelusuran waktu pada tugas manajemen insiden keamanan informasi untuk memfasilitasi asesmen kuantitatif dari penanganan organisasi terhadap insiden keamanan informasi. Hal ini dapat menyediakan informasi tentang berapa lama waktu yang dibutuhkan untuk mengatasi insiden keamanan informasi dari prioritas yang berbeda dan pada platform yang berbeda. Jika terdapat kemacetan dalam proses manajemen insiden keamanan informasi, hal ini sebaiknya juga dapat teridentifikasi.

g) Meningkatkan pembaruan pada asesmen risiko keamanan informasi dan hasil perlakuan

Penggunaan pendekatan terstruktur pada manajemen insiden keamanan informasi memfasilitasi:

— pengumpulan data yang lebih baik untuk membantu identifikasi dan penentuan karakteristik dari berbagai tipe ancaman dan kerentanan yang terasosiasi, dan

— penyediaan data mengenai frekuensi kejadian dari tipe-tipe ancaman yang teridentifikasi, membantu dengan analisis efikasi kontrol (misalnya mengidentifikasi kontrol yang gagal dan berakibat pada pelanggaran, dengan peningkatan kontrol tersebut untuk mengurangi keberulangan).

Data yang dikumpulkan tentang dampak yang merugikan pada operasi bisnis dari insiden keamanan informasi berguna untuk analisis dampak bisnis. Data yang dikumpulkan untuk mengidentifikasi frekuensi dari berbagai tipe ancaman dapat meningkatkan kualitas asesmen ancaman. Sama halnya, pengumpulan data pada kerentanan dapat meningkatkan kualitas asesmen kerentanan di masa mendatang. Untuk panduan pada asesmen dan perlakuan risiko keamanan informasi, lihat ISO/IEC 27005.

h) Menyediakan peningkatan materi program kesadaran dan pelatihan keamanan informasi

Suatu pendekatan terstruktur terhadap manajemen insiden keamanan informasi memampukan organisasi mengumpulkan pengalaman dan pengetahuan tentang bagaimana organisasi dan pihak yang terlibat menangani insiden, yang merupakan material yang berharga bagi suatu program kesadaran keamanan informasi. Program kesadaran yang mencakup pembelajaran pelajaran yang didapat dari pengalaman nyata akan menolong untuk mengurangi kesalahan atau kebingungan dalam penanganan insiden keamanan informasi di masa depan dan meningkatkan potensi waktu respons dan kesadaran umum tentang kewajiban pelaporan.

i) Menyediakan input kepada reviu kebijakan keamanan informasi dan dokumentasi terkait

Data yang disediakan melalui praktik pendekatan terstruktur kepada manajemen insiden keamanan informasi dapat menawarkan input yang berharga bagi reviu efektivitas dan peningkatan lanjutan dari kebijakan manajemen insiden (dan dokumen keamanan informasi lain yang terkait). Ini berlaku pada kebijakan dengan topik spesifik dan dokumen lainnya yang berlaku bagi organisasi secara keseluruhan dan bagi sistem, layanan dan jaringan secara individu.

4.4 Adaptabilitas

Panduan yang disediakan oleh seri ISO/IEC 27035 ini ekstensif dan, jika diadopsi sepenuhnya, dapat memerlukan sumber daya yang signifikan untuk operasi dan pengelolaan. Oleh karena itu penting bahwa organisasi yang menerapkan panduan ini sebaiknya tetap mempertahankan suatu rasa perspektif dan memastikan sumber daya yang digunakan untuk manajemen insiden keamanan informasi dan kompleksitas mekanisme yang diimplementasikan adalah sebanding dengan ha; berikut:

a) ukuran, struktur, dan sifat bisnis dari organisasi termasuk aset, proses, dan data penting utama yang sebaiknya dilindungi;

b) ruang lingkup dari sistem manajemen keamanan informasi mana pun untuk penanganan insiden;

c) potensi risiko akibat insiden;

d) tujuan bisnis.

Oleh karena itu, organisasi yang menggunakan dokumen ini sebaiknya mengadopsi panduan dengan cara yang relevan dengan skala dan karakteristik bisnisnya.

4.5 Kapabilitas

4.5.1 Umum

Insiden keamanan informasi dapat membahayakan pencapaian dari sasaran bisnis dan menghasilkan krisis. Mengikuti asesmen risiko, dimungkinkan untuk menggambarkan situasi yang kemungkinannya sedang sampai tinggi, dan konsekuensinya rendah sampai sedang, dan yang kemungkinannya (sangat) jarang dan konsekuensinya sangat tinggi. Situasi kedua mewakili krisis yang tidak selalu mungkin untuk dicegah sepenuhnya dan, dalam sejumlah kasus, mengganggu rantai pengambilan keputusan. ISO/IEC 27031 menyediakan panduan atas kesiapan teknologi informasi dan komunikasi (TIK) bagi kontinuitas bisnis untuk mendukung operasi bisnis dalam hal terjadi peristiwa dan insiden keamanan informasi, dan disrupsi terkait.

Sasaran menyeluruh dari manajemen krisis adalah:

— memproteksi kehidupan manusia termasuk infrastruktur vital sejauh yang diperlukan;

— mendukung kontinuitas aktivitas sehari-hari;

— memproteksi aset termasuk properti dan lingkungan alam, sejauh mungkin.

Tidak ada dua krisis yang sama. Sasaran ini didasari oleh prinsip berikut:

— Koordinasi: koordinasi dan komunikasi yang efektif yang memfasilitasi pembagian informasi.

— Kontinuitas: pencegahan, kesiapsiagaan, respons dan pemulihan krisis sebaiknya didasarkan dalam fungsi-fungsi organisasi yang ada dan cara-cara kerja yang lazim.

— Proporsionalitas: manajemen krisis sebaiknya dikalibrasi terhadap besaran dan sifat dari krisis.

— Akuntabilitas: pengambilan keputusan dan tindakan transparan dan akuntabel.

— Integrasi: pencegahan, kesiapsiagaan, respon dan pemulihan sebaiknya dipertimbangkan sebagai elemen dari sebuah kontinum yang mungkin terjadi secara bersamaan.

Manajemen insiden keamanan informasi memerlukan kapabilitas untuk memastikan koherensi manajemen untuk mencapai penanganan insiden yang efektif dan efisien. Kapabilitas ini sebaiknya ditetapkan melalui kebijakan, rencana, proses dan prosedur manajemen insiden, beserta pula tim yang terstruktur dengan baik, orang-orang yang terampil, berbagi informasi dan koordinasi dengan pihak-pihak lain baik internal dan eksternal.

4.5.2 Kebijakan, rencana dan proses

Kebijakan organisasi untuk manajemen keamanan informasi sebaiknya mempertimbangkan bagaimana manajemen insiden keamanan informasi sejalan dengan manajemen risiko. Untuk mencapai hal tersebut, organisasi sebaiknya mengidentifikasi, sebagai bagian dari proses manajemen risiko, daftar peristiwa/insiden yang ingin dikonter dan dikontrol, dengan memastikan dampak seminimal mungkin pada sasaran dan operasi bisnis.

Manajemen insiden memerlukan sebuah proses yang telah ditentukan yang telah disetujui oleh manajemen puncak termasuk alur tindakan (atau prosedur) yang akan dilakukan di semua fase proses dan sebuah protokol komunikasi dengan kanal yang tepat.

4.5.3 Struktur manajemen insiden

Untuk memungkinkan respon yang koheren terhadap peristiwa dan insiden, organisasi sebaiknya melembagakan suatu kapabilitas manajemen insiden yang menyiapkan kebijakan manajemen insiden keamanan informasi dan menjelaskan struktur respon insidennya. Organisasi sebaiknya juga memastikan bahwa arahan dan sumber daya tersedia untuk merespon insiden dengan memadai.

a) Tim manajemen insiden

Suatu tim manajemen insiden (*incident management team*-IMT) terdiri dari anggota yang cukup terampil dan tepercaya dari organisasi dengan peran memimpin semua aktivitas manajemen insiden keamanan informasi, berkoordinasi dengan pihak lain, baik internal dan eksternal, sepanjang siklus hidup insiden. IMT menyediakan semua layanan yang diperlukan untuk mengatasi insiden, tidak hanya mempersiapkan untuk, mendeteksi, melaporkan, menilai, dan merespon insiden, tetapi juga deteksi, advisori, berbagi informasi, pelajaran pembelajaran, peningkatan, pendidikan dan kesadaran ancaman dan kerentanan. TMI dapat mengintroduksi kapan saja sumber daya apa pun yang diperlukan untuk menyediakan layanan-layanan ini.

Organisasi sebaiknya menentukan dan mengalokasikan peran dan tanggung jawab untuk menangani, berkoordinasi dan merespons insiden. Ini termasuk:

b) Titik kontak (*point of contact*-PoC)

Titik kontak (PoC) adalah peran, alamat, atau orang yang dapat dihubungi oleh personel ketika mereka menemukan anomali dan apa yang dipertimbangkan sebagai suatu peristiwa dalam kebijakan dan sesi kesadaran. Tergantung pada sifat dan ukuran organisasi, mungkin saja memiliki lebih dari satu PoC. Sebagai contoh, satu untuk isu TIK dan satu untuk situasi fisik, organisasional dan prosedural, yang serupa dengan yang sudah ada untuk kecelakaan, kebakaran dan peralatan rusak lainnya.

c) Koordinator insiden yang:

— mengoordinasikan dan mengelola notifikasi dan peringatan peristiwa yang dimunculkan dari sistem informasi atau individual,

— melakukan evaluasi atas peristiwa dan menyatakan insiden,

— mengaktifkan IRT dan mengoordinasikan aktivitasnya,

— merekam semua informasi insiden dan penyelesaiannya,

— menyelesaikan dan mengirim laporan insiden, bersama proposal untuk peningkatan,

— mengoordinasikan dengan organisasi internal dan eksternal mengikuti arahan IMT terhadap penanganan insiden.

CATATAN Organisasi dapat memutuskan untuk menggunakan istilah lain bagi koordinator insiden.

Koordinator insiden yang dialokasikan sebaiknya memelihara kontrol untuk seluruh durasi insiden. Di mana insiden melampaui sesi jam kerja dan memerlukan seseorang tetap tinggal/tersedia, coordinator insiden yang lain sebaiknya mengambil alih semua informasi dan otoritas yang diperlukan.

Jika diperlukan panggilan kepada koordinator atau tim BCP (*business continuity planning*/perencanaan kontinuitas bisnis)/DRP (*disaster recovery planning*/perencanaan pemulihan bencana), koordinator insiden sebaiknya tetap terinformasi, dan melanjutkan pengelolaan insiden setelah krisis terselesaikan, untuk menyelesaikan penyelesaian.

d) Tim tanggap insiden (IRT) yang:

— melakukan “prosedur” untuk merespons insiden,

— mendeteksi akar penyebab dan kerentanan tersembunyi,

— menyelesaikan insiden,

— melaporkan kepada koordinator insiden.

e) Tim manajemen perubahan yang memutuskan tindakan yang harus diambil untuk meningkatkan pencegahan dan respon insiden.

f) Tim kesadaran dan pelatihan yang menyiapkan program dan sesi yang dimaksudkan untuk mengidentifikasi dan melaporkan peristiwa-peristiwa yang tidak diinginkan.

g) Tim manajemen kerentanan yang menganalisis kerentanan yang terdeteksi selama respon insiden dan menyediakan rekomendasi untuk tim manajemen perubahan.

h) Tim manajemen krisis yang memastikan koordinasi dengan koordinator BCP/DRP atau tim.

i) Tim monitoring keamanan yang memperbarui aturan sistem monitoring dan deteksi dalam implementasi keputusan yang sesuai dari pembelajaran yang telah dipelajari, dan memonitor keberulangan dari insiden serupa.

4.6 Komunikasi

Organisasi sebaiknya mengkomunikasikan kebijakan manajemen insiden keamanan informasi yang telah disetujui kepada pihak yang berkepentingan. Ini termasuk staf internal dan pihak eksternal yang memiliki akses ke informasi organisasi. Organisasi sebaiknya mengomunikasikan hal-hal berikut:

— kebijakan insiden keamanan informasi organisasi dan prosedur yang relevan;

— kewajiban/ekspektasi personel;

— prosedur pelaporan insiden;

— siapa yang harus dihubungi untuk informasi lebih lanjut;

— akibat dari insiden dan bagaimana meminimalkan keberulangan.

Organisasi sebaiknya mempromosikan manajemen insiden sebagai suatu proses pelaporan “bukan kesalahan” untuk memperkuat personel untuk maju dan melaporkan insiden tanpa takut sanksi. Sebaiknya fokus dialihkan pada hasil positif yang dapat diperoleh organisasi dari menerima laporan insiden, mempelajari dan melakukan peningkatan dari insiden untuk menjadi lebih aman dan tangguh.

Pelaporan insiden pada awalnya tentu “bukan kesalahan” misalnya tidak akan ada kesalahan atau hal mempersalahkan yang diasosiasikan dengan pelaporan insiden. Setelah investigasi, sanksi dapat diberikan jika ditemukan insiden itu merupakan akibat dari pelanggaran kebijakan atau prosedur organisasi yang disengaja, atau sudah dalam ranah kesalahan atau kelalaian yang berulang-ulang.

Komunikasi adalah hal yang esensial untuk mengontrol pesan seputar insiden termasuk di mana, kapan, apa dan bagaimana pesan disampaikan, baik untuk menyediakan respons yang tepat dan untuk memenuhi kebutuhan organisasi atau sosial. Komunikasi internal penting untuk respons dan pemulihan yang efektif, dan komunikasi eksternal sangat diperlukan misalnya untuk citra perusahaan.

CATATAN Sebuah pelanggaran informasi (alias komunikasi takterkendali) mengenai suatu insiden dapat menimbulkan konsekuensi serius.

Hanya personel yang diberi mandat dan dipersiapkan sebaiknya diperbolehkan untuk berkomunikasi dengan dunia eksternal untuk memberitahukan hal-hal yang diperlukan saja, pada momen terbaik dan dalam bentuk yang tepat.

4.7 Dokumentasi

4.7.1 Umum

Penting untuk mendokumentasikan sebanyak mungkin informasi terkait dengan peristiwa/insiden mulai dari deteksi sampai penyelesaiannya. Laporan insiden adalah sintesis dari semua informasi ini.

4.7.2 Laporan peristiwa

Laporan peristiwa sebaiknya berisi semua hal yang diperlukan untuk memahami peristiwa tersebut dan membuat keputusan mengenai apakah peristiwa diklasifikasikan sebagai insiden. Ini termasuk:

a) tanggal dan waktu deteksi;

b) nama informan, namun bisa disembunyikan untuk menjaga konfidensialitas;

c) semua keadaan dan fakta yang ada untuk pemahaman terhadap peristiwa tersebut.

4.7.3 Log manajemen insiden

Semua informasi yang dikumpulkan selama respons insiden sebaiknya didokumentasikan/direkam/dicatat untuk dijadikan sebagai catatan tindakan misalnya tanggal/waktu dan tindakan/keputusan terkait.

4.7.4 Laporan insiden

Laporan insiden adalah sintesis dari semua informasi yang dikumpulkan sepanjang siklus hidup insiden. Itu berfungsi untuk menganalisis dan mengevaluasi insiden, dan memutuskan jika perubahan direncanakan untuk kapabilitas manajemen insiden (lihat juga 4.5).

Dokumen templat yang sudah diformat sebelumnya untuk laporan insiden sebaiknya dipersiapkan untuk memastikan tidak ada informasi esensial yang terlewat atau diabaikan.

4.7.5 Register insiden

Semua insiden keamanan informasi sebaiknya direkam dalam daftar insiden yang dikelola secara terpusat. Daftar ini menyediakan IMT dengan gambaran umum dari insiden yang pernah muncul di organisasi, statusnya, dan semua kegiatan tindak lanjutnya. Ini juga bisa digunakan IMT untuk menyediakan laporan kepada manajemen puncak mengenai tren dan tema seputar lingkungan ancaman dan memberi masukan pada perencanaan organisasi dan asesmen risiko.

5 Proses

5.1 Gambaran Umum

Untuk mencapai sasaran yang diuraikan di 4.2, proses manajemen insiden keamanan informasi terdiri dari lima fase yang berbeda:

— perencanaan dan persiapan (lihat 5.2);

— deteksi dan pelaporan (lihat 5.3);

— asesmen dan pengambilan keputusan (lihat 5.4);

— respons (lihat 5.5);

— pembelajaran (lihat 5.6).

Gambaran level tinggi fase ini ditunjukkan dalam Gambar 3.

Beberapa aktivitas dapat muncul dalam banyak fase atau sepanjang proses penanganan insiden. Aktivitas tersebut dapat termasuk hal-hal berikut:

— bukti dokumentasi peristiwa dan insiden dan informasi kunci, tindakan respons yang

diambil, dan tindak lanjut yang telah dilakukan sebagai bagian dari proses penanganan insiden;
— koordinasi dan komunikasi antarpihak yang terlibat;

— notifikasi atas insiden signifikan kepada manajemen dan pihak berkepentingan lainnya;

— berbagi informasi antarpihak berkepentingan dan kolaborator internal dan eksternal seperti vendor dan IRT lainnya.

