MALAYSIAN STANDARD

MS ISO/IEC 27001:2013 (BM)

Teknologi maklumat - Teknik keselamatan - Sistem pengurusan keselamatan maklumat - Keperluan
(Semakan pertama)
(ISO/IEC 27001:2013, IDT)
(Diterbitkan oleh Jabatan Standard Malaysia pada tahun 2017)

ICS: 35.040

Perihal: teknologi maklumat, teknik keselamatan, sistem pengurusan keselamatan maklumat, keperluan

JABATAN STANDARD MALAYSIA

PEMBANGUNAN *MALAYSIAN STANDARD*

Jabatan Standard Malaysia (STANDARDS MALAYSIA) ialah badan standard dan akreditasi kebangsaan.

Fungsi utama Jabatan Standard Malaysia adalah untuk merangsang dan menggalakkan standard, penstandardan dan akreditasi sebagai cara bagi memajukan ekonomi negara, menggalakkan kecekapan dan pembangunan industri yang bermanfaat kepada kesihatan dan keselamatan awam, melindungi pengguna, memudahkan perdagangan dalam negeri dan antarabangsa serta melanjutkan kerjasama antarabangsa berhubung dengan standard dan penstandardan.

Malaysian Standard (MS) dibangunkan melalui sepersetujuan jawatankuasa-jawatankuasa yang dianggotai oleh perwakilan yang seimbang daripada pengeluar, pengguna dan pihak lain yang kepentingannya relevan, sebagaimana yang sesuai dengan perkara yang sedang diusahakan. *Malaysian Standard* adalah sejajar atau diterima guna daripada standard antarabangsa, seboleh mungkin. Kelulusan sesuatu standard sebagai *Malaysian Standard* ditentukan oleh Akta Standard Malaysia 1996 [Akta 549]. *Malaysian Standard* dikaji semula secara berkala. Penggunaan *Malaysian Standard* adalah secara sukarela, melainkan diwajibkan oleh pihak berkuasa yang mengawal selia melalui peraturan, undang-undang kecil tempatan atau apa-apa cara lain yang serupa.

Untuk tujuan *Malaysian Standard*, definisi-definisi berikut diguna pakai:

Semakan: Proses di mana *Malaysian Standard* yang sedia ada dikaji semula dan dikemaskini yang menjurus kepada penerbitan edisi baharu *Malaysian Standard*.

MS yang disahkan: *Malaysian Standard* yang telah dikaji semula oleh jawatankuasa yang bertanggungjawab dan mengesahkan bahawa kandungannya adalah terkini.

Pindaan: Proses di mana peruntukan-peruntukan dalam *Malaysian Standard* sedia ada diubah. Perubahan-perubahan dinyatakan dalam halaman pindaan yang dimasukkan ke dalam *Malaysian Standard* sedia ada. Pindaan-pindaan boleh dalam bentuk teknikal atau editorial.

***Corrigendum* teknikal:** Cetakan semula yang telah dibetulkan bagi edisi terkini yang dikeluarkan untuk membuat pembetulan kepada kesilapan teknikal atau kekeliruan dalam *Malaysian Standard* yang diwujudkan dengan tidak sengaja semasa mendraf atau percetakan yang menyebabkan penggunaan *Malaysian Standard* yang tidak betul atau tidak selamat.

NOTA: *Corrigendum* teknikal bukan untuk membetulkan kesilapan yang boleh dianggap mendatangkan akibat semasa penggunaan *Malaysian Standard*, sebagai contoh kesilapan kecil percetakan.

Jabatan Standard Malaysia melantik **SIRIM Berhad** sebagai ejen bagi membangunkan *Malaysian Standard*. Jabatan itu juga melantik SIRIM Berhad sebagai ejen pengedaran dan penjualan *Malaysian Standard*.

Untuk maklumat lanjut berkaitan dengan *Malaysian Standard*, sila hubungi:

Jabatan Standard Malaysia
Kementerian Sains, Teknologi dan Inovasi
Aras 1 & 2, Blok 2300, Century Square
Jalan Usahawan
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel.: 60 3 8318 0002
Faks: 60 3 8319 3131
http://www.jsm.gov.my
E-mel: central@jsm.gov.my

ATAU

SIRIM Berhad
(No. Syarikat 367474-V)
1, Persiaran Dato' Menteri
Seksyen 2, Peti Surat 7035,
40700 Shah Alam
Selangor Darul Ehsan
MALAYSIA

Tel.: 60 3 5544 6000
Faks: 60 3 5510 8095
http://www.sirim.my
E-mel: msonline@sirim.my

Kandungan

Muka surat

Perwakilan jawatankuasa

Jawatankuasa Standard Perindustrian mengenai Teknologi Maklumat, Komunikasi dan Multimedia (ISC G) yang di bawah kuasanya *Malaysian Standard* ini diterima pakai, dianggotai oleh wakil daripada organisasi yang berikut:

CyberSecurity Malaysia
Dewan Perdagangan dan Industri Antarabangsa Malaysia
Gabungan Komputer Nasional Malaysia
Institut Jurutera Malaysia
Institut Penyelidikan Sains dan Teknologi Pertahanan
Institut Tadbiran Awam Negara, Malaysia
Jabatan Standard Malaysia
Kementerian Komunikasi dan Multimedia
Kementerian Perdagangan Antarabangsa dan Industri
Kementerian Sains, Teknologi dan Inovasi
Kementerian Tenaga, Teknologi Hijau dan Air
Majlis Keselamatan Negara
Malaysia Digital Economy Corporation Sdn Bhd
Malaysian Technical Standards Forum Bhd
MIMOS Berhad
Multimedia University
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Persatuan Industri Komputer dan Multimedia Malaysia
Persatuan Jurutera Perunding Malaysia
Persekutuan Pekilang-Pekilang Malaysia
SIRIM Berhad (Sekretariat)
Suruhanjaya Komunikasi dan Multimedia Malaysia
Telekom Malaysia Berhad
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Universiti Teknologi Malaysia

Jawatankuasa Teknikal mengenai Keselamatan Maklumat yang mengawal selia penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* ini terdiri daripada perwakilan organisasi yang berikut:

CyberSecurity Malaysia
Kementerian Sains, Teknologi dan Inovasi
Malaysia Digital Economy Corporation Sdn Bhd
MIMOS Berhad
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Persatuan Industri Komputer dan Multimedia Malaysia
POS Malaysia Berhad
PricewaterhouseCoopers Risk Services Sdn Bhd
SIRIM Berhad (Sekretariat)
SIRIM QAS International Sdn Bhd
Suruhanjaya Komunikasi dan Multimedia Malaysia
TM Applied Business Sdn Bhd
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia

Perwakilan jawatankuasa (*sambungan*)

Kumpulan Kerja mengenai Sistem Pengurusan Keselamatan Maklumat yang mengesyorkan penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* ini dianggotai oleh wakil daripada organisasi yang berikut:

CyberSecurity Malaysia
Malaysian Electronic Payment System Sdn Bhd
PricewaterhouseCoopers Risk Services Sdn Bhd
Scope International (M) Sdn Bhd
SIRIM Berhad (Sekretariat)
SIRIM QAS International Sdn Bhd
Suruhanjaya Komunikasi dan Multimedia Malaysia
TM Applied Business Sdn Bhd
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Universiti Islam Antarabangsa Malaysia
Universiti Malaya
Universiti Pertahanan Nasional Malaysia
VADS Berhad

Ahli ambilan:

RHB Bank Berhad

Prakata kebangsaan

Penerimagunaan Standard ISO/IEC sebagai *Malaysian Standard* telah disyorkan oleh Kumpulan Kerja mengenai Sistem Pengurusan Keselamatan Maklumat di bawah kuasa Jawatankuasa Standard Perindustrian mengenai Teknologi Maklumat, Komunikasi dan Multimedia.

Malaysian Standard ini serupa dengan ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems - Requirements*, yang diterbitkan oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC). Walau bagaimanapun, bagi maksud *Malaysian Standard* ini, perkara yang berikut terpakai:

a) dalam teks sumber, “Standard Antarabangsa ini” hendaklah dibaca sebagai “*Malaysian Standard* ini”; dan

b) tanda koma yang digunakan sebagai titik perpuluhan (jika ada), hendaklah dibaca sebagai noktah.

Malaysian Standard ini membatalkan dan menggantikan MS ISO/IEC 27001:2007, *Information technology - Security techniques - Information security management systems - Requirements*.

Versi bahasa Malaysia ini adalah terjemahan daripada versi asal dalam bahasa Inggeris, iaitu MS ISO/IEC 27001:2013, *Information technology - Security techniques - Information security management systems - Requirements*. Jika terdapat sebarang pertikaian semasa penggunaan standard ini, versi bahasa Inggeris mengatasi versi ini.

Pematuhan kepada *Malaysian Standard* tidak dengan sendirinya memberikan kekebalan daripada obligasi undang-undang.

NOTA. IDT pada kulit depan menunjukkan standard yang serupa, iaitu standard dengan kandungan, struktur dan perkataan teknikal (atau terjemahan yang serupa) bagi *Malaysian Standard* adalah benar-benar sama dengan yang terdapat dalam Standard Antarabangsa atau serupa dari segi kandungan dan struktur teknikal, walaupun ia mungkin mengandungi perubahan editorial yang minimum seperti yang dinyatakan dalam klausa 4.2 ISO/IEC Guide 21-1.

Prakata

ISO [International Organization for Standardization] dan IEC [International Electrotechnical Commission] membentuk sistem khusus bagi penstandardan seluruh dunia. Badan kebangsaan yang menjadi ahli ISO atau IEC turut serta dalam membangunkan Standard Antarabangsa melalui jawatankuasa teknikal yang ditubuhkan oleh organisasi masing-masing untuk menangani aktiviti teknikal dalam bidang tertentu. Jawatankuasa teknikal ISO dan IEC bekerjasama dalam beberapa bidang yang melibatkan kepentingan bersama. Organisasi antarabangsa yang lain, kerajaan atau bukan kerajaan, dengan kerjasama ISO dan IEC, juga turut serta dalam usaha tersebut. Dalam bidang teknologi maklumat, ISO dan IEC telah menubuhkan jawatankuasa teknikal bersama, iaitu ISO/IEC JTC 1.

Standard Antarabangsa telah digubal menurut peraturan yang ditetapkan dalam ISO/IEC Directives, Part 2.

Tugas utama jawatankuasa teknikal bersama adalah menyediakan Standard Antarabangsa. Draf Standard Antarabangsa yang diterima pakai oleh jawatankuasa teknikal bersama, diedarkan kepada badan kebangsaan untuk undian. Penerbitan sebagai Standard Antarabangsa memerlukan kelulusan sekurang-kurangnya 75 % daripada badan kebangsaan yang mengundi.

Perlu ditegaskan bahawa terdapat kemungkinan sesetengah unsur dokumen ini tertakluk kepada hak paten. ISO dan IEC tidak boleh dipertanggungjawabkan untuk mengenal pasti mana-mana atau kesemua hak paten tersebut.

ISO/IEC 27001 disediakan oleh Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC27, IT Security techniques.

Edisi kedua in membatalkan dan menggantikan edisi pertama (ISO/IEC 27001:2005), yang telah disemak semula dari segi teknikal.

0 Pengenalan

0.1 Am

Standard Antarabangsa ini disediakan untuk menetapkan keperluan bagi menyediakan, melaksanakan, menyenggara dan menambah baik secara berterusan sistem pengurusan keselamatan maklumat. Penerimagunaan sistem pengurusan keselamatan maklumat merupakan keputusan yang strategik bagi sesebuah organisasi. Penyediaan dan pelaksanaan sistem pengurusan keselamatan maklumat organisasi dipengaruhi oleh keperluan dan objektif organisasi, keperluan keselamatan, proses organisasi yang digunakan serta saiz dan struktur organisasi. Semua faktor pengaruh ini dijangka berubah dari semasa ke semasa.

Sistem pengurusan keselamatan maklumat memelihara kerahsiaan, integriti dan ketersediaan maklumat melalui proses pengurusan risiko yang digunakan dan memberikan keyakinan kepada pihak berkepentingan bahawa risiko telah dikendalikan dengan sebaik-baiknya.

Adalah penting untuk menjadikan sistem pengurusan keselamatan maklumat sebagai sebahagian daripada, dan berintegrasi dengan pelbagai proses organisasi. Malahan keseluruhan struktur pengurusan, dan keselamatan maklumat hendaklah diambil kira dalam merangka proses, sistem maklumat dan kawalan. Pelaksanaan sistem pengurusan keselamatan maklumat diharapkan dapat disesuaikan menurut keperluan organisasi.

Standard Antarabangsa ini boleh digunakan oleh pihak dalaman dan luaran untuk menilai keupayaan organisasi memenuhi keperluan keselamatan maklumat organisasi masing-masing.

Susunan klausa keperluan dalam Standard Antarabangsa ini tidak menggambarkan kepentingannya atau menunjukkan susunan bagi melaksanakan keperluan itu. Nombor bagi perkara yang disenaraikan hanya untuk tujuan rujukan.