Pertimbangan waktu bagi setiap langkah dalam proses manajemen peristiwa/insiden sebaiknya:

a) Deteksi: secepat mungkin

b) Pelaporan: melengkapi formulir yang diperlukan tanpa penundaan yang tidak perlu, atau melalui metode-metode otomatis.

c) Respons: secepat mungkin memulai respons sebelum kerusakan (dampak dan konsekuensi) melewati batas yang ditentukan organisasi untuk menghindari situasi yang memerlukan pengambilan tindakan sesuai BCP/DRP. Batas yang dapat diterima sebaiknya terdefinisi dengan baik di BCP dan diketahui semua orang. Setiap tipe insiden mungkin memiliki jalur atau cara penyelesaian yang berbeda.

d) Komunikasi

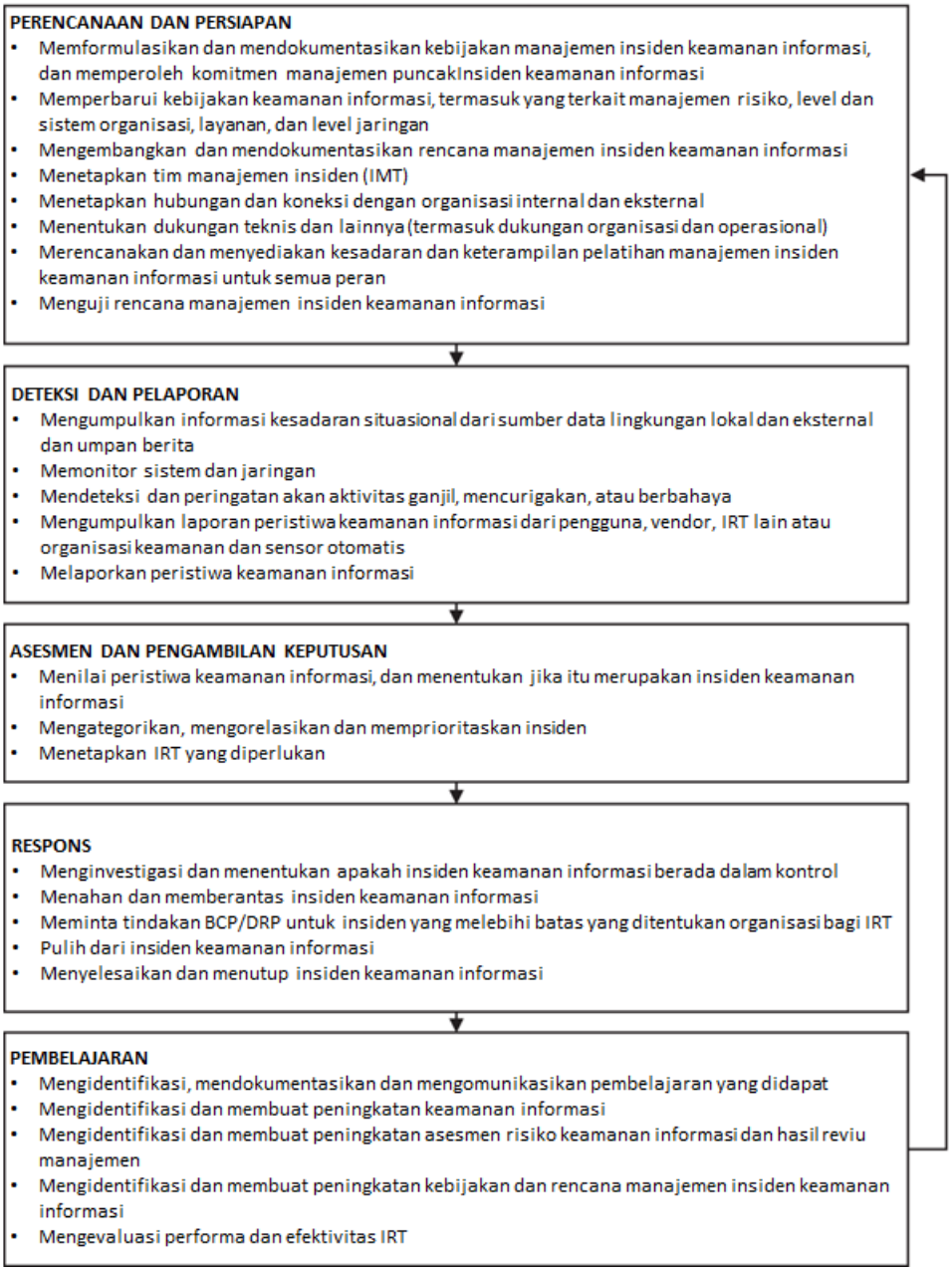
   — Internal: mengadopsi, secepat mungkin, tindakan dan perilaku dan mencegah perpanjangan insiden

   — Eksternal: menerima, secepat mungkin, pertolongan yang diperlukan dari pihak eksternal terkait untuk melakukan intervensi, dan memberi tahu para pihak yang berkepentingan

e) Eskalasi: dalam interval yang ditentukan organisasi dan/atau sebelum dampaknya melewati batas yang ditentukan organisasi

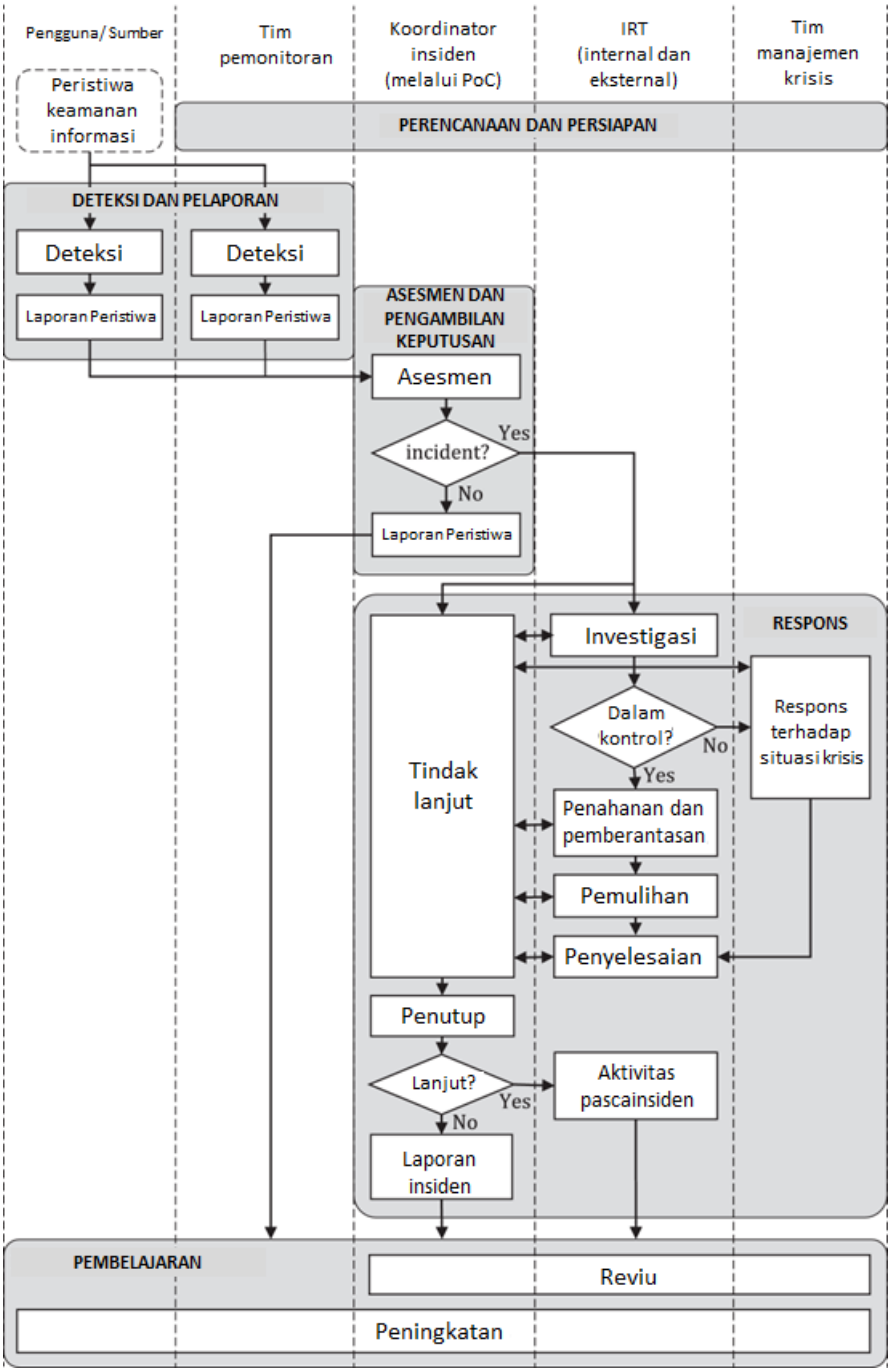
f) Notifikasi: dalam interval yang ditentukan organisasi atau interval apa pun yang diwajibkan secara hukum.

Semua tindakan sebaiknya dilakukan dan dimonitor tanpa penundaan yang tidak perlu.



Gambar 3 — Fase manajemen insiden keamanan informasi

Gambar 4 menunjukkan alur peristiwa dan insiden keamanan informasi melalui fase manajemen insiden keamanan informasi dan aktivitas terkait.



Gambar 4 — Diagram alir peristiwa dan insiden keamanan informasi

5.2 Perencanaan dan persiapan

Manajemen insiden keamanan informasi yang efektif memerlukan perencanaan dan persiapan yang tepat. Hal yang esensial untuk tetap tenang di semua tahapan respons insiden, dan bahwa waktu respons dikontrol dan dikuasai. Jika tidak, durasi insiden yang semakin panjang dapat meningkatkan dampak kerugian pada organisasi. Waktu respons ini sebaiknya dikomputasikan sebagai bagian dari sasaran waktu pemulihan (recovery time objective/RTO, lihat ISO/IEC 27031:2011, 3.13 dan 6.3) dan sebaiknya memperhitungkan rentang waktu yang diperlukan untuk deteksi, pelaporan dan asesmen.

Agar rencana manajemen insiden keamanan informasi yang efektif dan efisien dapat dijalankan, organisasi sebaiknya melengkapi sejumlah aktivitas persiapan dalam mendukung persyaratan manajemen insiden dari SMKI, yaitu:

a) merumuskan dan mendokumentasikan kebijakan manajemen insiden keamanan informasi dan memperoleh komitmen dari manajemen puncak, termasuk tujuan, sasaran dan ruang lingkup kebijakan, kategori dan kriteria untuk menentukan dan memprioritaskan insiden, struktur organisasi dan pengaturan peran, tanggung jawab dan otoritas untuk manajemen insiden, pengukuran performa, pelaporan dan daftar kontak;

b) memperbarui kebijakan keamanan informasi, termasuk yang terkait dengan manajemen risiko, baik pada level organisasi dan level sistem, layanan atau jaringan;

c) mengembangkan dan mendokumentasikan detail rencana manajemen insiden keamanan informasi, termasuk prosedur dan metode untuk penanganan insiden, komunikasi dan berbagi informasi, yang digunakan untuk menetapkan kapabilitas manajemen insiden. Organisasi sebaiknya

   — mendefinisikan indikator dan prekursor peristiwa/insiden keamanan informasi;

   — membuat daftar kemungkinan peristiwa/insiden yang organisasi inginkan untuk dapat dikontrol. Daftar ini terutama berdasarkan hasil dari asesmen risiko. Suatu peristiwa/insiden adalah risiko yang menjadi nyata;

   — merumuskan format dan isi dari laporan insiden. Ini memungkinkan pelaporan yang konsisten terlepas dari individu yang mengisi formulir dan penting untuk mendapat pembelajaran serta penentuan tema dan tren umum untuk pelaporan sampai manajemen;

   — mendefinisikan/menetapkan kategori insiden;

   — menetapkan prosedur penyerahan untuk diserahkan kepada penegak hukum ketika insiden administratif (misalnya pelanggaran kebijakan) menjadi insiden kriminal (misalnya *fraud*);

   — mendokumentasikan prosedur evaluasi untuk menyatakan suatu insiden;

   — menentukan pertukaran informasi dan tanggung jawab dengan tim manajemen krisis (BCP/DRP) dalam kedua arah;

   — menetapkan tim manajemen insiden yang mengumpulkan semua keterampilan yang dibutuhkan untuk menyiapkan rencana respons insiden;

   — menetapkan struktur keputusan/perintah dan bagan panggilan darurat (*emergency call tree*);

   — menyediakan poin kontak esensial internal dan eksternal (misalnya kontak legal);

   — menyiapkan tim tanggap insiden (IRT) yang berperan merespons dan menyelesaikan insiden. Terdapat sejumlah IRT dengan keterampilan-keterampilan yang spesifik untuk merespons insiden tertentu. Informasi lebih lanjut dapat ditemukan dalam ISO/IEC 27035-2:2023, 7.3.

d) menentukan IRT, dengan fungsi dan layanannya, dan merancang, mengembangkan, dan menyediakan suatu program pelatihan yang tepat untuk personelnya. Tim respons

sebaiknya mengetahui apa yang harus dilakukan, sumber daya apa yang digunakan dan dalam kerangka waktu yang digunakan. Merupakan hal yang esensial untuk personel dilatih bekerja dengan efisien dan berkemampuan bekerja di bawah tekanan.

e) menetapkan dan menjaga hubungan dan koneksi yang tepat dengan organisasi internal dan eksternal yang terlibat secara langsung dalam manajemen peristiwa, insiden, ancaman dan kerentanan keamanan informasi, dan mengomunikasikan kebijakan manajemen insiden keamanan informasi kepada mereka;

f) menetapkan, mengimplementasikan dan mengoperasikan mekanisme teknis, organisasional dan operasional untuk mendukung rencana manajemen insiden keamanan informasi. Mengembangkan dan menerapkan sistem informasi yang diperlukan untuk mendukung respons insiden, termasuk daftar insiden keamanan informasi. Mekanisme dan sistem ini dimaksudkan untuk mencegah kejadian insiden keamanan informasi atau mengurangi kemungkinan kejadian dari insiden keamanan informasi;

g) merancang dan mengembangkan program kesadaran dan kepedulian serta pelatihan untuk manajemen peristiwa keamanan informasi, insiden dan kerentanan;

h) menguji penggunaan rencana manajemen insiden keamanan informasi, semua proses dan prosedurnya.

Dengan selesainya fase ini, organisasi sebaiknya sudah siap untuk mengelola insiden keamanan informasi dengan baik. ISO/IEC 27035-2:2023, Pasal 4 sampai 11, menjelaskan setiap aktivitas yang tercantum di atas, termasuk isi dari dokumen kebijakan dan perencanaan.

5.3 Deteksi dan pelaporan

Fase kedua dari manajemen insiden keamanan informasi melibatkan deteksi dari, pengumpulan informasi yang terasosiasi dengan, dan pelaporan tentang, kejadian dari peristiwa keamanan informasi dan kerentanan keamanan informasi yang ditemukan atau yang terlibat, dengan cara-cara manual atau otomatis. Dalam fase ini, peristiwa dan kerentanan belum dapat diklasifikasikan sebagai insiden keamanan informasi.

Dimungkinkan terdapat beberapa kanal untuk pelaporan peristiwa keamanan ke titik kontak (PoC) yang tepat menggunakan laporan peristiwa. Sementara sejumlah peristiwa TIK dan teknis dilaporkan ke departemen TIK, isu-isu lainnya, seperti pelanggaran privasi, mungkin dinaikkan ke departemen lain dari organisasi. Organisasi sebaiknya memiliki prosedur yang sudah berlaku untuk mendistribusikan laporan peristiwa ke koordinator insiden untuk dapat berkoordinasi dan memberikan gambaran umum dari semua insiden keamanan informasi. Koordinator insiden sebaiknya mengoordinasikan input yang berbeda ini dengan departemen lain di dalam bisnisnya. Polisi, ambulans, pemadam kebakaran dan layanan darurat lainnya terkadang dapat dihubungi melalui nomor telepon yang berbeda. Lebih jauh, kanal komunikasi dapat berbeda: telepon, faks, pager, surel, alarm otomatis dalam sistem TIK, *mobile push notification*, dasbor (operator), dan lain-lain.

Entitas yang mendeteksi situasi tidaklah selalu yang mengalami konsekuensinya (misalnya satuan pengaman mendeteksi sebuah penyusupan dan seorang pencuri di kantor, kebakaran di sebuah rumah yang dideteksi oleh tetangga). Penting untuk mempertimbangkan konsep tim/entitas bisnis yang terkena atau terdampak, yaitu aktivitas bisnisnya dan lebih tepatnya personel/entitas yang melaksanakannya dan manajemen yang terkait.

Pelaporan peristiwa keamanan yang sejalan dengan kebijakan pelaporan organisasi memungkinkan analisis selanjutnya jika diperlukan.

Untuk fase mendeteksi dan melaporkan, suatu organisasi sebaiknya melakukan aktivitas utama berikut:

a) melakukan pemantauan dengan sistem atau tim monitoring (misalnya mengamati gambar kamera) dan aktivitas sistem log dan jaringan seperlunya;

b) mendeteksi dan melaporkan kejadian peristiwa keamanan informasi atau keberadaan dari kerentanan terkait dan ancaman, baik secara manual oleh personel atau secara otomatis;

c) mengumpulkan informasi tentang peristiwa keamanan informasi atau kerentanan dan ancaman terkait;

d) mengumpulkan informasi kesadaran situasional dari sumber data internal dan eksternal termasuk sistem lokal dan lalu lintas jaringan dan log aktivitas, umpan berita mengenai aktivitas politik, sosial, atau ekonomi yang sedang berlangsung yang dapat berdampak pada aktivitas insiden, umpan eksternal tentang tren insiden, vektor serangan baru, indikator pembobolan dan strategi mitigasi baru dan teknologi;

e) melaksanakan analisis ancaman eksternal/internal untuk membangun pemahaman lingkungan ancaman dan secara bergantian mendeteksi perubahan;

f) menentukan dan memasukkan reliabilitas dan kualitas informasi yang dianalisis dari asesmen ancaman;

g) melaksanakan analisis reguler untuk kerentanan dan vektor serangan, berdasarkan ancaman yang sudah ada dan yang potensial;

h) memastikan bahwa semua aktivitas deteksi dan hasilnya dicatat dengan benar untuk analisis selanjutnya;

i) memastikan bukti digital dikumpulkan dan disimpan dengan aman, dan preservasinya yang aman dimonitor terus-menerus, jika seandainya bukti diperlukan untuk penuntutan hukum atau tindakan disiplin internal. Untuk informasi detail mengenai identifikasi, pengumpulan, akuisisi dan preservasi bukti digital, lihat standar investigatif yang tercantum dalam Lampiran A;

j) menginformasikan, berdasarkan kebutuhan di sepanjang fase, untuk reviu atau keputusan lebih lanjut.

Semua informasi yang dikumpulkan terkait peristiwa keamanan informasi atau kerentanan dan ancaman terkait sebaiknya disimpan dalam daftar insiden keamanan informasi yang dikelola oleh IMT. Informasi yang dilaporkan pada setiap aktivitas sebaiknya sudah selengkap mungkin pada saat itu. Ini akan mendukung asesmen, keputusan dan tindakan yang akan diambil.

5.4 Asesmen dan pengambilan keputusan

Fase ketiga dari manajemen insiden keamanan informasi melibatkan asesmen informasi yang terasosiasi dengan kejadian peristiwa keamanan informasi dan keputusan mengklasifikasikan peristiwa sebagai insiden keamanan informasi. Koordinator insiden mengevaluasi peristiwa berdasarkan laporan peristiwa dan kriteria yang didefinisikan pada saat fase perencanaan dan persiapan dan menyatakannya sebagai insiden atau tidak.

Segera sesudah peristiwa keamanan informasi dideteksi dan dilaporkan, sebaiknya melaksanakan aktivitas berikut.

a) Mendistribusikan tanggung jawab untuk aktivitas manajemen insiden keamanan informasi melalui hierarki personel yang sesuai dengan asesmen, pengambilan keputusan dan tindakan yang melibatkan personel keamanan dan nonkeamanan.

b) Menyediakan prosedur formal untuk diikuti oleh setiap orang yang diberitahukan, termasuk dalam meninjau dan memperbaharui laporan, menilai kerusakan, dan memberi tahu personel yang relevan. Tindakan individual tergantung pada tipe dan keparahan dari insiden.

c) Menggunakan panduan untuk dokumentasi menyeluruh atas peristiwa keamanan informasi dan tindakan berikutnya untuk insiden keamanan informasi jika peristiwa keamanan informasi menjadi diklasifikasikan sebagai insiden keamanan informasi.

d) Mengevaluasi apakah suatu peristiwa merupakan insiden atau tidak, mengorelasikan peristiwa kejadian berulang dan mengambil data dari tindakan dan respons sebelumnya. Tipe dan kerangka waktu untuk penyelesaian tergantung pada keputusan yang berdasarkan pada faktor-faktor yang telah diputuskan pada saat fase perencanaan dan persiapan. Kriteria keputusan sebaiknya jelas dan teruji, mempertimbangkan aspek teknologi, bisnis dan manusia. Memprioritaskan semua insiden keamanan informasi menurut dokumentasi internal yang relevan.

e) Mengomunikasikan melalui kanal dan protokol yang sudah ditetapkan dan diaktifkan ke IRT dan manajemen bisnis, bila diperlukan.

f) Menghubungi tim respons yang diperlukan untuk merespons dan menyelesaikan berbagai masalah yang teridentifikasi saat deteksi dan informasi yang disediakan oleh penemu/pelapor.

g) Mengumpulkan informasi dari tim yang ditargetkan atau yang terdampak.

h) Memulai pewaktu untuk respons.