ISO/IEC 27000 menerangkan gambaran keseluruhan dan perbendaharaan kata bagi sistem pengurusan keselamatan maklumat, dengan merujuk standard bagi kelompok sistem pengurusan keselamatan maklumat (termasuk ISO/IEC 27003 [2], ISO/IEC 27004 [3], dan ISO/IEC 27005 [4]), dengan istilah dan takrifan yang berkaitan.

0.2 Keserasian dengan standard sistem pengurusan yang lain

Standard Antarabangsa ini menggunakan struktur peringkat tinggi, tajuk subklausa yang serupa, teks yang serupa, istilah lazim, dan takrifan teras *yang diterangkan dalam* Annex SL ISO/IEC Directives, Part 1, Consolidated ISO Supplement, dan oleh itu mengekalkan keserasian dengan standard sistem pengurusan yang lain yang menggunakan Annex SL itu.

Pendekatan biasa ini yang ditakrifkan dalam Annex SL sangat berguna bagi membantu organisasi yang ingin melaksanakan satu sistem pengurusan yang memenuhi keperluan dua standard sistem pengurusan atau lebih.

Teknologi maklumat - Teknik keselamatan - Sistem pengurusan keselamatan maklumat - Keperluan

1 Skop

Standard Antarabangsa ini menetapkan keperluan bagi mewujudkan, melaksanakan, menyenggara dan menambah baik secara berterusan sistem pengurusan keselamatan maklumat mengikut konteks organisasi. Standard Antarabangsa ini juga memasukkan keperluan untuk pentaksiran dan penguraian risiko keselamatan maklumat yang disesuaikan dengan keperluan organisasi. Keperluan yang ditetapkan dalam Standard Antarabangsa ini adalah umum dan bertujuan untuk digunakan oleh semua organisasi, tanpa mengira jenis, saiz atau ciri. Pengecualian sebarang keperluan yang ditetapkan dalam Klausa 4 hingga 10 tidak boleh diterima apabila sesebuah organisasi mendakwa memenuhi Standard Antarabangsa ini.

2 Rujukan normatif

Keseluruhan atau sebahagian daripada dokumen yang berikut dirujuk secara normatif dalam dokumen ini dan sangat diperlukan untuk penggunaannya. Bagi rujukan bertarikh, hanya edisi yang disebutkan diguna pakai. Bagi rujukan tidak bertarikh, edisi terkini dokumen yang dirujuk (termasuk sebarang pindaan) diguna pakai.

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

3 Istilah dan takrifan

Bagi tujuan dokumen ini, istilah dan takrifan yang diberikan dalam ISO/IEC 27000 adalah diguna pakai.

4 Konteks organisasi

4.1 Memahami organisasi dan konteksnya

Organisasi hendaklah menentukan isu luaran dan dalaman yang berkaitan dengan tujuannya dan isu yang menjejaskan keupayaannya untuk mencapai hasil yang diinginkan daripada sistem pengurusan keselamatan maklumatnya.

NOTA Penentuan isu ini merujuk penyediaan konteks luaran dan dalaman organisasi yang diambil kira dalam Klausa 5.3 ISO 31000:2009 [5].

4.2 Memahami keperluan dan jangkaan pihak berkepentingan

Organisasi hendaklah menentukan:

a) pihak berkepentingan yang berkaitan dengan sistem pengurusan keselamatan maklumat; dan

b) keperluan pihak berkepentingan ini yang berkaitan dengan keselamatan maklumat.

NOTA Keperluan pihak berkepentingan mungkin termasuk keperluan undang-undang dan kawal selia serta obligasi kontrak.

4.3 Menentukan skop sistem pengurusan keselamatan maklumat

Organisasi hendaklah menentukan sempadan dan kebolehgunaan sistem pengurusan keselamatan maklumat untuk mewujudkan skopnya.

Semasa menentukan skop ini, organisasi hendaklah mempertimbangkan:

a) isu luaran dan dalaman yang dirujuk dalam 4.1;

b) keperluan yang dirujuk dalam 4.2; dan

c) hubungan dan kebergantungan antara aktiviti yang dijalankan oleh organisasi dengan aktiviti yang dijalankan oleh organisasi lain.

Skop hendaklah disediakan dalam bentuk dokumentasi.

4.4 Sistem pengurusan keselamatan maklumat

Organisasi hendaklah mewujudkan, melaksanakan, menyenggara dan menambah baik secara berterusan sistem pengurusan keselamatan maklumat, selaras dengan keperluan Standard Antarabangsa ini.

5 Kepimpinan

5.1 Kepimpinan dan komitmen

Pengurusan atasan hendaklah menunjukkan kepimpinan dan komitmen berhubung dengan sistem pengurusan keselamatan maklumat dengan:

a) memastikan dasar keselamatan maklumat dan objektif keselamatan maklumat disediakan dan serasi dengan hala tuju strategik organisasi;

b) memastikan integrasi keperluan sistem pengurusan keselamatan maklumat dengan proses organisasi;

c) memastikan sumber yang diperlukan untuk sistem pengurusan keselamatan maklumat tersedia;

d) menyampaikan kepentingan pengurusan keselamatan maklumat yang berkesan dan memenuhi keperluan sistem pengurusan keselamatan maklumat;

e) memastikan sistem pengurusan keselamatan maklumat mencapai hasil yang dikehendaki;

f) mengarahkan dan menyokong mereka yang berkenaan supaya menyumbang ke arah keberkesanan sistem pengurusan keselamatan maklumat;

g) menggalakkan penambahbaikan berterusan; dan

h) menyokong peranan pengurusan lain yang berkenaan, bagi menunjukkan kepimpinan yang bersesuaian dengan bidang tanggungjawab masing-masing.

5.2 Dasar

Pengurusan atasan hendaklah menyediakan dasar keselamatan maklumat yang:

a) sesuai dengan tujuan organisasi;

b) merangkumi objektif keselamatan maklumat (rujuk 6.2) atau menyediakan rangka kerja untuk menetapkan objektif keselamatan maklumat;

c) merangkumi komitmen untuk memenuhi keperluan keselamatan maklumat yang bersesuaian; dan

d) merangkumi komitmen untuk terus menambah baik sistem pengurusan keselamatan maklumat.

Dasar keselamatan maklumat hendaklah:

e) disediakan dalam bentuk dokumentasi;

f) disampaikan dalam organisasi; dan

g) diberikan kepada pihak berkepentingan, yang bersesuaian.

5.3 Peranan, tanggungjawab dan autoriti organisasi

Pengurusan atasan hendaklah memastikan tanggungjawab dan autoriti untuk peranan yang berkaitan dengan keselamatan maklumat ditetapkan dan dimaklumkan.

Pengurusan atasan hendaklah menetapkan tanggungjawab dan autoriti untuk:

a) memastikan sistem pengurusan keselamatan maklumat memenuhi keperluan Standard Antarabangsa ini; dan

b) melaporkan prestasi sistem pengurusan keselamatan maklumat kepada pengurusan atasan.

NOTA Pengurusan atasan juga boleh menetapkan tanggungjawab dan autoriti untuk melaporkan prestasi sistem pengurusan keselamatan dalam organisasi.

6 Perancangan

6.1 Tindakan untuk menangani risiko dan peluang

6.1.1 Am

Apabila merancang sistem pengurusan keselamatan maklumat, organisasi hendaklah mengambil kira isu yang dirujuk dalam 4.1 dan keperluan yang dirujuk dalam 4.2. Organisasi juga perlu menentukan risiko dan peluang yang perlu ditangani untuk:

a) memastikan sistem pengurusan keselamatan maklumat mencapai hasil yang diinginkan;

b) mencegah, atau mengurangkan kesan yang tidak diingini; dan

c) mencapai penambahbaikan yang berterusan.

Organisasi hendaklah merancang:

d) tindakan untuk menangani risiko dan peluang ini; dan

e) cara untuk

    1) menggabungkan dan melaksanakan tindakan ini dalam proses sistem pengurusan keselamatan maklumat; dan

    2) menilai keberkesanan tindakan ini.

6.1.2 Pentaksiran risiko keselamatan maklumat

Organisasi hendaklah mentakrifkan dan menggunakan proses pentaksiran risiko keselamatan maklumat yang:

a) mewujudkan dan mengekalkan kriteria risiko keselamatan maklumat yang merangkumi:

    1) kriteria penerimaan risiko; dan

    2) kriteria untuk menjalankan pentaksiran risiko keselamatan maklumat;

b) memastikan penilaian berulang terhadap risiko keselamatan maklumat menghasilkan keputusan yang konsisten, sah dan dapat dibandingkan;

c) mengenal pasti risiko keselamatan maklumat:

    1) menggunakan proses pentaksiran risiko keselamatan maklumat untuk mengenal pasti risiko yang dikaitkan dengan kehilangan dari segi kerahsiaan, integriti dan ketersediaan maklumat dalam skop sistem pengurusan keselamatan maklumat; dan

    2) mengenal pasti pemilik risiko;

d) menganalisis risiko keselamatan maklumat:

    1) menilai akibat yang mungkin dialami jika risiko yang dikenal pasti dalam 6.1.2 c) 1) berlaku;

2) menilai kemungkinan yang realistik tentang kewujudan risiko yang dikenal pasti dalam 6.1.2 c) 1); dan

3) menentukan tahap risiko;

e) menilai risiko keselamatan maklumat:

1) membandingkan keputusan analisis risiko dengan kriteria risiko yang ditentukan dalam 6.1.2 a); dan

2) mengutamakan risiko yang dianalisis untuk penguraian risiko.

Organisasi hendaklah menyimpan maklumat yang didokumenkan tentang proses pentaksiran risiko keselamatan maklumat.

6.1.3 Penguraian risiko keselamatan maklumat

Organisasi hendaklah mentakrifkan dan menggunakan proses penguraian risiko keselamatan maklumat untuk:

a) memilih opsyen penguraian risiko keselamatan maklumat yang sesuai, dengan mengambil kira keputusan pentaksiran risiko;

b) menentukan semua kawalan yang perlu untuk melaksanakan opsyen penguraian risiko keselamatan maklumat yang dipilih;

NOTA Organisasi boleh merangka kawalan yang diperlukan, atau mengenal pasti kawalan tersebut daripada sebarang sumber.

c) membandingkan kawalan yang ditentukan dalam 6.1.3 b) di atas dengan yang terdapat dalam Lampiran A dan menentusahkan tiada kawalan yang perlu tertinggal;

NOTA 1 Lampiran A mengandungi senarai lengkap objektif kawalan dan kawalan. Pengguna Standard Antarabangsa ini diminta merujuk Lampiran A bagi memastikan tiada kawalan yang perlu tertinggal.

NOTA 2 Objektif kawalan dimasukkan sepenuhnya dalam kawalan yang dipilih. Objektif kawalan dan kawalan yang disenaraikan dalam Lampiran A tidak lengkap dan objektif kawalan serta kawalan tambahan mungkin diperlukan.

d) mengemukakan Penyata Pemakaian yang mengandungi:

- kawalan yang perlu [rujuk 6.1.3 b) dan c)];
- justifikasi untuk memasukkan kawalan;
- sama ada kawalan yang diperlukan dilaksanakan atau tidak; dan
- justifikasi untuk tidak memasukkan kawalan daripada Lampiran A;

e) merumus rancangan penguraian risiko keselamatan maklumat; dan

f) mendapatkan kelulusan pemilik risiko bagi rancangan penguraian risiko keselamatan maklumat dan penerimaan risiko residual keselamatan maklumat.

Organisasi hendaklah menyimpan maklumat yang didokumenkan tentang proses penguraian risiko keselamatan maklumat.

NOTA Proses penilaian dan penguraian risiko keselamatan maklumat dalam Standard Antarabangsa ini selaras dengan prinsip dan garis panduan generik yang disediakan dalam ISO 31000 [5].

6.2 Objektif keselamatan maklumat dan perancangan untuk mencapainya

Organisasi hendaklah menetapkan objektif keselamatan maklumat pada tahap dan fungsi yang relevan.

Objektif keselamatan maklumat hendaklah:

a) selaras dengan dasar keselamatan maklumat;

b) boleh diukur (jika boleh dilakukan);

c) mengambil kira keperluan keselamatan maklumat yang terpakai, dan keputusan daripada pentaksiran risiko dan penguraian risiko;

d) dimaklumkan; dan

e) dikemas kini sewajarnya.

Organisasi hendaklah menyimpan maklumat yang didokumenkan tentang objektif keselamatan maklumat.

Apabila merancang cara hendak mencapai objektif keselamatan maklumat, organisasi hendaklah menentukan;

f) apa yang perlu dilakukan;

g) apa sumber yang diperlukan;

h) siapa yang bertanggungjawab;

i) bila ia akan disiapkan; dan

j) bagaimana keputusan akan dinilai.

7 Sokongan

7.1 Sumber

Organisasi hendaklah menentukan dan menyediakan sumber yang diperlukan untuk mewujudkan, melaksanakan, menyenggara dan menambah baik secara berterusan sistem pengurusan keselamatan maklumat.