Merupakan hal yang krusial untuk membuat keputusan cepat yang menyatakan suatu peristiwa sebagai suatu insiden keamanan informasi karena ini memungkinkan penugasan IRT dengan cepat dan mengatur proses “hitung-mundur” untuk memastikan insiden diselesaikan dalam jangka waktu yang diharapkan. Tabel pengambilan keputusan sebaiknya telah disiapkan pada saat fase perencanaan dan persiapan.

Untuk fase asesmen dan keputusan, organisasi sebaiknya melakukan aktivitas utama berikut:

i) Mengumpulkan informasi yang dapat mencakup pengujian, pengukuran, dan pengumpulan data lain tentang deteksi peristiwa keamanan informasi. Tipe dan jumlah informasi yang dikumpulkan akan tergantung pada peristiwa keamanan informasi yang terjadi.

j) Melaksanakan asesmen oleh koordinator insiden untuk menentukan apakah peristiwa itu berpotensi atau insiden keamanan informasi yang sudah pasti atau alarm palsu. Alarm palsu (misalnya *false positive*) adalah indikasi dari peristiwa yang dilaporkan namun ternyata tidak nyata atau berdampak apa pun. Jika diinginkan, IRT dapat melaksanakan reviu kualitas untuk memastikan bahwa koordinator insider telah menyatakan suatu insiden dengan benar.

k) Mencatat semua aktivitas (membuat log), hasil dan keputusan terkait untuk analisis dan pencatatan selanjutnya.

l) Memastikan bahwa kontrol perubahan yang berlaku dipelihara untuk mencakup penelusuran insiden keamanan informasi dan pembaruan laporan insiden, dan untuk selalu menjaga register insiden keamanan informasi tetap mutakhir.

Semua informasi yang dikumpulkan perihal peristiwa/insiden keamanan informasi atau kerentanan dan ancaman terkait sebaiknya disimpan dalam register insiden keamanan informasi yang dikelola oleh IMT. Informasi yang dilaporkan selama setiap aktivitas sebaiknya selengkap mungkin pada saat itu. Ini akan mendukung asesmen, keputusan dan tindakan yang diambil.

5.5 Respons

Fase keempat dari manajemen insiden keamanan informasi melibatkan respons terhadap insiden keamanan informasi sesuai dengan keputusan dalam fase asesmen dan pengambilan keputusan, dan prosedur yang dijelaskan dalam rencana respons diuraikan pada saat fase perencanaan dan persiapan. Tergantung pada keputusannya, respons dapat segera dibuat, dalam waktu-nyata, atau mendekati waktu-nyata, dan beberapa respons dapat melibatkan investigasi keamanan informasi. Koordinator insiden merupakan peran kunci untuk mengoordinasikan aktivitas IRT dan memonitor pewaktu respons.

Setiap tipe insiden akan menerima respons khususnya. Tergantung pada apa yang ditemukan oleh IRT selama diaktifkan, respons insiden dapat mengambil berbagai jalur berbeda dan mungkin memerlukan sumber daya beragam/yang berbeda.

Koordinator insiden keamanan informasi dipastikan selalu mendapat informasi terkini dalam frekuensi yang sepadan dengan tingkat keparahan insiden, dan dapat membuat keputusan untuk menghubungi tim lain dengan keterampilan spesifik tergantung pada kebutuhan untuk merespons insiden yang ditemukan atau memperbaiki/memulihkan aset yang cacat, rusak atau hancur (fisik, material, perangkat lunak, prosedural, organisasional, dll.).

Ketika merespons kepada suatu peristiwa yang bukan insiden, umumnya, peristiwa terselesaikan dalam proses bisnis normal, karena tidak ada keadaan darurat atau bahaya langsung.

Koordinator insiden tetap melakukan kontak rutin dengan tim/entitas yang ditarget/terdampak insiden dan memutuskan, dengan mereka, apakah insiden bisa teratasi atau tidak. Ini untuk lebih memastikan apakah sumber daya cukup tersedia untuk memulai aktivitas bisnis kembali. Situasi ini bagaimanapun memerlukan penyelesaian yang lebih lengkap, dengan pemulihan menyeluruh dan dimulainya kembali kapabilitas dan pengoperasian.

Koordinator insiden mempersiapkan laporan insiden yang sebaiknya mencakup:

— analisis terhadap situasi;

— identifikasi masalah dan, jika memungkinkan, penyebabnya;

— penentuan gravitasi/keseriusan dan urgensi untuk merespons;

— ketercakupan dalam program perubahan.

CATATAN 1 Jika penyelesaian insiden melampaui sesi jam kerja koordinator insiden (misalnya sudah melebihi 8 jam sampai beberapa hari), koordinator insiden pertama mengumpulkan semua informasi dan catatan yang diterima yang dibuat oleh semua koordinator insiden yang terlibat untuk menghasilkan laporan akhir. Koordinator tersebut tetap menjadi koordinator insiden yang utama.

Prosedur respons yang perlu diikuti mensyaratkan:

— definisi insiden yang jelas untuk dikelola dan dikontrol;

— daftar sumber daya yang diperlukan dan dipersyaratkan;

— kronologi tindakan yang akan dilakukan secara detail, dengan pengaturan waktu;

— jangka waktu penyelesaian target;

— daftar poin kontak dan saluran untuk informasi dengan kriterianya;

— keterampilan dan ukuran dari tim (dengan pelatihan yang diperlukan/disyaratkan);

— kehadiran sumber daya.

Setelah suatu insiden keamanan informasi dikonfirmasi dan responsnya ditentukan, aktivitas berikutnya sebaiknya dilakukan:

a) Mendistribusikan tanggung jawab untuk aktivitas manajemen insiden keamanan informasi melalui hierarki personel yang tepat dengan pengambilan keputusan dan tindakan, melibatkan baik personel keamanan dan nonkeamanan seperlunya.

b) Menyediakan prosedur formal untuk diikuti setiap person yang terlibat, termasuk dalam mereviu dan memperbarui laporan, menilai ulang kerusakan, dan memberi tahu personel yang relevan. Tindakan individual tergantung pada tipe dan keparahan insidennya. Untuk informasi lebih lanjut tentang respons insiden TIK, lihat ISO/IEC 27035-3:2020, Pasal 8, 9 dan 11.

c) Mempertimbangkan kembali asesmen orisinal ketika tersedia informasi tambahan untuk mengidentifikasi apakah insiden keamanan informasi harus diprioritaskan kembali, atau aktivitas respons disesuaikan.

d) Menggunakan pedoman untuk dokumentasi menyeluruh atas insiden keamanan informasi dan tindakan yang dilakukan setelahnya.

e) Mengevaluasi penyelesaian yang diusulkan bersama tim/entitas yang ditarget/terdampak untuk memastikannya memenuhi kriteria penyelesaian dan ekspektasi dari semua pihak yang terlibat.

f) Menginvestigasi insiden seperlunya dan relatif pada peringkat skala klasifikasi insiden keamanan informasi. Peringkat sebaiknya berubah seperlunya. Investigasi dapat termasuk beragam jenis analisis yang berbeda demi menyediakan pemahaman insiden yang lebih mendalam.

g) Reviu oleh koordinator insiden dan IRT untuk menentukan apakah insiden keamanan informasi terkontrol, dan jika demikian, menjalankan respons yang diperlukan. Dalam hal insiden tidak terkontrol, atau akan mengakibatkan dampak kerugian parah ke organisasi, mengeskalasinya ke tim manajemen krisis. Eskalasi dapat menghasilkan tindakan (respons) di dua level berbeda:

    — satu yang berada di dalam tanggung jawab dan otoritas koordinator insiden (lihat 5.2 dan 5.3) untuk, sebagai contoh, memanggil lebih banyak tim respons dengan keterampilan berbeda untuk mengatasi hal apa yang ditemukan (ini yang terjadi dalam

kasus kebakaran ketika titik kontak darurat memanggil ambulans, polisi dan tim pemadam kebakaran lain);

— satu yang berada di luar otoritas koordinator insiden yang kemudian memanggil level manajemen lain (misalnya keterlibatan departemen lain dalam organisasi, memanggil dukungan eksternal dengan konsekuensi finansial yang memerlukan otorisasi dari departemen keuangan).

h) Menugaskan sumber daya internal dan mengidentifikasi sumber daya eksternal untuk merespons insiden.

i) Memastikan semua pihak yang terlibat, khususnya IRT, mencatat semua aktivitas (membuat log) dengan benar untuk analisis selanjutnya.

j) Memastikan bahwa bukti digital dikumpulkan dan disimpan secara aman dan terbukti aman, dan preservasi keamanannya terus dimonitor, dalam hal bukti diperlukan untuk penuntutan hukum atau tindakan disipliner internal.

Pengumpulan bukti digital termasuk tindakan yang berikut:

— menyediakan pembaruan status secara berkala kepada pemangku kepentingan utama;

— mengumpulkan, merekam, dan memelihara rantai pengawasan atas bukti yang terkait insiden;

— menyampaikan notifikasi kepada regulator mengenai insiden tersebut (bilamana berlaku);

— memperbarui register insiden dengan detail penutupan insiden;

— mengikuti aturan retensi dan preservasi bukti apa pun yang berkaitan dengan insiden keamanan informasi (persyaratan hukum dan peraturan dapat berlaku).

CATATAN 2 Untuk informasi lebih detail tentang identifikasi, pengumpulan, akuisisi dan preservasi bukti digital, lihat standar investigatif yang tercantum dalam Lampiran A.

k) memastikan bahwa kontrol perubahan yang berlaku dipelihara untuk mencakup penelusuran insiden keamanan informasi dan pembaruan laporan insiden, dan untuk selalu menjaga register insiden keamanan informasi tetap mutakhir.

l) Mengikuti protokol komunikasi dan/atau rencana keterlibatan yang sudah ditentukan sebelumnya yang mengidentifikasi siapa yang berotoritas untuk berkomunikasi dengan pemangku kepentingan yang berbeda-beda, dan mengomunikasikan adanya insiden keamanan informasi dan membagikan detail apa pun yang relevan (misalnya informasi ancaman, serangan, dan kerentanan) dengan individual atau organisasi internal dan eksternal, sesuai dengan rencana komunikasi manajemen organisasi dan insiden dan kebijakan pengungkapan informasi. Bisa menjadi sangat penting untuk memberi tahu pemilik aset (ditentukan pada saat analisis dampak) dan organisasi internal dan eksternal (misalnya tim tanggap insiden lain, agensi penegak hukum, penyedia layanan internet, dan organisasi yang berbagi informasi) yang dapat membantu perihal manajemen dan penyelesaian insiden. Berbagi informasi juga dapat bermanfaat bagi organisasi lain karena ancaman dan serangan yang sama sering kali berdampak pada banyak organisasi. Untuk informasi lebih detail tentang berbagi informasi, lihat ISO/IEC 27010.

m) Setelah pemulihan dari insiden, suatu aktivitas pascainsiden sebaiknya dimulai dengan bergantung pada sifat dan keparahan insiden. Aktivitas ini termasuk:

   — investigasi informasi yang berkaitan dengan insiden,

   — investigasi sumber relevan lainnya seperti personel yang terlibat,

   — ringkasan laporan temuan investigasi.

n) Setelah insiden terselesaikan, sebaiknya ditutup sesuai dengan aturan yang sudah ditentukan dalam kebijakan manajemen insiden informasi dan semua pihak yang berkepentingan sebaiknya diberi notifikasi.

Semua informasi yang dikumpulkan perihal peristiwa/insiden keamanan informasi, atau kerentanan dan ancaman terkait sebaiknya disimpan dalam register insiden keamanan informasi yang dikelola oleh IMT. Informasi yang dilaporkan selama setiap aktivitas sebaiknya selengkap mungkin pada saat itu. Ini akan mendukung asesmen, keputusan dan tindakan yang diambil, termasuk potensi analisis lebih lanjut.

5.6 Pembelajaran

Fase kelima dari manajemen insiden keamanan informasi muncul ketika insiden keamanan informasi sudah diselesaikan. Fase ini melibatkan pembelajaran dari bagaimana insiden, kerentanan terkait dan ancaman dapat ditangani.

Pelajaran dapat berasal dari satu atau banyak insiden keamanan informasi atau kerentanan keamanan yang dilaporkan. Peningkatan dibantu oleh metrik yang dimasukkan ke dalam strategi organisasi dalam berinvestasi pada kontrol keamanan informasi. Merupakan hal yang penting untuk pembelajaran dihubungkan dengan kapabilitas perubahan manajemen keamanan informasi yang membuat keputusan bisnis dan, bila dianggap perlu, memasukkan modifikasi yang diusulkan ke dalam proses peningkatan manajemen keamanan informasi.

Laporan insiden sebaiknya mengindikasikan berbagai situasi yang mengarah ke berbagai tindakan untuk diteruskan ke proses peningkatan manajemen keamanan informasi. Laporan ini sebaiknya juga membuat peningkatan untuk rencana manajemen insiden keamanan informasi dan dokumentasinya berdasarkan pembelajaran.

Untuk fase pembelajaran, organisasi sebaiknya melakukan aktivitas utama berikut:

a) mereviu seberapa efektif proses, prosedur, format pelaporan dan struktur organisasi saat merespons, penilaian dan pemulihan dari insiden keamanan informasi dan penanganan kerentanan keamanan informasi;

b) mengidentifikasi, mendokumentasikan dan mengomunikasikan pembelajaran dari insiden keamanan informasi, kerentanan terkait dan ancaman;
c) mereviu, mengidentifikasi dan membuat peningkatan pada implementasi kontrol keamanan informasi (kontrol baru atau yang diperbarui), beserta kebijakan manajemen insiden keamanan informasi;

d) mereviu, mengidentifikasi dan membuat peningkatan pada asesmen risiko dan manajemen reviu keamanan informasi milik organisasi yang ada saat ini;

e) mengomunikasikan dan berbagi hasil reviu di dalam komunitas tepercaya (jika organisasi menghendakinya);

f) menentukan jika informasi insiden, vektor serangan dan kerentanan terkait dapat dibagikan dengan organisasi mitra untuk membantu mencegah insiden yang sama terjadi di lingkungan mereka. Untuk lebih detail, lihat ISO/IEC 27010 tentang berbagi informasi;

g) melakukan evaluasi secara komprehensif atas performa dan efektivitas IRT secara periodik.

Ditekankan bahwa aktivitas manajemen insiden keamanan informasi bersifat berulang, dan oleh karena itu organisasi sebaiknya membuat peningkatan berkala ke sejumlah elemen keamanan informasi dari waktu ke waktu. Peningkatan ini sebaiknya diusulkan berdasarkan reviu data pada insiden keamanan informasi, respons, dan kerentanan keamanan informasi yang dilaporkan.

Lampiran D menyediakan pertimbangan dari situasi yang ditemukan pada saat investigasi insiden.

ISO/IEC 27035-2:2023, Pasal 12 menjelaskan detail setiap aktivitas yang dicantumkan di atas.

Lampiran A
(informatif)
Hubungan dengan standar investigatif

Dokumen ini menjelaskan bagian dari proses investigatif komprehensif yang termasuk, tetapi tidak terbatas pada, penerapan standar berikut:

— ISO/IEC 27037

ISO/IEC 27037 menjelaskan cara yang digunakan dalam tahap awal investigasi, termasuk respons awal, dapat menjamin didapatnya bukti digital potensial yang cukup untuk memungkinkan investigasi berjalan dengan tepat.

— ISO/IEC 27038

Sejumlah dokumen dapat mengandung informasi yang sebaiknya tidak diungkapkan kepada beberapa komunitas. Dokumen yang sudah dimodifikasi dapat dirilis untuk komunitas tersebut setelah pemrosesan yang tepat pada dokumen orisinal. Proses menghapus informasi yang tidak boleh diungkapkan disebut “*redaction*”.

Redaction digital pada dokumen merupakan area yang relatif baru dari praktik manajemen dokumen, mengangkat isu-isu unik dan potensi risiko. Ketika dokumen digital disensor (*redacted*), informasi yang dihapus sebaiknya tidak dapat dipulihkan. Oleh karena itu, harus diperhatikan supaya informasi yang disensor terhapus secara permanen dari dokumen digital (misalnya, sebaiknya tidak hanya sekadar tersembunyi di dalam bagian yang tidak dapat ditampilkan dari dokumen).

ISO/IEC 27038 menetapkan metode untuk *redaction* digital pada dokumen digital. Standar ini juga menetapkan persyaratan atas perangkat lunak yang dapat digunakan untuk *redaction*.

— ISO/IEC 27040

ISO/IEC 27040 menyediakan panduan teknis yang detail tentang bagaimana organisasi dapat mendefinisikan level mitigasi risiko yang tepat menggunakan pendekatan yang telah terbukti dan konsisten untuk perencanaan, desain, dokumentasi dan implementasi keamanan penyimpanan data. Keamanan penyimpanan berlaku untuk proteksi (keamanan) informasi di mana ia tersimpan dan keamanan informasi yang ditransfer melalui tautan komunikasi yang terkait dengan penyimpanan. Keamanan penyimpanan termasuk keamanan peranti dan media, keamanan aplikasi dan layanan, dan keamanan yang relevan ke pengguna akhir selama masa pakai peranti dan media serta setelah penggunaannya berakhir.
Mekanisme keamanan seperti enkripsi dan sanitasi dapat memengaruhi kemampuan menginvestigasi karena menerapkan mekanisme pengaburan (*obfuscation*). Hal ini sebaiknya dipertimbangkan sebelum dan selama pelaksanaan investigasi. Hal ini juga dapat menjadi penting untuk memastikan penyimpanan bahan pembuktian selama dan setelah investigasi dipersiapkan dan diamankan secara memadai.

— ISO/IEC 27041

Hal yang penting untuk metode dan proses yang diterapkan selama investigasi dapat terbukti tepat. ISO/IEC 27041 menyediakan panduan tentang bagaimana memberikan jaminan bahwa metode dan proses memenuhi persyaratan investigasi dan telah diuji dengan tepat.

— ISO/IEC 27042

Dokumen ini menjelaskan bagaimana metode dan proses yang akan digunakan selama investigasi dapat dirancang dan diimplementasikan untuk memungkinkan evaluasi yang benar dari bukti digital potensial, interpretasi bukti digital dan pelaporan temuan yang efektif.

— ISO/IEC 27043

Dokumen ini mendefinisikan prinsip dan proses umum utama yang mendasari investigasi insiden dan menyediakan model kerangka kerja untuk semua tahapan investigasi.