7.2 Kecekapan

Organisasi hendaklah:

a) menentukan kecekapan yang sewajarnya bagi mereka yang menjalankan tugas di bawah kawalan organisasi, yang memberi kesan ke atas prestasi keselamatan maklumat;

b) memastikan mereka cekap berdasarkan pendidikan, latihan atau pengalaman yang sesuai;

c) di mana berkenaan, mengambil tindakan untuk memperoleh kecekapan yang sewajarnya, dan menilai keberkesanan tindakan yang telah diambil; dan

d) menyimpan maklumat berkenaan yang didokumenkan sebagai bukti kecekapan.

NOTA Tindakan yang boleh diambil termasuk: peruntukan latihan, pementoran atau penugasan semula kakitangan sedia ada; atau pengambilan kakitangan atau mengambil bekerja secara kontrak mereka yang mempunyai kecekapan.

7.3 Kesedaran

Mereka yang menjalankan tugas di bawah kawalan organisasi perlu ada kesedaran tentang:

a) dasar keselamatan maklumat;

b) sumbangan mereka ke arah keberkesanan sistem pengurusan keselamatan maklumat, termasuk manfaat daripada prestasi keselamatan maklumat yang telah ditambah baik; dan

c) implikasi sekiranya tidak memenuhi keperluan sistem pengurusan keselamatan maklumat.

7.4 Komunikasi

Organisasi hendaklah menentukan keperluan komunikasi dalaman dan luaran yang berkaitan dengan sistem pengurusan keselamatan maklumat termasuk:

a) apa yang hendak disampaikan;

b) bila hendak disampaikan;

c) dengan siapa hendak disampaikan;

d) siapa yang hendak menyampaikan; dan

e) proses untuk melaksanakan komunikasi.

7.5 Maklumat yang didokumenkan

7.5.1 Am

Sistem pengurusan keselamatan maklumat organisasi hendaklah merangkumi:

a) maklumat yang didokumenkan yang dikehendaki oleh Standard Antarabangsa ini; dan

b) maklumat yang didokumenkan yang ditentukan oleh organisasi sebagai perlu untuk keberkesanan sistem pengurusan keselamatan maklumat.

NOTA Jumlah maklumat yang didokumenkan untuk sistem pengurusan keselamatan maklumat berbeza antara satu organisasi dengan yang lain disebabkan oleh:

1) saiz organisasi dan jenis aktiviti, proses, produk dan perkhidmatannya;

2) kerumitan proses dan saling kait antaranya; dan

3) kecekapan mereka yang berkenaan.

7.5.2 Penyediaan dan pengemaskinian

Apabila menyediakan dan mengemaskinikan maklumat yang didokumenkan, organisasi hendaklah memastikan perkara berikut dilakukan sewajarnya:

a) pengenalpastian dan keterangan (contohnya, tajuk, tarikh, pengarang atau nombor rujukan);

b) format (contohnya, bahasa, versi perisian, grafik) dan media (contohnya, kertas, elektronik); dan

c) kajian semula dan kelulusan berhubung dengan kesesuaian dan kecukupan.

7.5.3 Kawalan maklumat yang didokumenkan

Maklumat yang didokumenkan yang diperlukan oleh sistem pengurusan keselamatan maklumat dan Standard Antarabangsa ini hendaklah dikawal bagi memastikan:

a) ia tersedia dan sesuai untuk digunakan, di mana dan bila diperlukan; dan

b) ia dilindungi secukupnya (contohnya, daripada ketirisan rahsia, penyalahgunaan atau kehilangan integriti).

Untuk kawalan dokumentasi, organisasi hendaklah menangani aktiviti yang berikut, jika berkenaan:

c) pengedaran, akses, dapatan semula dan kegunaan;

d) penyimpanan dan pemeliharaan, termasuk pemeliharaan untuk mudah baca;

e) kawalan perubahan (contohnya, kawalan versi); dan

f) pengekalan dan pelupusan.

Dokumentasi yang berasal dari luar, yang diperlukan oleh organisasi untuk perancangan dan operasi sistem pengurusan keselamatan maklumat, hendaklah dikenal pasti secara wajar dan terkawal.

NOTA Akses bermaksud keputusan berhubung dengan kebenaran melihat dokumentasi sahaja, atau kebenaran dan kuasa untuk melihat dan mengubah dokumentasi itu, dan sebagainya.

8 Operasi

8.1 Perancangan dan kawalan operasi

Organisasi hendaklah merancang, melaksanakan dan mengawal proses yang perlu bagi memenuhi keperluan keselamatan maklumat, dan melaksanakan tindakan yang ditetapkan dalam 6.1. Organisasi hendaklah juga melaksanakan rancangan untuk mencapai objektif keselamatan maklumat yang ditetapkan dalam 6.2.

Organisasi hendaklah menyimpan maklumat yang didokumenkan setakat yang perlu sehingga diyakini proses itu telah dijalankan seperti yang dirancang.

Organisasi hendaklah mengawal perubahan yang dirancang dan mengkaji semula akibat daripada perubahan yang tidak disengajakan, mengambil tindakan untuk mengurangkan kesan yang menjejaskan, jika perlu.

Organisasi hendaklah memastikan proses yang diserahkan kepada khidmat luaran ditentukan dan dikawal.

8.2 Pentaksiran risiko keselamatan maklumat

Organisasi hendaklah menjalankan pentaksiran risiko keselamatan maklumat pada sela masa yang dirancang atau apabila perubahan yang ketara dicadangkan atau berlaku, dengan mengambil kira kriteria yang ditetapkan dalam 6.1.2 a).

Organisasi hendaklah menyimpan maklumat yang didokumenkan bagi keputusan pentaksiran risiko keselamatan maklumat.

8.3 Penguraian risiko keselamatan maklumat

Organisasi hendaklah melaksanakan rancangan penguraian risiko keselamatan maklumat.

Organisasi hendaklah menyimpan maklumat yang didokumenkan bagi keputusan penguraian risiko keselamatan maklumat.

9 Penilaian prestasi

9.1 Pemantauan, pengukuran, analisis dan penilaian

Organisasi hendaklah menilai prestasi keselamatan maklumat dan keberkesanan sistem pengurusan keselamatan maklumat.

Organisasi hendaklah menentukan:

a) perkara yang perlu dipantau dan diukur, termasuk proses dan kawalan keselamatan maklumat;

b) kaedah pemantauan, pengukuran, analisis dan penilaian, apabila berkenaan, bagi memastikan keputusan yang sahih;

NOTA Kaedah yang dipilih hendaklah menghasilkan keputusan yang dapat dibandingkan dan boleh dihasilkan semula supaya boleh dianggap sahih.

c) bila pemantauan dan pengukuran perlu dilakukan;

d) siapa yang menjalankan pemantauan dan pengukuran;

e) bila keputusan daripada pemantauan dan pengukuran perlu dianalisis dan dinilai; dan

f) siapa yang akan menganalisis dan menilai keputusan tersebut.

Organisasi hendaklah menyimpan maklumat yang didokumenkan yang berkaitan sebagai bukti daripada hasil pemantauan dan pengukuran.

9.2 Audit dalaman

Organisasi hendaklah menjalankan audit dalaman pada sela masa yang dirancang untuk menyediakan maklumat sama ada sistem pengurusan keselamatan maklumat:

a) memenuhi

1) keperluan organisasi terhadap sistem pengurusan keselamatan maklumat; dan

2) keperluan Standard Antarabangsa ini;

b) dilaksanakan dan disenggara dengan berkesan.

Organisasi hendaklah:

c) merancang, mewujudkan, melaksanakan dan menyenggara program audit, termasuk kekerapan, kaedah, tanggungjawab, keperluan perancangan dan pelaporan. Program audit hendaklah mengambil kira kepentingan proses yang berkenaan dan hasil audit terdahulu;

d) mentakrifkan kriteria audit dan skop bagi setiap audit;

e) memilih juruaudit dan mengendali audit yang memastikan objektiviti dan kesaksamaan proses audit;

f) memastikan hasil audit dilaporkan kepada pengurusan yang berkaitan; dan

g) menyimpan maklumat yang didokumenkan sebagai bukti bagi program audit dan hasil audit.

9.3 Kajian semula pengurusan

Pengurusan atasan hendaklah mengkaji semula sistem pengurusan keselamatan maklumat organisasi pada sela masa yang dirancang bagi memastikan kesesuaian, kecukupan dan keberkesanan yang berterusan.

Kajian semula pengurusan hendaklah mengandungi pertimbangan tentang:

a) status tindakan daripada kajian semula pengurusan terdahulu;

b) perubahan dalam isu luaran dan dalaman yang berkaitan dengan sistem pengurusan keselamatan maklumat;

c) maklum balas tentang prestasi keselamatan maklumat, termasuk trend dalam:

   1) ketakakuran dan tindakan pembetulan;

   2) hasil pemantauan dan pengukuran;

   3) hasil audit; dan

   4) pencapaian objektif keselamatan maklumat;

d) maklum balas daripada pihak berkepentingan;

e) hasil pentaksiran risiko dan pelan penguraian risiko; dan

f) peluang untuk penambahbaikan berterusan.

Output kajian semula pengurusan hendaklah merangkumi keputusan yang berkaitan dengan peluang penambahbaikan yang berterusan dan sebarang keperluan untuk perubahan dalam sistem pengurusan keselamatan maklumat.

Organisasi hendaklah menyimpan maklumat yang didokumenkan sebagai bukti daripada hasil kajian semula pengurusan.

10 Penambahbaikan

10.1 Ketakakuran dan tindakan pembetulan

Apabila berlaku ketakakuran, organisasi hendaklah:

a) bertindak ke atas ketakakuran, dan jika berkenaan;

   1) mengambil tindakan untuk mengawal dan membetulkannya; dan

   2) menangani akibatnya;

b) menilai keperluan untuk bertindak menghapuskan punca ketakakuran, supaya ia tidak berulang atau berlaku di tempat lain, dengan:

   1) mengkaji semula ketakakuran;

   2) menentukan punca ketakakuran; dan

   3) menentukan jika ketakakuran yang serupa wujud, atau berpotensi berlaku;

c) melaksanakan sebarang tindakan yang diperlukan;

d) mengkaji semula keberkesanan bagi sebarang tindakan pembetulan yang diambil; dan

e) membuat perubahan dalam sistem pengurusan keselamatan maklumat, jika perlu.

Tindakan pembetulan hendaklah bersesuaian dengan kesan daripada ketakakuran yang ditemui.

Organisasi hendaklah menyimpan maklumat yang didokumenkan sebagai bukti bagi:

f) jenis ketakakuran dan sebarang tindakan seterusnya yang telah diambil; dan

g) hasil daripada sebarang tindakan pembetulan.

10.2 Penambahbaikan berterusan

Organisasi hendaklah menambah baik secara berterusan kesesuaian, kecukupan dan keberkesanan sistem pengurusan keselamatan maklumat.

Lampiran A
(normatif)

Rujukan bagi objektif kawalan dan kawalan

Objektif kawalan dan kawalan yang disenaraikan dalam Jadual A.1 diambil terus daripada dan diselaraskan dengan yang disenarai dalam ISO/IEC 27002:2013 [1], Klausa 5 hingga 18 dan hendaklah digunakan mengikut konteks Klausa 6.1.3.