— seri ISO/IEC 27050

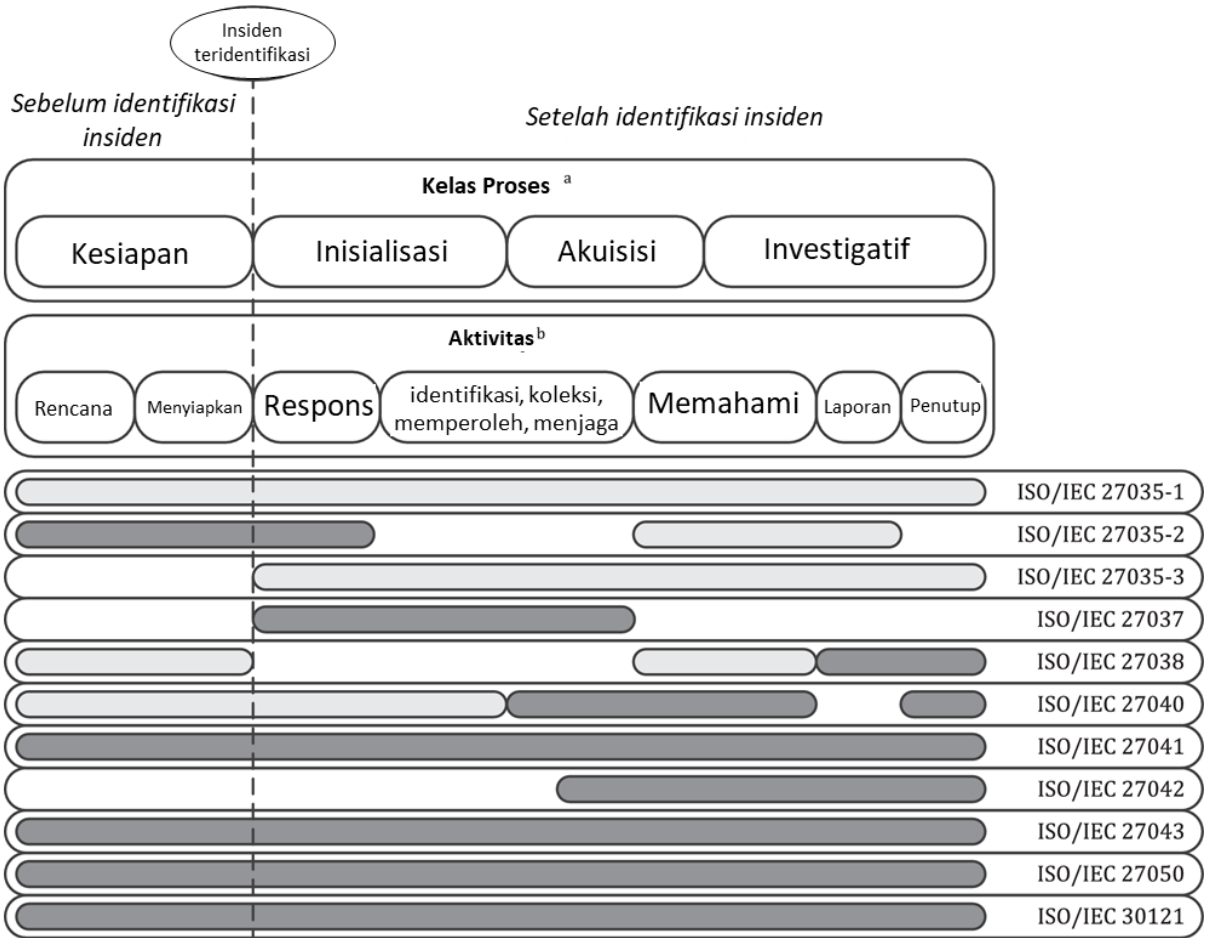
Seri ISO/IEC 27050 membahas aktivitas dalam *electronic discovery*, termasuk, tetapi tidak terbatas pada identifikasi, preservasi, pengumpulan, pemrosesan, reviu, analisis, dan produksi dari informasi yang disimpan secara elektronik (*Electronically Stored Information*/ESI). Sebagai tambahan, terdapat panduan untuk langkah-langkah, mulai dari penciptaan awal ESI hingga disposisi akhirnya, yang dapat dilakukan organisasi untuk memitigasi risiko dan biaya jika *electronic discovery* menjadi masalah. Ini relevan untuk personel teknis dan nonteknis yang terlibat dalam beberapa atau seluruh aktivitas *electronic discovery*.

Electronic discovery sering berfungsi sebagai penggerak untuk investigasi dan juga aktivitas perolehan dan penanganan bukti. Sebagai tambahan, sensitivitas dan kekritisan data terkadang memerlukan proteksi seperti keamanan penyimpanan untuk mencegah pelanggaran data.

— ISO/IEC 30121

ISO/IEC 30121 menyediakan kerangka kerja untuk badan pengurus organisasi (termasuk pemilik, dewan komisaris, direktur, partner, eksekutif senior, atau yang serupa) tentang cara terbaik menyiapkan organisasi untuk investigasi digital sebelum hal itu terjadi. ISO/IEC 30121 berlaku untuk pengembangan proses strategis (dan keputusan) terkait retensi, availabilitas, akses dan efektivitas biaya atas pengungkapan bukti digital. ISO/IEC 30121 berlaku untuk semua tipe dan ukuran organisasi. ISO/IEC 30121 adalah tentang persiapan strategis yang hati-hati untuk investigasi digital dari suatu organisasi. Kesiapan forensik memastikan bahwa organisasi telah membuat persiapan strategis yang tepat dan relevan untuk menerima peristiwa potensial yang bersifat bukti. Tindakan dapat muncul sebagai akibat dari pelanggaran keamanan, penipuan, dan penegasan reputasi yang tidak dapat dihindari. Dalam segala situasi Teknologi Informasi (TI) sebaiknya dikerahkan secara strategis untuk memaksimalkan efektivitas dari ketersediaan bukti, aksesibilitas dan efisiensi biaya

Gambar A.1 menunjukkan aktivitas tipikal di sekitar suatu insiden dan investigasinya. Nomor referensi dokumen yang ditunjukkan pada gambar ini (misalnya ISO/IEC 27037) menandakan dokumen yang tercantum di atas dan batang yang diarsir menunjukkan di mana masing-masing yang kemungkinan besar dapat diterapkan secara langsung atau mempunyai pengaruh terhadap proses investigatif tersebut (misalnya dengan mengatur kebijakan atau menciptakan batasan). Namun, direkomendasikan agar semua dokumen dikonsultasikan sebelum, dan selama, fase perencanaan dan persiapan. Kelas proses yang ditampilkan didefinisikan sepenuhnya dalam ISO/IEC 27043 dan aktivitasnya yang teridentifikasi cocok dibahas lebih detail dalam ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27042 dan ISO/IEC 27041.



Key

the document can be directly applied to these activities

the document contains information which may influence and/or assist with these activities

a Process classes are defined in ISO/IEC 27043.

b Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037, and ISO/IEC 27042.

Gambar A.1 — Penerapan standar pada kelas dan aktivitas proses investigasi

Lampiran B
(informatif)
Contoh insiden keamanan informasi dan penyebabnya

B.1 Tipe insiden

B.1.1 Umum

Peristiwa dan insiden yang dicakup oleh seri ISO/IEC 27035 menyangkut keamanan informasi dan TIK. Peristiwa dan insiden itu dihasilkan dari manajemen risiko yang tidak sempurna dan kemajuan yang berkelanjutan atas orang, proses dan teknologi – dan kerentanan terkaitnya – dalam konteks berkembangnya motivasi dan kapabilitas penyerang.

Peristiwa/insiden terjadi dalam domain-domain berikut dan manajemen insiden sebaiknya mencakup semua kasus-kasus potensial.

B.1.2 Konfidensialitas

Kebocoran informasi dapat berdampak langsung pada organisasi, dan dapat membuat informasi tersedia secara permanen bagi penyerang takterotorisasi dan/atau kriminal.

Oleh karena itu, sebaiknya ada yang “menutup pintu” (misalnya menghentikan kebocoran, menambal kebocoran) dan mencegah pelanggaran di masa mendatang dengan mengidentifikasi tempat di mana itu terjadi dan penyebabnya.

B.1.3 Integritas

Insiden integritas (informasi yang dimodifikasi secara berlebihan) sebaiknya dideteksi dan dikoreksi sebelum informasi dipublikasi dan/atau digunakan.

Pencegahan diperlukan dengan mengidentifikasi penyebabnya.

B.1.4 Availabilitas

Ketidaktersediaan informasi (informasi yang tidak dapat dijangkau, tidak dapat digunakan, dihapus atau hilang) dapat membuat efek sehubungan dengan perjanjian level layanan (*service level agreement*/SLA) dan RPO. Informasi sebaiknya telah ditemukan dan dipulihkan sebelum dampak bisnis menjadi tidak dapat diterima.

CONTOH Laporan keuangan lengkap yang siap kirim ke otoritas fiskal tidak dipatuhi di tanggal yang ditentukan.

B.1.5 Kontrol akses

Akses takterotorisasi mengarah pada kebobolan sistem, pencurian sumber daya, dan pelanggaran informasi.

Kejadian di masa depan sebaiknya dicegah dengan mengidentifikasi eksposur dan penyebab yang mendasari dan, bilamana berlaku, peninjauan izin akses kontrol (otorisasi, autentikasi, peran, hak Istimewa, akses jaringan, dan lain-lain.)

B.1.6 Kerentanan

Kerentanan teknis, orang atau procedural, seperti kesalahan alokasi hak akses, memungkinkan eksploitasi berhasil. Contoh kerentanan termasuk:

— server, mesin atau perangkat lunak yang *unpatched* (tidak mutakhir);

— proteksi aset (informasi, peralatan, ruangan) yang tidak memadai sehubungan dengan kekritisannya.

B.1.7 Kegagalan teknis

Kegagalan teknis membuat peranti fisik atau TIK tidak dapat digunakan atau tidak dapat beroperasi. Hal ini menciptakan baik kerentanan atau potensi pelanggaran SLA dan RTO.

B.1.8 Pencurian atau kehilangan peralatan

Pencurian atau kehilangan peralatan, terutama yang berisi informasi, sebaiknya dipertimbangkan sebagai insiden availabilitas dan/atau konfidensialitas.

B.2 Serangan

B.2.1 Penolakan layanan (*Denial of Service*)

Penolakan layanan (*Denial of Service*/DoS) dan penolakan layanan terdistribusi (*Distributed Denial of Service*/DDoS) merupakan kategori insiden yang luas dengan ancaman umum. Insiden semacam itu menyebabkan suatu sistem, layanan atau jaringan gagal untuk lanjut beroperasi dalam kapasitas yang dimaksudkan, paling sering dengan penolakan akses total ke pengguna yang sah. Terdapat dua tipe utama dari insiden DoS/DDoS yang disebabkan oleh cara-cara teknis: eliminasi sumber daya dan kekurangan sumber daya.

Contoh tipikal dari insiden teknis Dos/DDoS yang disengaja termasuk yang berikut ini:

— *forging of traffic* (seperti *pinging*) ke alamat siaran jaringan atau layanan lain dalam upaya untuk membanjiri *bandwidth* jaringan target organisasi;

— mengirim data dalam format tidak terduga kepada sistem, layanan atau jaringan dalam upaya untuk melumpuhkan, atau mengganggu operasi normalnya;

— membuka banyak sesi terotorisasi dengan sistem, layanan atau jaringan tertentu dalam upaya menghabiskan sumber dayanya (yaitu untuk memperlambatnya, menguncinya atau melumpuhkannya).

Serangan-serangan itu sering dilakukan melalui bot, suatu sistem komputer yang menjalankan perangkat perusak yang dikontrol melalui botnet. Botnet adalah sebuah jaringan komando dan kontrol bot pusat yang dikelola oleh manusia. Ukuran botnet dapat berkisar dari ratusan sampai jutaan komputer yang terpengaruh.

Sejumlah insiden teknis DoS dapat disebabkan secara tidak sengaja, sebagai contoh, disebabkan oleh kesalahan konfigurasi operator atau melalui inkompatibilitas dari perangkat lunak aplikasi, tetapi sering kali, mereka disengaja. Sejumlah insiden teknis DoS sengaja diluncurkan untuk melumpuhkan sistem atau layanan, atau mematikan jaringan, dengan yang lainnya hanyalah produk sampingan hasil dari aktivitas jahat lain. Contohnya, beberapa teknik

pemindaian senyap dan identifikasi yang lebih umum dapat menyebabkan sistem atau layanan yang lebih tua atau salah konfigurasi menjadi lumpuh ketika dipindai. Sebaiknya dicatat bahwa banyak insiden teknis DoS yang sering dieksekusi secara anonim (yakni sumber serangan adalah “palsu”), karena tipikalnya tidak bergantung pada penyerang untuk menerima kembali informasi apa pun dari jaringan atau sistem yang diserang.

Insiden DoS yang disebabkan oleh sarana nonteknis, yang mengakibatkan kehilangan informasi, layanan dan/atau fasilitas, dapat disebabkan, sebagai contoh, oleh:

— pelanggaran pengaturan keamanan fisik mengakibatkan pencurian atau kerusakan yang disengaja dan kehancuran peralatan;

— kerusakan takdisengaja pada perangkat keras (dan/atau lokasinya) karena kebakaran atau kerusakan akibat air/banjir;

— kondisi lingkungan ekstrem, sebagai contoh suhu operasi yang tinggi (misalnya karena kegagalan pendingin ruangan);

— sistem malafungsi atau kelebihan beban;

— perubahan sistem takterkontrol;

— malafungsi perangkat lunak atau perangkat keras.

B.2.2 Akses takterotorisasi

Secara umum, insiden kategori ini berisi percobaan takterotorisasi aktual untuk mengakses atau menyalahgunakan suatu sistem, layanan atau jaringan. Beberapa contoh insiden akses takterotorisasi teknis termasuk:

— percobaan mengambil fail kata sandi;

— serangan *buffer overflow* untuk mencoba mendapatkan akses hak Istimewa (misalnya administrator sistem) ke suatu target;

— eksploitasi kerentanan protokol untuk membajak atau menyesatkan koneksi jaringan yang sah;

— percobaan untuk mengangkat suatu hak istimewa ke sumber daya atau informasi melampaui apa yang seorang pengguna atau administrator sudah miliki secara sah;

— membobol di level *registrar* nama domain atau penyedia *hosting*, yang mengakibatkan hilangnya kontrol atas portofolio domain milik organisasi, layanan surel, atau atas pengoperasian atau konten situs web.

Insiden akses takterotorisasi yang disebabkan oleh cara-cara nonteknis, yang mengakibatkan pengungkapan atau modifikasi informasi secara langsung atau tidak langsung, pelanggaran akuntabilitas atau penyalahgunaan sistem informasi, dapat disebabkan, sebagai contoh, oleh:

— pelanggaran terhadap pengaturan keamanan fisik yang mengakibatkan akses takterotorisasi pada informasi;

— sistem operasi yang buruk dan/atau salah konfigurasi karena perubahan sistem yang takterkontrol, atau malafungsi dari perangkat lunak atau perangkat keras;

— orang dalam yang merusak misalnya personel yang menggunakan aksesnya ke aset informasi milik organisasi demi keuntungan pribadi.

B.2.3 Perangkat lunak perusak

Perangkat lunak perusak adalah sebuah program atau bagian dari program yang dimasukkan ke dalam program lain dengan maksud memodifikasi perilaku orisinalnya, biasanya untuk melakukan aktivitas jahat seperti pencurian informasi dan identitas, penghancuran informasi dan sumber daya, penolakan layanan (*Denial of Service*), spam, dll. Serangan perangkat lunak perusak dapat dibagi ke dalam lima kategori: virus, *worms*, *Trojan horses*, kode seluler dan campuran. Sementara virus dibuat untuk menyasar sistem yang terinfeksi kerentanan apa pun, perangkat lunak perusak lainnya juga digunakan untuk melakukan serangan yang ditargetkan. Terkadang ini dilakukan dengan memodifikasi perangkat lunak perusak yang sudah ada dan membuat varian yang sering kali tidak dikenali oleh teknologi deteksi perangkat lunak perusak.

B.2.4 Penyalahgunaan

Insiden semacam ini terjadi ketika pengguna melanggar kebijakan keamanan sistem informasi milik organisasi. Insiden tersebut bukan serangan dalam arti sebenarnya, tetapi sering dilaporkan sebagai insiden dan sebaiknya ditangani oleh IRT. Penggunaan yang tidak pantas dapat termasuk:

— mengunduh dan menginstal alat peretasan;

— menggunakan surel perusahaan untuk spam atau promosi bisnis pribadi;

— menggunakan sumber daya perusahaan untuk mengatur situs web takterotorisasi;

— menggunakan aktivitas *peer-to-peer* untuk memperoleh atau mendistribusikan fail bajakan (musik, video, perangkat lunak);

— menyalahgunakan akses fisik dan logikal untuk mencuri informasi demi keuntungan pribadi;

— menyalahgunakan hak Istimewa/posisi untuk mendapatkan informasi dan mengungkapkannya ke pihak lain.

B.3 Pengumpulan informasi

Dalam istilah umum, kategori pengumpulan informasi insiden memasukkan aktivitas yang terasosiasi dengan mengidentifikasi target potensial dan memahami layanan yang berjalan pada target tersebut. Tipe insiden ini melibatkan pengintaian, dengan gol untuk mengidentifikasi:

— keberadaan suatu target, dan memahami topologi jaringan fisik dan logikalnya (misalnya jaringan TI, fasilitas, struktur organisasi) di sekitarnya, dan dengan siapa target berkomunikasi secara rutin;

— potensi kerentanan pada target atau lingkungan langsungnya yang dapat dieksploitasi.

Contoh tipikal dari pengumpulan informasi dengan cara teknis termasuk yang berikut ini:

— pengintaian dan identifikasi infrastruktur dalam jaringan milik korban dengan melakukan pencarian pada nama-nama domain atau alamat-alamat IP yang diketahui, atau dengan menganalisis informasi DNS pasif;

— *pinging* alamat jaringan untuk menemukan sistem yang “hidup”;

— menyelidiki sistem untuk mengidentifikasi (misalnya sidik jari) sistem operasi hos;

— memindai porta jaringan yang tersedia pada sistem untuk mengidentifikasi layanan jaringan (misalnya surel, *File Transfer Protocol* (FTP), situs, dll.] dan versi perangkat lunak dari layanan-layanan tersebut;

— memindai satu atau lebih layanan rentan yang diketahui di seluruh rentang alamat jaringan (pemindaian horizontal).

Dalam sejumlah kasus, pengumpulan informasi teknis meluas menjadi akses takterotorisai jika, sebagai contoh, sebagai bagian dari pencarian kerentanan, penyerang juga mencoba memperoleh akses takterotorisasi. Hal ini umumnya terjadi dengan alat otomatis yang tidak hanya mencari kerentanan tetapi juga secara otomatis mencoba mengeksploitasi sistem, layanan dan/atau jaringan rentan yang ditemukan.

Insiden pengumpulan informasi yang disebabkan oleh cara-cara nonteknis, mengakibatkan:

— pengungkapan langsung atau tidak langsung atau modifikasi informasi;

— pencurian kekayaan intelektual yang disimpan secara elektronik;

— pelanggaran akuntabilitas, misalnya dalam log akun;

— penyalahgunaan sistem informasi (misalnya bertentangan dengan hukum atau kebijakan organisasi).