Jadual A.1 – Objektif kawalan dan kawalan

A.5 Dasar keselamatan maklumat		
A.5.1 Hala tuju pengurusan untuk keselamatan maklumat		
Objektif: Menyediakan hala tuju dan sokongan pengurusan untuk keselamatan maklumat menurut keperluan perniagaan serta undang-undang dan peraturan yang berkaitan.		
A.5.1.1	Dasar keselamatan maklumat	*Kawalan* Satu set dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan dan disampaikan kepada kakitangan dan pihak luaran yang berkaitan.
A.5.1.2	Kajian semula dasar untuk keselamatan maklumat	*Kawalan* Dasar untuk keselamatan maklumat hendaklah dikaji semula pada sela masa yang dirancang atau jika berlaku perubahan yang ketara bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan.
A.6 Perancangan bagi keselamatan maklumat		
A.6.1 Perancangan dalaman		
Objektif: Menyediakan rangka kerja pengurusan untuk memulakan dan mengawal pelaksanaan dan operasi keselamatan dalam organisasi.		
A.6.1.1	Peranan dan tanggungjawab keselamatan maklumat	*Kawalan* Semua tanggungjawab keselamatan maklumat hendaklah ditakrifkan dan diperuntukkan.
A.6.1.2	Pengasingan tugas	*Kawalan* Tugas dan bidang tanggungjawab yang bercanggah hendaklah diasingkan bagi mengurangkan peluang mengubah suai, tanpa kebenaran atau dengan tidak sengaja mengubah, atau menyalahgunakan aset organisasi.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.6.1.3	Hubungan dengan pihak berkuasa	*Kawalan* Hubungan yang baik dengan pihak berkuasa yang berkaitan hendaklah dikekalkan.
A.6.1.4	Hubungan dengan kumpulan berkepentingan yang khusus	*Kawalan* Hubungan baik dengan kumpulan berkepentingan yang khusus atau forum pakar keselamatan dan persatuan/pertubuhan profesional yang lain hendaklah dikekalkan.
A.6.1.5	Keselamatan maklumat dalam pengurusan projek	*Kawalan* Keselamatan maklumat hendaklah ditangani dalam pengurusan projek, tanpa mengambil kira jenis projek.
A.6.2 Peranti mudah alih dan telekerja		
Objektif: Memastikan keselamatan telekerja dan penggunaan peranti mudah alih.		
A.6.2.1	Dasar peranti mudah alih	*Kawalan* Dasar dan langkah-langkah keselamatan sokongan hendaklah digunakan bagi menguruskan risiko yang timbul melalui penggunaan peranti mudah alih.
A.6.2.2	Telekerja	*Kawalan* Dasar dan langkah-langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di tapak telekerja.
A.7 Keselamatan sumber manusia		
A.7.1 Sebelum penjawatan		
Objektif: Memastikan kakitangan dan kontraktor memahami tanggungjawab mereka dan sesuai dengan peranan yang dipertimbangkan untuk mereka.		
A.7.1.1	Saringan	*Kawalan* Semakan penentusahan latar belakang ke atas semua calon untuk penjawatan hendaklah dilakukan menurut undang-undang, peraturan dan etika yang berkaitan dan hendaklah bersesuaian dengan keperluan perniagaan, klasifikasi maklumat yang hendak diakses dan risiko yang dikenal pasti.
A.7.1.2	Terma dan syarat penjawatan	*Kawalan* Persetujuan berkontrak dengan kakitangan dan kontraktor hendaklah menyatakan tanggungjawab mereka dan tanggungjawab organisasi terhadap keselamatan maklumat.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.7.2 Dalam tempoh penjawatan		
Objektif: Memastikan kakitangan dan kontraktor mengetahui dan memenuhi tanggungjawab keselamatan maklumat mereka.		
A.7.2.1	Tanggungjawab pengurusan	*Kawalan* Pengurusan hendaklah menghendaki semua kakitangan dan kontraktor supaya mengamalkan keselamatan maklumat menurut dasar dan prosedur organisasi yang ditetapkan.
A.7.2.2	Kesedaran, pendidikan dan latihan tentang keselamatan maklumat	*Kawalan* Semua kakitangan organisasi dan, jika berkaitan, kontraktor hendaklah diberikan kesedaran, pendidikan dan latihan sewajarnya dan menerima maklumat secara tetap tentang dasar dan prosedur organisasi, yang berkaitan dengan fungsi tugas mereka.
A.7.2.3	Proses tatatertib	*Kawalan* Proses tatatertib yang formal hendaklah diadakan dan disampaikan kepada kakitangan bagi membolehkan tindakan diambil terhadap mereka yang melakukan pelanggaran keselamatan maklumat.
A.7.3 Penamatan dan pertukaran penjawatan		
Objektif: Melindungi kepentingan organisasi sebagai sebahagian daripada proses pertukaran atau penamatan penjawatan.		
A.7.3.1	Penamatan atau pertukaran tanggungjawab penjawatan	*Kawalan* Tanggungjawab dan tugas keselamatan maklumat yang masih sah selepas penamatan atau pertukaran penjawatan hendaklah ditakrifkan, disampaikan kepada kakitangan dan kontraktor dan dikuatkuasakan.
A.8 Pengurusan aset		
A.8.1 Tanggungjawab terhadap aset		
Objektif: Mengenal pasti aset organisasi dan mentakrifkan tanggungjawab perlindungan yang sewajarnya.		
A.8.1.1	Inventori aset	*Kawalan* Maklumat, lain-lain aset yang dikaitkan dengan maklumat, dan fasiliti pemprosesan maklumat hendaklah dikenal pasti dan inventori aset ini hendaklah disediakan dan disenggarakan.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.8.1.2	Pemilikan aset	*Kawalan* Aset yang disenggara dalam inventori hendaklah mempunyai pemilik.
A.8.1.3	Penggunaan aset yang dibenarkan	*Kawalan* Peraturan penggunaan yang dibenarkan bagi maklumat dan aset yang dikaitkan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti, didokumenkan dan dilaksanakan.
A.8.1.4	Pemulangan aset	*Kawalan* Semua kakitangan dan pengguna pihak luar hendaklah memulangkan semua aset organisasi yang berada dalam pemilikannya apabila ditamatkan penjawatan, kontrak atau perjanjian mereka.
A.8.2 Pengelasan maklumat		
Objektif: Memastikan maklumat mendapat tahap perlindungan yang sesuai menurut kepentingannya kepada organisasi.		
A.8.2.1	Pengelasan maklumat	*Kawalan* Maklumat hendaklah dikelaskan berdasarkan keperluan undang-undang, nilai, tahap kritikal dan sensitiviti terhadap pendedahan atau pengubahsuaian yang tidak dibenarkan.
A.8.2.2	Pelabelan maklumat	*Kawalan* Set prosedur yang sesuai untuk pelabelan maklumat hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.
A.8.2.3	Pengendalian aset	*Kawalan* Prosedur pengendalian aset hendaklah dibangunkan dan dilaksanakan menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.
A.8.3 Pengendalian media		
Objektif: Mencegah pendedahan, pengubahsuaian, penyingkiran, atau pemusnahan tanpa kebenaran terhadap maklumat yang disimpan dalam media.		