Insiden pengumpulan informasi dapat disebabkan, sebagai contoh, oleh:

— pelanggaran pengaturan keamanan fisik yang mengakibatkan akses takterotorisasi pada informasi, dan pencurian peralatan penyimpanan data yang berisi data penting, misalnya kunci enkripsi;

— sistem operasi yang buruk dan/atau salah konfigurasi karena perubahan sistem yang takterkontrol, atau malafungsi dari perangkat lunak atau perangkat keras, mengakibatkan personel internal atau eksternal memperoleh akses pada informasi yang tidak mereka miliki otorisasinya;

— rekayasa sosial, yaitu tindakan memanipulasi orang untuk melakukan tindakan atau membocorkan informasi konfidensial, misalnya pengelabuan (*phishing*), peniruan identitas orang lain dalam panggilan telepon;

— membuntuti ke area terbatas;

— mendengarkan percakapan;

— mengintip (*shoulder surfing*)/pengintipan atas dokumen terbuka;

— mencari di tempat sampah (*dumpster diving*);

— memanipulasi staf.

Lampiran C
(informatif)
Tabel referensi silang dari ISO/IEC 27001 dengan seri ISO/IEC 27035

Tabel C.1 menunjukkan referensi dari ISO/IEC 27001:2022, Lampiran A, mengenai manajemen insiden keamanan informasi dan di mana referensi ini berkorespondensi dengan yang ada dalam seri ISO/IEC 27035. Subpasal spesifik dari tiap dokumen ini ditunjukkan di tiap awal baris.

Tabel C.1 — Referensi silang dari ISO/IEC 27001:2022 di dalam seri ISO/IEC 27035

ISO/IEC 27001:2022, Lampiran A	**Seri ISO/IEC 27035**
5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi Kontrol: Organisasi harus merencanakan dan menyiapkan pengelolaan insiden keamanan informasi dengan mendefinisikan, menetapkan dan mengomunikasikan proses, peran dan tanggung jawab manajemen insiden keamanan informasi.	**ISO/IEC 27035-1:2023** **5.2 Perencanaan dan persiapan** **ISO/IEC 27035-2:2023** **4. Kebijakan manajemen insiden keamanan informasi** **5. Memperbarui kebijakan keamanan informasi** **6. Membuat rencana manajemen insiden keamanan informasi** **7. Menetapkan kapabilitas manajemen insiden** **8. Menetapkan hubungan internal dan eksternal** **9. Menentukan dukungan teknis dan lainnya** **10. Membuat kesadaran dan kepedulian serta pelatihan insiden keamanan informasi** **11. Menguji rencana manajemen insiden keamanan informasi**
6.8 Pelaporan peristiwa keamanan informasi Kontrol: Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan peristiwa keamanan informasi yang diamati atau dicurigai melalui saluran yang sesuai pada waktu yang tepat.	**ISO/IEC 27035-1:2023** **5.3 Deteksi dan pelaporan** **ISO/IEC 27035-3:2020** **7 Operasi deteksi insiden** **8 Operasi notifikasi insiden** **12 Operasi pelaporan insiden**
5.25 Asesmen dan keputusan tentang peristiwa keamanan informasi Kontrol: Organisasi harus menilai peristiwa keamanan informasi dan memutuskan apakah peristiwa tersebut akan dikategorikan sebagai insiden keamanan informasi.	**ISO/IEC 27035-1:2023** **5.4 Asesmen dan pengambilan keputusan** **ISO/IEC 27035-3:2020** **9 Operasi triase insiden** **10 Operasi analisis insiden**
5.26 Respons terhadap insiden keamanan informasi Kontrol: Insiden keamanan informasi harus direspons sesuai dengan prosedur yang terdokumentasi.	**ISO/IEC 27035-1:2023** **5.5 Respons** **ISO/IEC 27035-3:2020** **11 Operasi kontainmen, eradikasi dan pemulihan insiden**

5.27 Belajar dari insiden keamanan informasi Kontrol: Pengetahuan yang diperoleh dari insiden keamanan informasi harus digunakan untuk memperkuat dan meningkatkan kontrol keamanan informasi.	**ISO/IEC 27035-1:2023** **5.6 Pembelajaran** **ISO/IEC 27035-2:2023** **12 Pembelajaran**
5.28 Pengumpulan bukti Kontrol: Organisasi harus menetapkan dan mengimplementasikan prosedur untuk identifikasi, pengumpulan, akuisisi dan preservasi bukti yang terkait dengan peristiwa keamanan informasi.	**ISO/IEC 27035-1:2023** **5.3 Deteksi dan pelaporan** d), i) **5.4 Asesmen dan pengambilan keputusan** i), l) **5.5 Respons** f), j), m)

Lampiran D
(informatif)
Pertimbangan atas situasi yang ditemukan selama investigasi insiden

Dalam respons insiden, terdapat situasi yang menantang di mana koordinator insiden dapat memainkan peran penting dalam mengontrol dan memajukan proses investigasi. Hal-hal berikut menyediakan potensi situasi dan tindakan yang dapat diambil oleh koordinator insiden.

Dalam hal insiden, permasalahan yang berbeda dapat muncul:

a) Tidak ada permasalahan mendasar ditemukan, dan alur respons sebagaimana yang diperkirakan, di dalam jangka waktunya. Laporan merekam semua informasi yang berguna untuk masa depan.

b) Penemuan atas satu atau lebih permasalahan mendasar. Koordinator insiden memutuskan apakah akan memanggil tim lain yang lebih terspesialisasi atau tidak. Penyelesaian terjadi:

   — sebelum jangka waktu berakhir: laporan merekam semua informasi yang berguna untuk masa depan;

   — kemungkinan besar di luar jangka waktu: koordinator insiden menginformasikan tim/entitas yang ditarget/terdampak bersama dengan manajer krisis supaya mereka dapat menyiapkan aksi/reaksi.

c) Penemuan atas permasalahan mendasar atau potensi korban (atau yang terdampak) internal atau eksternal yang dapat ditangani oleh tim respons yang telah diaktifkan. Koordinator insiden menginformasikan:

   — manajemen dari kemungkinan perpanjangan dan potensi kegagalan untuk diselesaikan dalam jangka waktu yang ditentukan; ini memungkinkan untuk komunikasi internal;

   — entitas yang berhak berkomunikasi dengan pihak luar organisasi [layanan pers, petugas proteksi data (*data protection officer*/DPO), dll.] jika diperintahkan demikian.

d) Penemuan atas permasalahan mendasar atau potensi korban (atau yang terdampak) internal atau eksternal yang dapat ditangani oleh tim respons yang telah diaktifkan. Koordinator insiden menginformasikan:

   — manajemen untuk mengaktifkan koordinator insiden lainnya. Koordinasi yang erat sebaiknya kemudian terbangun antara kapabilitas berbeda dan tim respons khusus lain yang diaktifkan (misalnya keamanan fisik, asistensi eksternal, dll.);

   — entitas yang berhak berkomunikasi dengan pihak luar organisasi [layanan pers, DPO, dll.].

e) Penemuan berbagai permasalahan yang terkait dengan SLA. Koordinator insiden mengeskalasi ke manajer krisis, yang bertanggung jawab untuk:

   — menginformasikan manajemen;

   — memberi kontrol ke manajer krisis;

— tetap terinformasi mengenai proses insiden (koordinator insiden mengambil tindakan ketika diperlukan tanpa menunggu informasi);

— mengaktifkan, berdasarkan permintaan, tim-tim yang dikontrolnya;

— tetap bersiap untuk mengambil kontrol kembali ketika krisis berakhir.

Information technology — Information security incident management — Part 1: Principles and process

1 Scope

This document is the foundation of the ISO/IEC 27035 series. It presents basic concepts, principles and process with key activities of information security incident management, which provide a structured approach to preparing for, detecting, reporting, assessing, and responding to incidents, and applying lessons learned.

The guidance on the information security incident management process and its key activities given in this document are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance according to their type, size and nature of business in relation to the information security risk situation. This document is also applicable to external organizations providing information security incident management services.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following 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
incident management team
IMT

team consisting of appropriately skilled and trusted members of an organization responsible for leading all information security incident management activities, in coordination with other parties both internal and external, throughout the incident lifecycle

Note 1 to entry: The head of this team can be called the incident manager who has been appointed by top management to adequately respond to all types of incidents.

3.1.2
incident response team
IRT

team of appropriately skilled and trusted members of an organization that responds to and resolves incidents in a coordinated way

Note 1 to entry: There can be several IRTs, one for each aspect of the incident.

Note 2 to entry: Computer Emergency Response Team (CERT[1]) and Computer Security Incident Response Team (CSIRT) are specific examples of IRTs in organizations and sectorial, regional, and national entities wanting to coordinate their response to large scale ICT and cybersecurity incidents.

3.1.3
incident coordinator

person responsible for leading all *incident response* (3.1.9) activities and coordinating the *incident response team* (3.1.2)

Note 1 to entry: An organization can decide to use another term for the incident coordinator.

3.1.4
information security event

occurrence indicating a possible breach of information security or failure of controls

3.1.5
information security incident

related and identified *information security event(s)* (3.1.4) that can harm an organization's assets or compromise its operations

3.1.6
information security incident management

collaborative activities to handle *information security incidents* (3.1.5) in a consistent and effective way

3.1.7
information security investigation

application of examinations, analysis and interpretation to aid understanding of an *information security incident* (3.1.5)

[SOURCE: ISO/IEC 27042:2015, 3.10, modified — “information security” was added to the term and the phrase “an incident” was replaced by “an information security incident” in the definition.]

[1] CERT is an example of a suitable product available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC of this product.

3.1.8
incident handling

actions of detecting, reporting, assessing, responding to, dealing with, and learning from *information security incidents* (3.1.5)

3.1.9
incident response

actions taken to mitigate or resolve an *information security incident* (3.1.5), including those taken to protect and restore the normal operational conditions of an information system and the information stored in it

3.1.10
point of contact
PoC

defined organizational function or role serving as the coordinator or focal point of information concerning incident management activities
Note 1 to entry: The most obvious PoC is the role to whom the information security event is raised.

3.2 Abbreviated terms

BCP	business continuity planning
CERT	computer emergency response team
CSIRT	computer security incident response team
DRP	disaster recovery planning
ICT	information and communications technology
IMT	incident management team
IRT	incident response team
ISMS	information security management system
PoC	point of contact
RPO	recovery point objective
RTO	recovery time objective

4 Overview

4.1 Basic concepts

Information security events and incidents may happen due to several reasons:
— technical/technological, organizational or physical vulnerabilities, partly due to incomplete implementations of the decided controls, are likely to be exploited, as complete elimination of exposure or risk is unlikely;

— humans can make errors;

— technology can fail;

— risk assessment is incomplete and risks have been omitted;

— risk treatment does not sufficiently cover the risks;

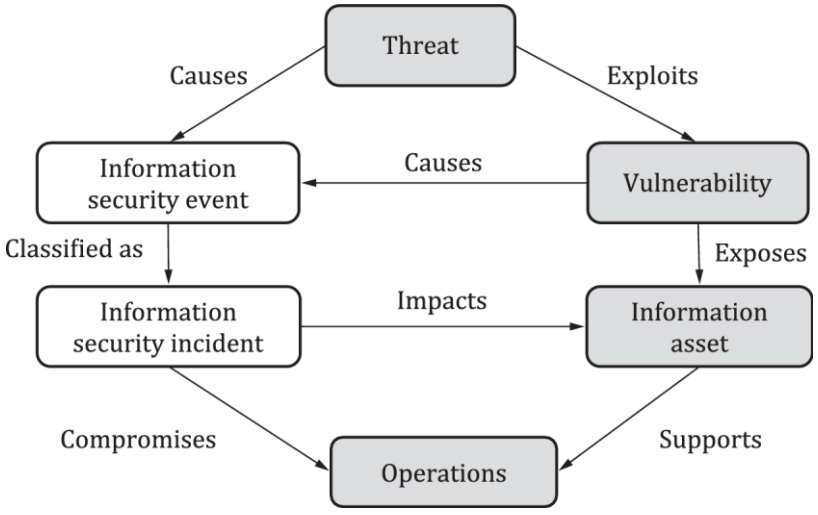
— changes in the context (internal and/or external) so that new risks exist or treated risks are no longer sufficiently covered.

The occurrence of an information security event does not necessarily mean that an attack has been successful or that there are any implications on confidentiality, integrity or availability, i.e. not all information security events are classified as information security incidents.

Information security incidents can be deliberate (e.g. caused by malware or breach of discipline), accidental (e.g. caused by inadvertent human error) or environmental (e.g. caused by fire or flood) and can be caused by technical (e.g. computer viruses) or non-technical (e.g. loss or theft of hardcopy documents) means. Incidents can include the unauthorized disclosure, modification, destruction, or unavailability of information, or the damage or theft of organizational assets that contain information.

Annex B provides descriptions of selected examples of information security incidents and their causes for informative purposes only. It is important to note that these examples are by no means exhaustive.

A threat exploits vulnerabilities (weaknesses) in information systems, services, or networks, causing the occurrence of information security events and thus potentially causing incidents to information assets exposed by the vulnerabilities. Figure 1 shows the relationship of objects in an information security incident.



NOTE The shaded objects are pre-existing, affected by the unshaded objects that result in an information security incident.

Figure 1 — Relationship of objects in an information security incident

Coordination is an important aspect in information security incident management. Many incidents cross organizational boundaries and cannot be easily resolved by a single

organization or, a part of an organization where the incident has been detected. Organizations should commit to the overall incident management objectives. Incident management coordination is required across the incident management process for multiple organizations to work together to handle information security incidents. This is for example the role of CERTs and CSIRTs. Information sharing is necessary for incident management coordination, where different organizations share threat, attack, and vulnerability information with each other so that each organization's knowledge benefits the other. Organizations should protect sensitive information during information sharing and communication. See ISO/IEC 27010 for further details.

It is important to indicate that resolving an information security incident should be done within a defined time frame to avoid unacceptable damage or a resulting catastrophe. This resolution delay is not as important in case of an event, vulnerability or a non-conformity.

4.2 Objectives of incident management

As a key part of an organization's overall information security strategy, the organization should put controls including procedures in place to enable a structured well-planned approach to the management of information security incidents. From an organization's perspective, the prime objective is to avoid or contain the impacts of information security incidents in order to minimize the direct and indirect damage to its operations caused by the incidents. Since damage to information assets can have a negative consequence on operations, business and operational perspectives should have a major influence in determining more specific objectives for information security incident management.

More specific objectives of a structured well-planned approach to incident management should include the following:

a) information security events are detected and efficiently dealt with, in particular deciding whether they should be classified as information security incidents;

b) identified information security incidents are assessed and responded to in the most appropriate and efficient manner and within the predetermined time frame;

c) the adverse impact(s) of information security incidents on the organization and involved parties and their operations are minimized by appropriate controls as part of incident response;

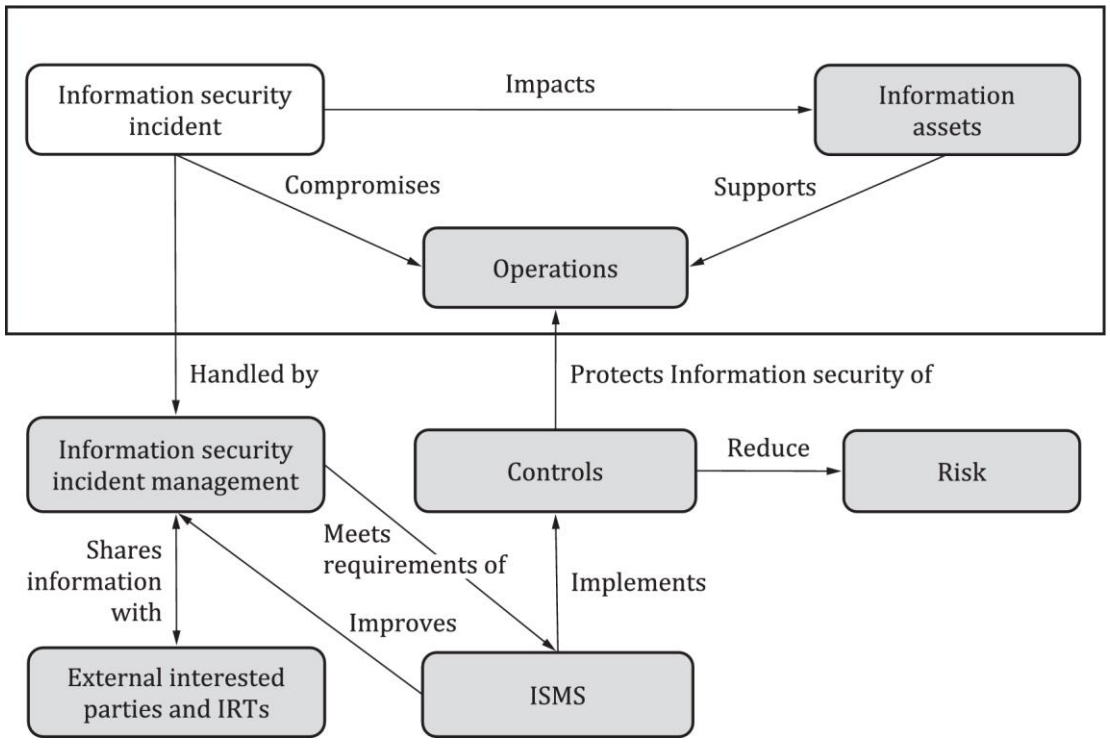
d) a link with relevant elements from crisis management and business continuity management through an escalation process is established. There is a need for a swift transfer of responsibility and action from incident management to crisis management when the situation requires it, with this order reversed once the crisis is resolved to allow for a complete resolution of the incident;

e) information security vulnerabilities involved with or discovered during the incident are assessed and dealt with appropriately to prevent or reduce incidents. This assessment can be done either by the incident response team (IRT) or other teams within the organization and involved parties, depending on duty distribution;

f) lessons are learnt quickly from information security incidents, related vulnerabilities and their management. This feedback mechanism is intended to increase the chances of preventing future information security incidents from occurring, improve the implementation and use of information security controls, and improve the overall information security incident management plan.

To help achieve these objectives, organizations should ensure that information security incidents are documented in a consistent manner, using appropriate standards or procedures for incident categorization, classification, prioritization and sharing, so that metrics can be derived from aggregated data over a period of time. This provides valuable information to aid the strategic decision making process when investing in information security controls. The information security incident management system should be able to share information with relevant internal and external parties.

Another objective associated with this document is to provide guidance to organizations that aim to meet the information security management system (ISMS) requirements specified in ISO/IEC 27001 which are supported by guidance from ISO/IEC 27002. ISO/IEC 27001 includes requirements related to information security incident management. Table C.1 provides cross-references on information security incident management clauses from ISO/IEC 27001 and clauses in this document. ISMS relationships are also explained in Figure 2. This document can also support the requirements of information security management systems that do not follow ISO/IEC 27001.



NOTE See also Figure 1.

Figure 2 — Information security incident management in relation to ISMS and applied controls

4.3 Benefits of a structured approach

Using a structured approach to information security incident management can yield significant benefits, which can be grouped under the following topics.

a) Improving overall information security

To ensure adequate identification of and response to information security events and incidents, it is a prerequisite that there be a structured process for planning and preparation, detection, reporting and assessment, and relevant decision-making. This improves overall security by

helping to quickly identify and implement a consistent solution, and thus provides a means of preventing similar information security incidents in the future. Furthermore, benefits are gained by metrics, sharing and aggregation. The credibility of the organization can be improved by the demonstration of its implementation of best practices with respect to information security incident management.

b) Reducing adverse business consequences

A structured approach to information security incident management can assist in reducing the level of potential adverse business consequences associated with information security incidents. These consequences can include immediate financial loss and longer-term loss arising from damaged reputation and credibility. For further guidance on consequence assessment, see ISO/IEC 27005. For guidance on information and communication technology readiness for business continuity, see ISO/IEC 27031.

c) Strengthening the focus on information security incident prevention

Using a structured approach to information security incident management helps to create a better focus on incident prevention within an organization, including the development of methods to identify new threats and vulnerabilities. Analysis of incident-related data enables the identification of patterns and trends, thereby facilitating a more accurate focus on incident prevention and identification of appropriate actions and controls to prevent further occurrence.

d) Improving prioritization

A structured approach to information security incident management provides a solid basis for prioritization when conducting information security incident investigations, including the use of effective categorization and classification scales. If there are no clear procedures, there is a risk that investigation activities may be conducted in an overly reactive mode, responding to incidents as they occur and overlooking what activities should be handled with a higher priority.

e) Supporting evidence collection and investigation

If and when needed, clear incident investigation procedures help to ensure that data collection and handling are evidentially sound and legally admissible. These are important considerations if legal prosecution or disciplinary action follows. For more information on digital evidence and investigation, see the investigative standards in Annex A.

f) Contributing to budget and resource justifications

A well-defined and structured approach to information security incident management helps to justify and simplify the allocation of budgets and resources for involved organizational units. Furthermore, benefit accrues for the information security incident management plan itself, with the ability to better plan for the allocation of staff and resources.

One example of a way to control and optimize budget and resources is to add time tracking to information security incident management tasks to facilitate quantitative assessment of the organization's handling of information security incidents. It can provide information on how long it takes to resolve information security incidents of different priorities and on different platforms. If there are bottlenecks in the information security incident management process, these should also be identifiable.

g) Improving updates to information security risk assessment and treatment results

The use of a structured approach to information security incident management facilitates:

— better collection of data for assisting in the identification and determination of the characteristics of the various threat types and associated vulnerabilities, and

— provision of data about frequencies of occurrence of the identified threat types, to assist with analysis of control efficacy (i.e. identify controls that failed and resulted in a breach, with uplift of such controls to reduce reoccurrence).

The data collected about adverse impacts on business operations from information security incidents is useful in business impact analysis. The data collected to identify the frequency of various threat types can improve the quality of a threat assessment. Similarly, the data collected on vulnerabilities can improve the quality of future vulnerability assessments. For guidance on information security risk assessment and treatment, see ISO/IEC 27005.

h) Providing enhanced information security awareness and training programme material

A structured approach to information security incident management enables an organization to collect experience and knowledge of how the organization and involved parties handle incidents, which is valuable material for an information security awareness programme. An awareness programme that includes lessons learned from real experience helps to reduce mistakes or confusion in future information security incident handling and improve potential response times and general awareness of reporting obligations.

i) Providing input to the information security policy and related documentation reviews

Data provided by the practice of a structured approach to information security incident management can offer valuable input to reviews of the effectiveness and subsequent improvement of incident management policies (and other related information security documents). This applies to topic-specific policies and other documents applicable both for organization-wide and for individual systems, services and networks.

4.4 Adaptability

The guidance provided by the ISO/IEC 27035 series is extensive and, if adopted in full, can require significant resources to operate and manage. It is therefore important that an organization applying this guidance should retain a sense of perspective and ensure that the resources applied to information security incident management and the complexity of the mechanisms implemented are proportional to the following:

a) size, structure and business nature of an organization including key critical assets, processes, and data that should be protected;

b) scope of any information security management system for incident handling;

c) potential risk due to incidents;

d) the goals of the business.

An organization using this document should therefore adopt its guidance in a manner that is relevant to the scale and characteristics of its business.

4.5 Capability

4.5.1 General

Information security incidents can jeopardize achievement of business objectives and generate

crises. Following the risk assessment, it is possible to delineate between situations whose likelihood is medium to high, and consequence low to medium, and those whose likelihood is (very) rare and consequences very high. The second situation represents crises that are not always possible to completely prevent and, in some cases, disrupts the decision chain. ISO/IEC 27031 provides guidance on information communication technology (ICT) readiness for business continuity to support business operations in the event of emerging information security events and incidents, and related disruptions.

The overarching objectives of crisis management are:

— to protect human life including critical infrastructure to the extent necessary;

— to support continuity of everyday activity;

— to protect assets including property and the natural environment, as far as possible.

No two crises are the same. These objectives are underpinned by the following principles:

— Coordination: effective coordination and communication facilitates information sharing.

— Continuity: prevention, preparedness, response and recovery to crises should be grounded in the existing functions of organisations and familiar ways of working.

— Proportionality: crisis management should be calibrated to the magnitude and nature of the crisis.

— Accountability: decision-making and actions are transparent and accountable.

— Integration: prevention, preparedness, response and recovery should be considered as elements of a continuum that may occur concurrently.

Information security incident management requires a capability to ensure coherency of management to achieve efficient and effective incident handling. This capability should be established by incident management policy, plan, process and procedure, as well as properly structured team, skilled people, information sharing and coordination with other parties both internal and external.

4.5.2 Policies, plan and process

The organization’s policies for information security management should consider how information security incident management aligns with risk management. To achieve this, the organization should identify, as part of the risk management process, the list of events/incidents they want to counter and control, with ensuring as minimal impact as possible on the business operations and objectives.

Incident management requires a defined process approved by the top management that includes flows of actions (or procedures) to be performed at all phases of the process and a communication protocol with appropriate channels.

4.5.3 Incident management structure

To allow a coherent response to the events and incidents, organizations should institute an incident management capability that prepares the information security incident management policy and describes the incident response structure. Organizations should also ensure that the directives and resources exist to adequately respond to the incidents.

a) Incident management team

An incident management team (IMT) consists of appropriately skilled and trusted members of an organization with the role of leading all information security incident management activities, in coordination with other parties, both internal and external, throughout the incident life cycle. IMT provides all necessary services to cope with incidents, not only preparing for, detecting, reporting, assessing, and responding to incidents, but also threat and vulnerability detection, advisory, information sharing, learning lessons, improvement, education and awareness. IMT can introduce any necessary resources at any time in order to provide these services.

The organization should determine and allocate roles and responsibilities to handle, coordinate and respond to the incidents. This includes:

b) Point of contact

The point of contact (PoC) is the role, address or person which personnel can turn to when they discover anomalies and what is considered as an event in the policy and awareness sessions. Depending on the nature and size of the organizations, there can be more than one PoC. For example, one for ICT issues and one for physical, organizational and procedural situations, which is similar to what already exists for accidents, fire and other damaged equipment.

c) Incident coordinator who:

— coordinates and manages event notifications and alerts that are raised either by information systems or individuals,

— performs the evaluation of the event and declares the incident,

— activates the IRT(s) and coordinates its/their activities,

— records all information on the incident and its resolution,

— completes and sends the incident report, with their proposals for improvement,

— coordinates with internal and external organisations following the IMT’s direction with respect of incident handling.

NOTE The organization can decide to use another term for the incident coordinator.

The incident coordinator allocated should maintain control for the whole duration of the incident. Where an incident goes beyond the work shift and requires someone to remain present/available, another incident coordinator should take over with all the necessary information and authority.

If a call to the BCP (business continuity planning)/DRP (disaster recovery planning) coordinator or team is required, the incident coordinator should remain informed, and resume managing the incident upon crisis resolution, as to complete resolution.

d) Incident response teams (IRTs) that:

— perform the “procedures” to respond to the incident,

— detect the root cause(s) and hidden vulnerabilities,

— resolve the incident,

— report to the incident coordinator.

e) Change management team that decides on the actions to be taken to improve the incident prevention and response.

f) Awareness and training team that prepares the programme and sessions aimed to identify and report unwanted events.

g) Vulnerability management team that analyses the vulnerabilities detected during the incident response and provides its recommendations to the change management team.

h) Crisis management team that ensures the coordination with the BCP/DRP coordinator or team.

i) Security monitoring team that updates the monitoring and detection system rules in application of a decision following lessons learned, and monitors for reoccurrence of similar incidents.

4.6 Communication

Organizations should communicate the approved information security incident management policies to interested parties. This includes both internal staff and external parties with access to the organization's information. The organization should communicate the following:

— the organization's information security incident policies and relevant procedures;

— obligations/expectations of personnel;

— incident reporting procedures;

— who to contact for more information;

— outcomes of incidents and how to minimize reoccurrence.

The organization should promote incident management as a "no-fault" reporting process to empower personnel to come forward and report incidents without the fear of retribution. Focus should instead be on the positive outcomes that an organization can gain from receiving incident reporting, learning and improving from incidents to become more secure and resilient. Reporting of incidents is "no-fault" in the first instance i.e. no fault or blame will be associated with a reported incident. Following investigation, sanctions may occur if the incident is found to be the result of intentional violation of the organization's policies and procedures, or in repeated instances of misconduct or negligence.

Communication is essential to control the messaging surrounding the incident including where, when, what and how this messaging is delivered, both to provide the appropriate response and to satisfy organizational or societal needs. Internal communication is necessary for an effective response and recovery, and external communication is indispensable e.g. for company image.

NOTE An information breach (aka uncontrolled communication) about an incident can have serious consequences.

Only duly mandated and prepared personnel should be allowed to communicate with the external world as to only tell what is necessary, at the best moment and in the appropriate form.

4.7 Documentation

4.7.1 General

It is crucial to document as much information as possible related to the event/incident from its detection through to its resolution. The incident report is the synthesis of all this information.

4.7.2 Event report

The event report should contain all that is necessary to understand the event and make a decision regarding whether to classify the event as an incident. This includes:

a) date and time of the detection;

b) name of informant which can however be hidden to keep confidentiality;

c) all circumstances and facts for comprehension of the event.

4.7.3 Incident management log

All information gathered during the incident response should be documented/recorded/logged to serve as a record of actions i.e. date/time and corresponding action/decision.

4.7.4 Incident report

The incident report is the synthesis of all gathered information throughout the incident life cycle. It serves to analyse and evaluate the incident, and decide if changes are planned for incident management capability (see also 4.5).

A pre-formatted template document for incident reports should be prepared to ensure no essential information is missed or overlooked.

4.7.5 Incident register

All information security incidents should be recorded in a centrally managed incident register. This register provides the IMT with an overview of the incidents that have occurred in the organization, their status, and any follow up activities. It can also be used by the IMT to provide reports to top management regarding trends and themes around the threat environment and feed into organizational planning and risk assessments.

5 Process

5.1 Overview

To achieve the objectives outlined in 4.2, information security incident management process consists of five distinct phases:

— plan and prepare (see 5.2);

— detect and report (see 5.3);

— assess and decide (see 5.4);

— respond (see 5.5);

— learn lessons (see 5.6).

A high-level view of these phases is shown in Figure 3.

Some activities can occur in multiple phases or throughout the incident handling process. Such activities include the following:

— documentation of event and incident evidence and key information, response actions taken, and follow-up actions done as part of the incident handling process;

— coordination and communication between the involved parties;

— notification of significant incidents to management and other interested parties;

— information sharing between interested parties and internal and external collaborators such as vendors and other IRTs.

The time considerations for each step in the event/incident management process should be:

a) Detection: as soon as possible

b) Reporting: complete required forms without unnecessary delay, or via automated methods.

c) Response: as soon as possible to start the response before the damages (impacts and consequences) exceed the organizationally-determined limits to avoid having a situation that requires taking BCP/DRP measures. Acceptable limits should be well defined in BCP and known by everyone. Each type of incident may therefore have a different path for or mode of resolution.

d) Communication

   — Internal: to adopt, as soon as possible, measures and behaviours and prevent prolonging of the incident

   — External: to receive, as soon as possible, the necessary help from relevant external intervening parties, and notify the interested parties

e) Escalation: within an organizationally-determined interval and/or before impacts exceed organizationally-determined limits

f) Notification: within an organizationally-determined interval or any legally required interval.

All actions should be performed and monitored with no unnecessary delay.

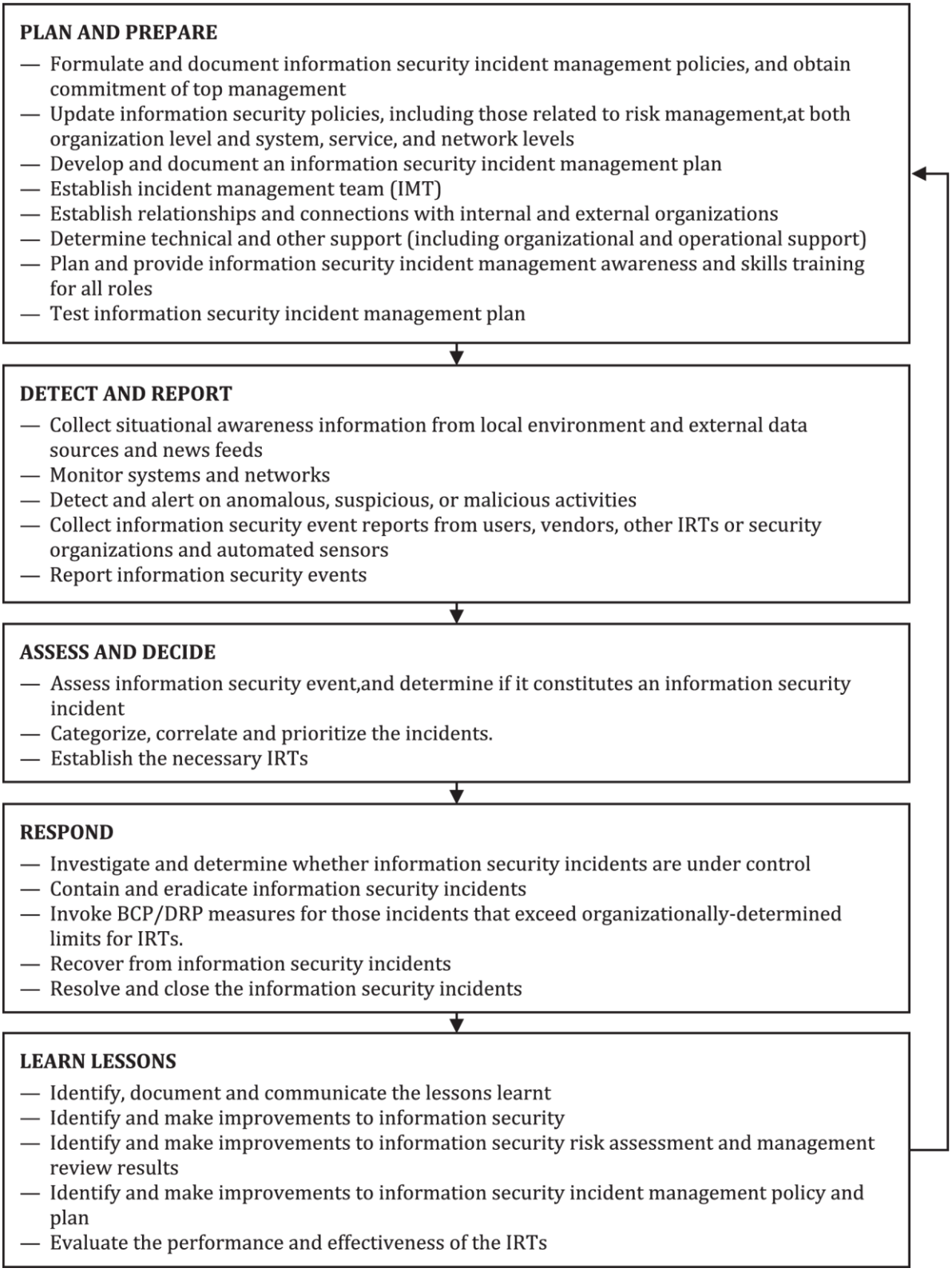


Figure 3 — Information security incident management phases

Figure 4 shows the flow of information security events and incidents through information security incident management phases and related activities.

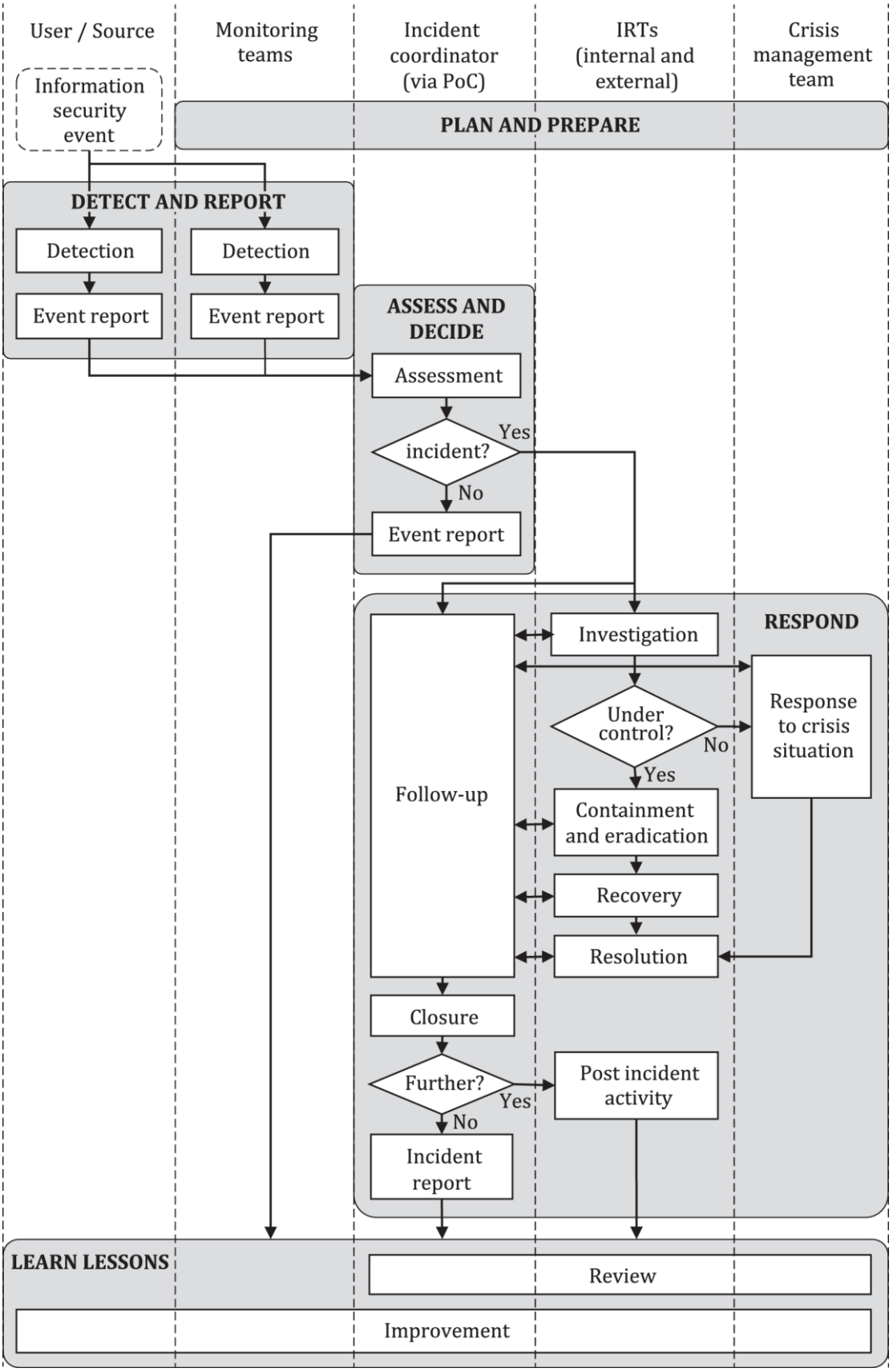


Figure 4 — Information security event and incident flow diagram

5.2 Plan and prepare

Effective information security incident management requires appropriate planning and preparation. It is essential to keep calm at all stages of incident response, and that this response time is controlled and mastered. If it is not, prolonged incident duration may increase adverse impact to the organization. This response time should be computed as a portion of the recovery time objective (RTO, see ISO/IEC 27031:2011, 3.13 and 6.3) and should take into consideration the inevitable delay necessary for detection, reporting and assessment.

For an efficient and effective information security incident management plan to be put into operation, an organization should complete a number of preparatory activities in support of the incident management requirements of ISMS, namely:

a) formulate and document information security incident management policies and obtain commitment of top management, including purpose, objectives and scope of policies, categories and criteria for determining and prioritizing incidents, organizational structure and setting of roles, responsibilities and authorities for incident management, performance measures, reporting and contact forms;

b) update information security policies, including those related to risk management, at both organization level and system, service or network level;

c) develop and document a detailed information security incident management plan, including procedures and methods for incident handling, communications and information sharing, by which to establish incident management capability. The organization should

   — define information security event/incident indicators and precursors;

   — list possible events/incidents that the organization wants to be able to control. This list is mainly based on the result of the risk assessment. An event/incident is a risk that becomes real;

   — formulate the format and content of the incident report. This enables consistent reporting regardless of the individual filling in the form and is important for lessons learned as well as determining common themes and trends for reporting up to management;

   — define/establish incident categories;

   — establish handover procedures for handover to law enforcement when administrative incidents (e.g. policy violation) become criminal incidents (e.g. fraud);

   — document the evaluation procedure to declare an incident;

   — determine the information and responsibility exchange with the crisis management team (BCP/DRP) in both directions;

   — establish an incident management team that gathers all the skills necessary to prepare the incident response plan;

   — establish a decision/command structure and an emergency call tree;

   — provide essential internal and external contact points (e.g. legal);

— set up an incident response team(s) (IRT) whose role is to respond to and resolve the incident. Several IRTs can exist with specific skills to respond to specific incidents. More information can be found in ISO/IEC 27035-2:2023, 7.3.

d) determine the IRT, with its functions and services, and an appropriate training programme designed, developed, and provided to its personnel. The response teams should know what to do, which resources to use and in which time frames. It is essential that the personnel is trained to perform with efficiency and ability to work under pressure.

e) establish and preserve appropriate relationships and connections with internal and external organizations that are directly involved in information security event, incident, threat and vulnerability management, and communicate information security incident management policies and procedures to them;

f) establish, implement and operate technical, organizational and operational mechanisms to support the information security incident management plan. Develop and deploy necessary information systems to support the incident response, including an information security incident register. These mechanisms and systems are intended to prevent information security incident occurrences or reduce the likelihood of occurrences of information security incidents;

g) design and develop an awareness and training programme for information security event, incident and vulnerability management;

h) test the use of the information security incident management plan, its processes and procedures.

With this phase completed, organizations should be fully prepared to properly manage information security incidents. ISO/IEC 27035-2:2023, Clauses 4 to 11, describes each of the activities listed above, including the contents of policy and planning documents.

5.3 Detect and report

The second phase of information security incident management involves the detection of, collection of information associated with, and reporting on, occurrences of information security events and the discovered or involved information security vulnerabilities, by manual or automatic means. In this phase, events and vulnerabilities cannot yet be classified as information security incidents.

It is likely that several channels exist for reporting security events to the adequate point of contact (PoC) using the event report. While some ICT and technical events are reported to an ICT department, other issues, such as privacy breaches, may be raised to other departments of the organization. The organization should have procedures in place to distribute the event reports to the incident coordinator to enable coordination and overview of all information security incidents. The incident coordinator should coordinate these different inputs with other departments of the business. Police, ambulances, fire brigades and other emergency services are sometimes reached at different telephone numbers. Further, the communication channels can be different: telephone, fax, beeper, email, automated alarm in ICT systems, mobile push notification, (operator's) dashboard, etc.

The entity that detects the situation is not always the one that suffers from its consequences (e.g. a security agent detecting an intrusion and a theft in offices, a fire in a house detected by a neighbour). It is important to consider the concept of targeted or impacted business team/entity, which is the business activity and more exactly the personnel/entity who performs it and its related management.

The reporting of security events in line with the organization's reporting policies enables later analysis if required.

For the detect and report phase, an organization should undertake the following key activities:

a) monitor by monitoring systems or monitoring teams (e.g. watching for camera images) and log system and network activity as appropriate;
b) detect and report the occurrence of an information security event or the existence of related vulnerabilities and threats, whether manually by personnel or automatically;

c) collect information on an information security event or related vulnerabilities and threats;

d) collect situational awareness information from internal and external data sources including local system and network traffic and activity logs, news feeds concerning ongoing political, social, or economic activities that can impact incident activity, external feeds on incident trends, new attack vectors, indicators of compromise and new mitigation strategies and technologies;

e) perform external/internal threat analysis to establish an understanding of the threat environment and in turn detect changes;

f) determine and include the reliability and quality of the information being analysed of the threat assessments;

g) perform regular analysis for vulnerabilities and attack vectors, based on the existing and potential threats;

h) ensure that all detection activities and results are properly logged for later analysis;

i) ensure that digital evidence is gathered and stored securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action. For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards listed in Annex A;

j) inform, on an as-needed basis throughout the phase, for further review or decisions.

All information collected pertaining to an information security event or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as possible at the time. This supports assessments, decisions and actions to be taken.

5.4 Assess and decide

The third phase of information security incident management involves the assessment of information associated with occurrences of information security events and the decision on whether to classify events as information security incidents. The incident coordinator evaluates the event based on the event report and the criteria defined during the plan and prepare phase and declare if it is an incident or not.

Once an information security event has been detected and reported, the subsequent activities should be performed.

a) Distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with assessment, decision making and actions involving both security and non-security personnel.

b) Provide formal procedures for each notified person to follow, including reviewing and amending reports, assessing damage, and notifying relevant personnel. Individual actions depend on the type and severity of the incident.

c) Use guidelines for thorough documentation of an information security event and the subsequent actions for an information security incident if the information security event becomes classified as an information security incident.

d) Evaluate whether the event is an incident or not, correlate the event for reoccurrence and retrieve data from prior actions and responses. The type and time frame for resolution depends on this decision based on factors decided during the plan and prepare phase. The decision criteria should be clear and tested, considering technological, business and human aspects. Prioritize all information security incidents according to relevant internal documentation.

e) Communicate through the established and already activated channels and protocols to the IRT(s) and to business management, when needed.

f) Call to the response team(s) necessary to respond and resolve the various problems identified during detection and the information provided by the finder/reporter.

g) Gather information of the targeted or affected teams.

h) Start the timer for the response.

It is crucial that a decision to declare an event as an information security incident is made rapidly as it allows the rapid designation of the IRT and setting the “count-down” process to make sure the incident is resolved within the expected time frame. Decision tables should have been prepared during the plan and prepare phase.

For the assess and decide phase, an organization should perform the following key activities:

i) Collect information that can include testing, measuring, and other data gathering about the detection of an information security event. The type and amount of information collected will depend on the information security event that has occurred.

j) Conduct an assessment by the incident coordinator to determine whether the event is a possible or confirmed information security incident or a false alarm. A false alarm (i.e. a false positive) is an indication of a reported event that is found not to be real or of any impact. If desired, the IRT can conduct a quality review to ensure that the incident coordinator correctly declared an incident.

k) Log all activities, results and related decisions for later analysis and recordkeeping.

l) Ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security incident register up to date.

All information collected pertaining to an information security event/incident or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as

possible at the time. This supports assessments, decisions and actions to be taken.

5.5 Respond

The fourth phase of information security incident management involves responding to information security incidents in accordance with the decision in the assess and decide phase, and the procedures described in the response plan elaborated during the plan and prepare phase. Depending on the decisions, the responses can be made immediately, in real-time, or in near real-time, and some responses can involve information security investigation. The incident coordinator is the key role to coordinate the activities of the IRT(s) and monitor the response timer.

Each type of incident will receive its specific response. Depending on what is discovered by the IRT(s) during activation, the incident response may take various/different paths to recovery and may require varying/differing resources.

The information security incident coordinator is kept up to date at a frequency commensurate with incident severity, and may make decisions to contact other teams with specific skills depending on the need to respond to the discovered incident or repair/restore the defective, damaged or destroyed assets (physical, material, software, procedural, organizational, etc.).

When responding to an event rather than an incident, generally, an event is solved within the normal business processes, as there is no emergency or immediate danger.

The incident coordinator keeps regular contact with the targeted/affected teams/entities of the incident and decides, with them, if the incident is resolved or not. It is to further ensure if sufficient resources are available to start business activities again. The situation can however require a more complete resolution, with complete restoration and resumption of capabilities and operations.

The incident coordinator prepares the incident report which should include:

— analysis of the situation;

— identification of the problem and, if possible, its cause;

— determination of the gravity/seriousness and the urgency to respond;

— inclusion in the change programme.

NOTE 1 If the incident resolution exceeds the work shift of the incident coordinator (e.g. more than 8 hours to several days), the initial incident coordinator gathers all received information and notes taken by all involved incident coordinator(s) as to produce the final report. He/she remains the main incident coordinator.

The response procedure to be followed requires:

— a clear definition of the incident to be managed and controlled;

— a list of necessary and required resources;

— a detailed chronology of the actions to be performed, with timing;

— the target resolution time frame;

— a list of contact points and channels for information with the criteria;

— the skills and size of the teams (with the necessary/required training);

— the presence of the resources.

Once an information security incident has been confirmed and the responses determined, the subsequent activities should be undertaken:

a) Distribute the responsibility for information security incident management activities through an appropriate hierarchy of personnel with decision making and actions, involving both security and non-security personnel as necessary.

b) Provide formal procedures for each involved person to follow, including reviewing and amending the reports, reassessing damage, and notifying the relevant personnel. Individual actions depend on the type and severity of the incident. For more information on ICT incident response, see ISO/IEC 27035-3:2020, Clauses 8, 9 and 11.

c) Reconsider the original assessment as additional information becomes available to identify whether the information security incident shall be re-prioritised, or response activities adjusted.

d) Use guidelines for thorough documentation of an information security incident and subsequent actions.

e) Evaluate the proposed resolution with targeted/affected teams/entities to ensure it meets the resolution criteria and expectations of all parties involved.

f) Investigate incidents as required and relative to the information security incident classification scale rating. The rating should be changed as necessary. Investigation can include different kinds of analyses to provide a more in-depth understanding of incidents.

g) Review by the incident coordinator and IRT to determine whether the information security incident is under control, and if so, perform the required response. If the incident is not under control, or will result in severe adverse impact to the organization, escalate it to the crisis management team. Escalation can result in action (response) at two different levels:

   — one that falls within the responsibility and authority of the incident coordinator (see 5.2 and 5.3) to, for example, call more response teams with different skills to cope with what is discovered (it is what happens in case of a fire when the emergency point of contact calls ambulances, police and other fire-fighter teams);

   — one that falls beyond the authority of the incident coordinator who then calls for another management level (e.g. involvement of another department in the organization, call for external support with financial consequences that requires the authorization by the finance department).

h) Assign internal resources and identify external resources in order to respond to an incident.

i) Ensure that all parties involved, particularly the IRT, properly log all activities for later analysis.

j) Ensure that digital evidence is gathered and stored provably securely, and that its secure preservation is continually monitored, in case the evidence is required for legal prosecution or internal disciplinary action.

Gathering digital evidence includes the following actions:

— provide frequent status updates to key stakeholders;

— gather, record, and maintain a chain of custody of evidence related to the incident;

— notify regulators of the incident (where applicable);

— update the incident register with incident closure details;

— follow any retention and preservation of evidence relating to the information security incident (legal and regulatory requirements can apply).

NOTE 2 For more detailed information on the identification, collection, acquisition and preservation of digital evidence, see the investigative standards listed in Annex A.

k) Ensure that the change control regime is maintained to cover information security incident tracking and incident report updates, and to keep the information security incident register up to date.

l) Follow pre-defined communication protocols and/or an engagement plan that identifies who has the authority to communicate to different stakeholders, and communicate the existence of the information security incident and share any relevant details (e.g. threat, attack, and vulnerability information) with other internal and external individuals or organizations, in accordance with organizational and incident management communication plans and information disclosure policies. It can be particularly important to notify asset owners (determined during the impact analysis) and internal and external organizations (e.g. other incident response teams, law enforcement agencies, Internet service providers, and information sharing organizations) that can assist with the management and resolution of the incident. Sharing information can also benefit other organizations since the same threats and attacks often affect multiple organizations. For further detail about information sharing, see ISO/IEC 27010.

m) After recovery from an incident, a post incident activity should be initiated depending on the nature and severity of the incident. This activity includes:

— investigation of the information pertaining to the incident,

— investigation of other relevant sources such as involved personnel,

— summarized report of the investigation findings.

n) Once the incident has been resolved, it should be closed according to the rules defined in the information security incident management policy and all interested parties should be notified.

All information collected pertaining to an information security event/incident, or related vulnerabilities and threats should be stored in the information security incident register managed by the IMT. The information reported during each activity should be as complete as possible at the time. This supports assessments, decisions and actions to be taken, including potential further analysis.

5.6 Learn lessons

The fifth phase of information security incident management occurs when information security incidents have been resolved. This phase involves learning lessons from how incidents, related vulnerabilities and threats have been handled.

Lessons can come from one or many information security incidents or reported security vulnerabilities. Improvements are aided by metrics fed into the organization's strategy on where to invest in information security controls. It is crucial that lessons learned are linked with the information security management change capability that makes the business decisions and, when deemed necessary, include the proposed modification in the information security management improvement process.

The incident report should indicate various situations leading to different actions to be forwarded to the information security management improvement process. The report should also make improvements to the information security incident management plan and its documentation based on the lessons learned.

For the learn lessons phase, an organization should perform the following key activities:

a) review how effective the processes, procedures, reporting formats and organizational structure were in responding to, assessing and recovering from information security incidents and dealing with information security vulnerabilities;

b) identify, document and communicate the lessons learned from information security incidents, related vulnerabilities and threats;

c) review, identify and make improvements to information security control implementation (new or updated controls), as well as information security incident management policy;

d) review, identify and make improvements to the organization's existing information security risk assessment and management reviews;

e) communicate and share the results of review within a trusted community (if the organization so wishes);

f) determine if the incident information, associated attack vectors and vulnerabilities may be shared with partner organizations to assist in preventing the same incidents from occurring in their environments. For more details, see ISO/IEC 27010 on information sharing;

g) perform a comprehensive evaluation of IRT performance and effectiveness on a periodic basis.

It is emphasized that information security incident management activities are iterative, and therefore an organization should make regular improvements to a number of information security elements over time. These improvements should be proposed on the basis of reviews of the data on information security incidents, responses, and reported information security vulnerabilities.

Annex D provides considerations of situations discovered during the investigation of an incident.

ISO/IEC 27035-2:2023, Clause 12 describes in detail each of the activities listed above.

Annex A
(informative)
Relationship to investigative standards

This document describes part of a comprehensive investigative process which includes, but is not limited to, the application of the following standards:

— ISO/IEC 27037

ISO/IEC 27037 describes the means by which those involved in the early stages of an investigation, including initial response, can ensure that sufficient potential digital evidence is captured to allow the investigation to proceed appropriately.

— ISO/IEC 27038

Some documents can contain information that should not be disclosed to some communities. Modified documents can be released to these communities after an appropriate processing of the original document. The process of removing information that shall not be disclosed is called “redaction”.

The digital redaction of documents is a relatively new area of document management practice, raising unique issues and potential risks. Where digital documents are redacted, removed information should not be recoverable. Hence, care shall be taken so that redacted information is permanently removed from the digital document (e.g. it should not be simply hidden within non-displayable portions of the document).

ISO/IEC 27038 specifies methods for digital redaction of digital documents. It also specifies requirements for software that can be used for redaction.

— ISO/IEC 27040

ISO/IEC 27040 provides detailed technical guidance on how organizations can define an appropriate level of risk mitigation by employing a well-proven and consistent approach to the planning, design, documentation and implementation of data storage security. Storage security applies to the protection (security) of information where it is stored and to the security of the information being transferred across the communication links associated with storage. Storage security includes the security of devices and media, the security of management activities related to the devices and media, the security of applications and services, and security relevant to end-users during the lifetime of devices and media and after end of use.

Security mechanisms like encryption and sanitization can affect one’s ability to investigate by introducing obfuscation mechanisms. They should be considered prior to and during the conduct of an investigation. They can also be important in ensuring that storage of evidential material during and after an investigation is adequately prepared and secured.

— ISO/IEC 27041

It is important that methods and processes deployed during an investigation can be shown to be appropriate. ISO/IEC 27041 provides guidance on how to provide assurance that methods and processes meet the requirements of the investigation and have been appropriately tested.

— ISO/IEC 27042

This document describes how methods and processes to be used during an investigation can be designed and implemented in order to allow correct evaluation of potential digital evidence, interpretation of digital evidence and effective reporting of findings.

— ISO/IEC 27043

This document defines the key common principles and processes underlying the investigation of incidents and provides a framework model for all stages of investigations.

— the ISO/IEC 27050 series

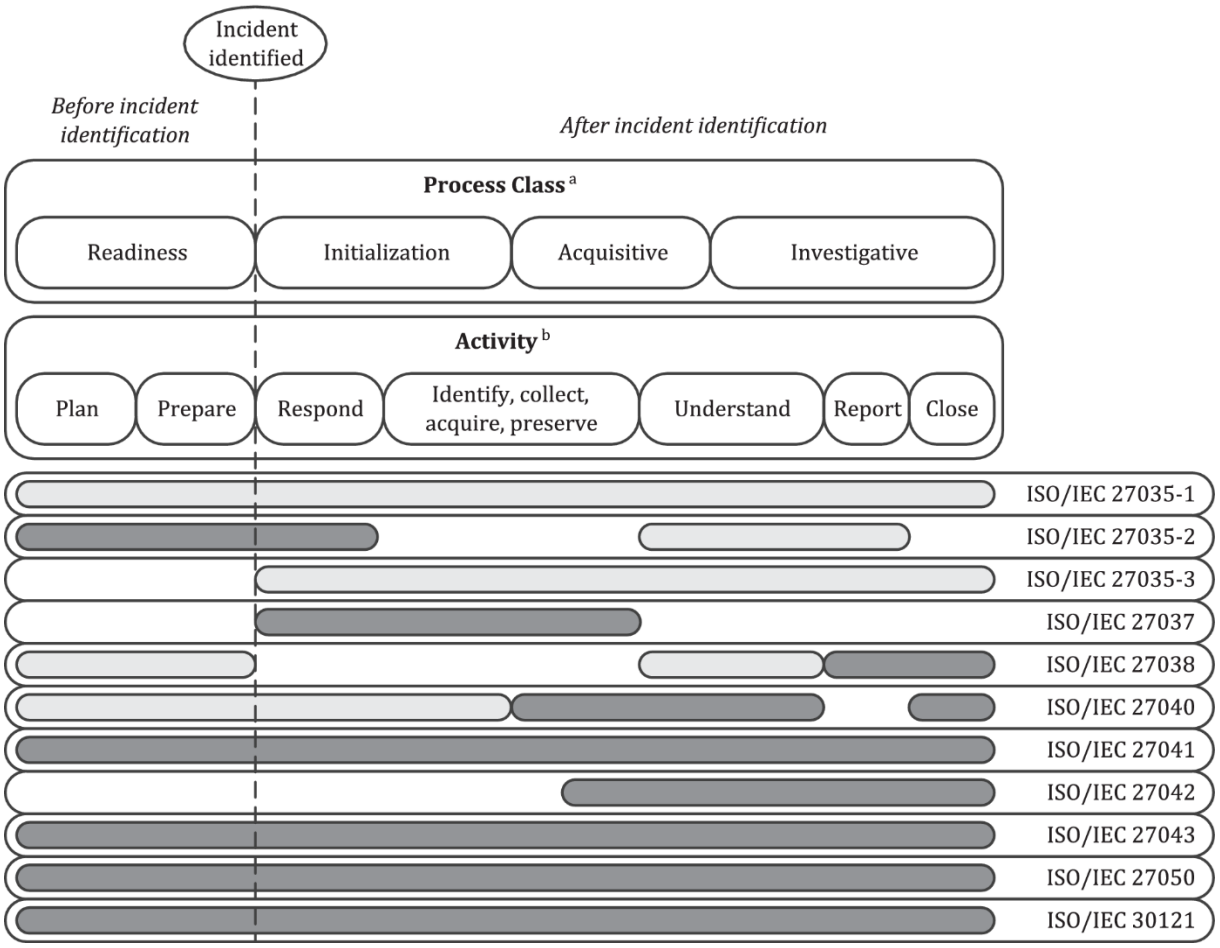
The ISO/IEC 27050 series addresses activities in electronic discovery, including, but not limited to identification, preservation, collection, processing, review, analysis, and production of Electronically Stored Information (ESI). In addition, it provides guidance on measures, spanning from initial creation of ESI through its final disposition, which an organization can undertake to mitigate risk and expense should electronic discovery become an issue. It is relevant to both non-technical and technical personnel involved in some or all of the electronic discovery activities.

Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities. In addition, the sensitivity and criticality of the data sometimes necessitate protections like storage security to guard against data breaches.

— ISO/IEC 30121

ISO/IEC 30121 provides a framework for governing bodies of organizations (including owners, board members, directors, partners, senior executives, or similar) on the best way to prepare an organization for digital investigations before they occur. ISO/IEC 30121 applies to the development of strategic processes (and decisions) relating to the retention, availability, access and cost effectiveness of digital evidence disclosure. ISO/IEC 30121 is applicable to all types and sizes of organizations. ISO/IEC 30121 is about the prudent strategic preparation for digital investigation of an organization. Forensic readiness ensures that an organization has made the appropriate and relevant strategic preparation for accepting potential events of an evidential nature. Actions can occur as the result of inevitable security breaches, fraud, and reputation assertion. In every situation Information Technology (IT) should be strategically deployed to maximize the effectiveness of evidential availability, accessibility and cost efficiency

Figure A.1 shows typical activities surrounding an incident and its investigation. The document reference numbers shown in this figure (e.g. ISO/IEC 27037) indicate the documents listed above and the shaded bars show where each is most likely to be directly applicable or has some influence over the investigative process (e.g. by setting policy or creating constraints). It is recommended, however, that all of the documents are consulted prior to, and during, the planning and preparation phases. The process classes shown are defined fully in ISO/IEC 27043 and the activities identified match those discussed in more detail in ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27042 and ISO/IEC 27041.



Key

the document can be directly applied to these activities

the document contains information which may influence and/or assist with these activities

[a] Process classes are defined in ISO/IEC 27043.

[b] Detail of activities is given in ISO/IEC 27035-2, ISO/IEC 27037, and ISO/IEC 27042.

Figure A.1 — Applicability of standards to investigation process classes and activities

Annex B
(informative)
Examples of information security incidents and their causes

B.1 Type of incidents

B.1.1 General

Events and incidents covered by the ISO/IEC 27035 series concern information and ICT security. Such events and incidents result from imperfect risk management and the continuous advancement of people, processes and technology – and their associated vulnerabilities – in the context of evolving attacker motivation and capability.

The events/incidents happen in the following domains and incident management should cover all potential cases.

B.1.2 Confidentiality

Information leaks may have immediate effects on an organization, and may make information irretrievably available to unauthorized attackers and/or criminals.

One should hence “close the doors” (i.e. stop the leak, fill the breach) and prevent future breaches by identifying the place where it happened and its cause.

B.1.3 Integrity

Integrity incidents (unduly modified information) should be detected and corrected before the information is published and/or used.

Prevention is necessary by identifying the cause.

B.1.4 Availability

Unavailability of information (unreachable, unusable, wiped or disappeared information) can create effects in relation with the service level agreement (SLA) and the RPO. The information should be found and recovered before the business effect is unacceptable.

EXAMPLE A completed financial report ready to be sent to the fiscal authorities at a defined date was not respected.

B.1.5 Access control

Unauthorized access leads to system compromise, theft of resources, and information breach. Future occurrences should be prevented by identifying underlying exposures and causes and, where applicable, review of access control permissions (authorization, authentication, roles, privileges, network access, etc.)

B.1.6 Vulnerabilities

A technical, people or procedural vulnerability, such as an incorrect allocation of access rights, may allow for successful exploitation. Examples of vulnerabilities include:

— unpatched server, machine or software (not up to date);

— insufficient protection of assets (information, equipment, rooms) with regards to the criticality.

B.1.7 Technical failure

Technical failures render the ICT or physical device inoperative or unusable. It creates either a vulnerability or potential breach of the SLA and the RTO.

B.1.8 Theft or loss of equipment

Theft and loss of equipment, principally those containing information, should be considered as availability and/or confidentiality incidents.

B.2 Attacks

B.2.1 Denial of Service

Denial of Service (DoS) and Distributed Denial of Service (DDoS) are a broad category of incidents with a common thread. Such incidents cause a system, service or network to fail to continue operating in its intended capacity, most often with complete denial of access to legitimate users. There are two main types of DoS/DDoS incidents caused by technical means: resource elimination and resource starvation.

Typical examples of deliberate technical DoS/DDoS incidents include the following:

— forging of traffic (such as pinging) to network broadcast addresses or other services in an effort to overwhelm a target organization’s network bandwidth;

— sending data in an unexpected format to a system, service or network in an attempt to crash it, or disrupt its normal operation;

— opening up multiple authorized sessions with a particular system, service or network in an attempt to exhaust its resources (i.e. to slow it down, lock it up or crash it).

Such attacks are often performed through bots, a computer system running malware that is controlled via a botnet. A botnet is a central bot command and control network managed by humans. Botnet sizes can range from hundreds to millions of affected computers.

Some technical DoS incidents can be caused accidentally, for example, caused by operator misconfiguration or through incompatibility of application software, but most of the time, they are deliberate. Some technical DoS incidents are intentionally launched in order to crash a system or service, or take down a network, while others are merely the by-products of other malicious activity. For instance, some of the more common stealth scanning and identification techniques can cause older or misconfigured systems or services to crash when scanned. It should be noted that many deliberate technical DoS incidents are often executed anonymously (i.e. the source of the attack is “faked”), since they typically do not rely on the attacker receiving any information back from the network or system being attacked.

DoS incidents caused by non-technical means, resulting in loss of information, service and/or facilities, can be caused, for example, by:

— breaches of physical security arrangements resulting in theft or wilful damage and destruction of equipment;

— accidental damage to hardware (and/or its location) by fire or water damage/flood;

— extreme environmental conditions, for example high operating temperatures (e.g. due to air conditioning failure);

— system malfunctions or overload;

— uncontrolled system changes;

— malfunctions of software or hardware.

B.2.2 Unauthorized access

In general, this category of incidents consists of actual unauthorized attempts to access or misuse a system, service or network. Some examples of technical unauthorized access incidents include:

— attempts to retrieve password files;

— buffer overflow attacks to attempt to gain privileged (e.g. system administrator) access to a target;

— exploitation of protocol vulnerabilities to hijack or misdirect legitimate network connections;

— attempts to elevate privileges to resources or information beyond what a user or administrator already legitimately possesses;

— compromise at the domain name registrar or hosting provider level, that results in loss of control of the organization's domain portfolio, email service, or of website operations or content.

Unauthorized access incidents caused by non-technical means, resulting in direct or indirect disclosure or modification of information, breaches of accountability or misuse of information systems, can be caused, for example, by:

— breaches of physical security arrangements resulting in unauthorized access to information;

— poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware;

— malicious insider e.g. personnel using their access to the organization’s information assets for personal gain.

B.2.3 Malware

Malware is a program or part of a program inserted into another program with the intent to modify its original behaviour, usually to perform malicious activities such as information and identity theft, information and resource destruction, Denial of Service, spam, etc. Malware attacks can be divided into five categories: viruses, worms, Trojan horses, mobile code and blended. While viruses are created to target any vulnerable infected system, other malware are also used to perform targeted attacks. This is sometimes performed by modifying existing

malware and creating a variant that often is not recognized by malware detection technologies.

B.2.4 Abuse

This kind of incident occurs when a user violates an organization's information system security policies. Such incidents are not attacks in the strict sense of the word, but are often reported as incidents and should be handled by an IRT. Inappropriate usage can include:

— downloading and installing hacking tools;

— using corporate e-mail for spam or promotion of personal business;

— using corporate resources to set up an unauthorized website;

— using peer-to-peer activities to acquire or distribute pirated files (music, video, software);

— abusing physical or logical access to steal information for personal gain;

— abusing privilege/position to get information and disclosing it to other parties.

B.3 Information gathering

In general terms, the information gathering category of incidents includes those activities associated with identifying potential targets and understanding the services running on those targets. This type of incident involves reconnaissance, with the goal being to identify:

— the existence of a target, and to understand the network physical or logical topology (e.g. IT network, facility, organisational structure) surrounding it, and with whom the target routinely communicates;

— potential vulnerabilities in the target or its immediate environment that can be exploited.

Typical examples of information gathering by technical means include the following:

— reconnaissance and identification of a victim's online infrastructure by performing searches on known domain names or IP addresses, or by analysing passive DNS information;

— pinging network addresses to find systems that are “alive”;

— probing the system to identify (e.g. fingerprint) the host operating system;

— scanning the available network ports on a system to identify network services [e.g. e-mail, File Transfer Protocol (FTP), web, etc.] and the software versions of those services;

— scanning for one or more known vulnerable services across a network address range (horizontal scanning).

In some cases, technical information gathering extends into unauthorized access if, for example, as part of searching for vulnerabilities, the attacker also attempts to gain unauthorized access. This commonly occurs with automated tools that not only search for vulnerabilities but also automatically attempt to exploit the vulnerable systems, services and/or networks that are found.

Information gathering incidents caused by non-technical means, resulting in:

— direct or indirect disclosure or modification of information;

— theft of intellectual property stored electronically;

— breaches of accountability, e.g. in account logging;

— misuse of information systems (e.g. contrary to law or organization policy).

Information gathering incidents can be caused, for example, by:

— breaches of physical security arrangements resulting in unauthorized access to information, and theft of data storage equipment that contains important data, for example encryption keys;

— poorly and/or misconfigured operating systems due to uncontrolled system changes, or malfunctions of software or hardware, resulting in internal or external personnel gaining access to information for which they have no authority;

— social engineering, which is an act of manipulating people into performing actions or divulging confidential information, e.g. phishing, impersonation of someone else in a phone call;

— tailgating into restricted areas;

— listening in on conversations;

— shoulder surfing/oversight of open documents;

— dumpster diving;

— manipulation of staff.

Annex C
(informative)
Cross-reference table of ISO/IEC 27001 to the ISO/IEC 27035 series

Table C.1 shows references from ISO/IEC 27001:2022, Annex A, regarding information security incident management and where these references correspond in the ISO/IEC 27035 series. The specific subclauses of each document are indicated at the beginning of each row.

Table C.1 — Cross-references from ISO/IEC 27001:2022 in the ISO/IEC 27035 series

ISO/IEC 27001:**2022**, **Annex A**	**ISO/IEC 27035** series
5.24 Information security incident management planning and preparation Control: The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	**ISO/IEC 27035-1:2023** **5.2 Plan and prepare** **ISO/IEC 27035-2:2023** **4. Information security incident management policy** **5. Updating of information security policies** **6. Creating information security incident management plan** **7. Establishing an incident management capability** **8. Establishing internal and external relationships** **9. Defining technical and other support** **10. Creating information security incident awareness and training** **11. Testing the information security incident management plan**
6.8 Information security event reporting Control: The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	**ISO/IEC 27035-1:2023** **5.3 Detect and report** **ISO/IEC 27035-3:2020** **7 Incident detection operations** **8 Incident notification operations** **12 Incident reporting operations**
5.25 Assessment and decision on information security events Control: The organization shall assess information security events and decide if they are to be categorized as information security incidents.	**ISO/IEC 27035-1:2023** **5.4 Assess and decide** **ISO/IEC 27035-3:2020** **9 Incident triage operations** **10 Incident analysis operations**
5.26 Response to information security incidents Control: Information security incidents shall be responded to in accordance with the documented procedures.	**ISO/IEC 27035-1:2023** **5.5 Respond** **ISO/IEC 27035-3:2020** **11 Incident containment, eradication and recovery operations**
5.27 Learning from information security incidents Control: Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	**ISO/IEC 27035-1:2023** **5.6 Learn lessons** **ISO/IEC 27035-2:2023** **12 Learn lessons**

5.28 Collection of evidence Control: The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence related to information security events.	**ISO/IEC 27035-1:2023** **5.3 Detect and report** d), i) **5.4 Assess and decide** i), l) **5.5 Respond** f), j), m)

Annex D
(informative)
Considerations of situations discovered during the investigation of an incident

In the course of incident response, there are challenging situations where the incident coordinator can play a key role in controlling and advancing the investigation process. The following items provide possible situations and actions to be taken by incident coordinator.

For the incidents, different problems can arise:

a) No underlying problem is found, and the response flows as foreseen, within the time frame. The report records all information useful for the future.

b) Discovery of one or more underlying problems. The incident coordinator decides whether or not to call up other teams who are more specialized. The resolution happens:

   — before the end of the time frame: the report records all information useful for the future;

   — potentially outside the time frame: the incident coordinator informs the targeted/affected teams/entities along with the crisis manager so that they can prepare the (re)actions.

c) Discovery of underlying problems or other potential (or affected) internal or external victims that the activated response teams can handle. The incident coordinator informs:

   — the management of a possible extension and a potential failure to conclude within the time frame; this allows for internal communication;

   — the entity entitled to communicate with the outside of the organization [press service, data protection officer (DPO), etc.] if ordered so.

d) Discovery of underlying problems or other potential (or affected) internal or external victims that the activated response teams cannot handle. The incident coordinator informs:

   — the management to activate another incident coordinator. Close coordination should then be established between the different activated capabilities and other specific response teams (e.g. physical security, external assistance, etc.);

   — the entity entitled to communicate with the outside of the organization (press service, DPO, etc.).

e) Discovery of various problems related to the SLA. The incident coordinator escalates to the crisis manager, who is responsible for:

   — informing management;

   — giving control to the crisis manager;

   — keeping informed on the incident progress (the incident coordinator takes action when needed without waiting for information);

   — activating, at request, the teams he/she controls;

— keeping ready to take control again once the crisis is over.

Bibliografi

[1] ISO 22320, *Security and resilience — Emergency management — Guidelines for incident management*

[2] ISO/IEC 20000 (all parts), *Information technology — Service management*

[3] ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

[4] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[5] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*

[6] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*

[7] ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

[8] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[9] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[10] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[11] ISO/IEC 27033-2, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[12] ISO/IEC 27033-3, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[13] ISO/IEC 27035-2:2023, *Information technology — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*

[14] ISO/IEC 27035-3, *Information technology — Information security incident management — Part 3: Guidelines for ICT incident response operations*

[15] ISO/IEC 27037, *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*

[16] ISO/IEC 27038, *Information technology — Security techniques — Specification for digital redaction*

[17] ISO/IEC 27039, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*

[18] ISO/IEC 27040, *Information technology — Security techniques — Storage security*

[19] ISO/IEC 27041, *Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method*

[20] ISO/IEC 27042, *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*

[21] ISO/IEC 27043, *Information technology — Security techniques — Incident investigation principles and processes*

[22] ISO/IEC 27050 (all parts), *Information technology — Electronic discovery*

[23] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*

[24] ISO/IEC 30111, *Information technology — Security techniques — Vulnerability handling processes*

[25] ISO/IEC 30121, *Information technology — Governance of digital forensic risk framework*

Informasi Pendukung Standardisasi

[1] Komtek perumus SNI
Komite Teknis 35-04 Keamanan Informasi, Keamanan Siber, dan Perlindungan Privasi

[2] Susunan keanggotaan Komtek perumus SNI Tahun 2024
Ketua : Soetedjo Joewono
Sekretaris : Didik Utomo
Anggota :
1. Pedro Libratu Putu Wirya
2. Zaenal Arifin
3. Wisnoe Prasetyo Pribadi
4. Bisyron Wahyudi
5. Satriyo Wibowo
6. Sarwono Sutikno
7. Chandra Yulistia
8. Pratama Dahlian Persadha
9. Sugi Guritman
10. Bety Hayat Susanti
11. Sari Agustini Hafman

[3] Konseptor rancangan SNI Tahun 2024
Gugus Kerja 4 Kontrol dan Layanan Keamanan – Komtek 35-04 Tahun 2024:
Ketua : Sarwono Sutikno
Wakil Ketua : Pedro Libratu Putu Wirya
Sekretaris : Yasril Andriawan
Anggota :
1. Yusuf Kurniawan
2. Agus Salim
3. Ricky Aji Pratama
4. Javalina Harsari
5. Ruth Novida Sihite

[4] Sekretariat pengelola Komtek perumus SNI
Direktorat Kebijakan Teknologi Keamanan Siber dan Sandi
Badan Siber dan Sandi Negara (BSSN)