A.8.3.1	Pengurusan media boleh alih	*Kawalan* Prosedur hendaklah dilaksanakan bagi pengurusan media boleh alih menurut skim pengelasan maklumat yang diterima pakai oleh organisasi.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.8.3.2	Pelupusan media	*Kawalan* Media hendaklah dilupuskan dengan selamat melalui prosedur formal apabila tidak diperlukan lagi.
A.8.3.3	Pemindahan media fizikal	*Kawalan* Media yang mengandungi maklumat hendaklah dilindungi daripada akses tanpa izin, penyalahgunaan atau kerosakan semasa pengangkutan.
A.9 Kawalan akses		
A.9.1 Kawalan akses bagi keperluan perniagaan		
Objektif: Mengehadkan akses kepada maklumat dan kemudahan pemprosesan maklumat.		
A.9.1.1	Dasar kawalan akses	*Kawalan* Dasar kawalan akses hendaklah diwujudkan, didokumenkan dan dikaji semula berdasarkan keperluan perniagaan dan keperluan keselamatan maklumat.
A.9.1.2	Akses kepada rangkaian dan perkhidmatan rangkaian	*Kawalan* Pengguna hanya hendaklah diberikan akses kepada rangkaian dan perkhidmatan rangkaian yang dibenarkan secara khusus.
A.9.2 Pengurusan akses pengguna		
Objektif: Memastikan akses oleh pengguna yang dibenarkan dan menghalang akses tanpa izin kepada sistem dan perkhidmatan.		
A.9.2.1	Pendaftaran dan pembatalan pengguna	*Kawalan* Proses formal pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan pemberian hak akses.
A.9.2.2	Peruntukan akses pengguna	*Kawalan* Proses formal peruntukan akses pengguna hendaklah dilaksanakan dalam pemberian atau pembatalan hak akses kepada semua jenis pengguna untuk semua sistem dan perkhidmatan.
A.9.2.3	Pengurusan hak akses istimewa	*Kawalan* Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.9.2.4	Pengurusan maklumat pengesahan rahsia pengguna	*Kawalan* Peruntukan maklumat pengesahan rahsia hendaklah dikawal melalui proses pengurusan formal.
A.9.2.5	Kajian semula hak akses pengguna	*Kawalan* Pemilik aset hendaklah mengkaji semula hak akses pengguna pada sela masa tetap.
A.9.2.6	Penyingkiran atau pelarasan hak akses	*Kawalan* Hak akses semua kakitangan dan pengguna pihak luar kepada maklumat dan kemudahan pemprosesan maklumat hendaklah disingkirkan apabila ditamatkan penjawatan, kontrak atau perjanjian, atau diselaraskan apabila terdapat perubahan.
A.9.3 Tanggungjawab pengguna		
Objektif: Memastikan pengguna bertanggungjawab melindungi maklumat pengesahan mereka.		
A.9.3.1	Penggunaan maklumat pengesahan rahsia	*Kawalan* Pengguna dikehendaki mematuhi amalan organisasi dalam menggunakan maklumat pengesahan rahsia.
A.9.4 Kawalan akses sistem dan aplikasi		
Objektif: Menghalang akses tanpa izin kepada sistem dan aplikasi.		
A.9.4.1	Sekatan akses maklumat	*Kawalan* Akses kepada maklumat dan fungsi sistem aplikasi hendaklah dihadkan menurut dasar kawalan akses.
A.9.4.2	Prosedur log masuk yang selamat	*Kawalan* Jika dikehendaki oleh dasar kawalan akses, akses kepada sistem dan aplikasi hendaklah dikawal oleh prosedur log masuk yang selamat.
A.9.4.3	Sistem pengurusan kata laluan	*Kawalan* Sistem pengurusan kata laluan hendaklah interaktif dan memastikan kata laluan yang berkualiti.
A.9.4.4	Penggunaan program utiliti yang mempunyai hak istimewa	*Kawalan* Penggunaan program utiliti yang mungkin mampu melepasi kawalan sistem dan aplikasi hendaklah disekat dan dikawal dengan ketat.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.9.4.5	Kawalan akses kepada kod sumber program	*Kawalan* Akses kepada kod sumber program hendaklah dihadkan.
A.10 Kriptografi		
A.10.1 Kawalan kriptografi		
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan bagi melindungi kerahsiaan, kesahihan dan/atau integriti maklumat.		
A.10.1.1	Dasar penggunaan kawalan kriptografi	*Kawalan* Dasar penggunaan kawalan kriptografi bagi melindungi maklumat hendaklah dibangunkan dan dilaksanakan.
A.10.1.2	Pengurusan kekunci	*Kawalan* Dasar penggunaan, perlindungan dan tempoh hayat kekunci kriptografi hendaklah dibangunkan dan dilaksanakan sepanjang kitar hayatnya.
A.11 Keselamatan fizikal dan persekitaran		
A.11.1 Kawasan selamat		
Objektif: Menghalang akses fizikal tanpa kebenaran, kerosakan dan gangguan terhadap maklumat dan kemudahan pemprosesan maklumat organisasi.		
A.11.1.1	Perimeter keselamatan fizikal	*Kawalan* Perimeter keselamatan hendaklah ditakrifkan dan digunakan bagi melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat yang sensitif atau kritikal.
A.11.1.2	Kawalan kemasukan fizikal	*Kawalan* Kawasan selamat hendaklah dilindungi oleh kawalan kemasukan yang sesuai bagi memastikan kakitangan yang diberi kebenaran sahaja dibenarkan masuk.
A.11.1.3	Keselamatan pejabat, bilik dan kemudahan	*Kawalan* Keselamatan fizikal untuk pejabat, bilik dan kemudahan hendaklah direka bentuk dan dilaksanakan.
A.11.1.4	Perlindungan daripada ancaman luar dan persekitaran	*Kawalan* Perlindungan fizikal daripada bencana alam, serangan hasad atau kemalangan hendaklah direka bentuk dan dilaksanakan.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.11.1.5	Bekerja di kawasan selamat	*Kawalan* Prosedur bekerja di kawasan selamat hendaklah direka bentuk dan dilaksanakan.
A.11.1.6	Kawasan penyerahan dan pemunggahan	*Kawalan* Akses keluar masuk seperti kawasan penyerahan dan pemunggahan serta akses lain yang membolehkan mereka yang tidak dibenarkan melaluinya untuk memasuki premis hendaklah dikawal, dan jika boleh, diasingkan daripada kemudahan pemprosesan maklumat bagi mengelakkan akses tanpa kebenaran.
A.11.2 Peralatan		
Objektif: Untuk mengelakkan kehilangan, kerosakan, kecurian atau penjejasan aset dan gangguan terhadap operasi organisasi.		
A.11.2.1	Penempatan dan perlindungan peralatan	*Kawalan* Peralatan hendaklah ditentukan penempatannya dan dilindungi bagi mengurangkan risiko ancaman dan bahaya persekitaran, dan peluang akses tanpa kebenaran.
A.11.2.2	Utiliti sokongan	*Kawalan* Peralatan hendaklah dilindungi daripada kegagalan bekalan kuasa dan gangguan lain yang disebabkan oleh kegagalan utiliti sokongan.
A.11.2.3	Keselamatan kabel	*Kawalan* Kabel bekalan kuasa dan telekomunikasi yang membawa data atau menyokong perkhidmatan maklumat hendaklah dilindungi daripada pintasan, gangguan atau kerosakan.
A.11.2.4	Penyenggaraan peralatan	*Kawalan* Peralatan hendaklah disenggara dengan betul bagi memastikan ketersediaan dan integriti yang berterusan.
A.11.2.5	Pengalihan aset	*Kawalan* Peralatan, maklumat atau perisian tidak boleh dibawa keluar dari premis tanpa mendapat kebenaran terlebih dahulu.
A.11.2.6	Keselamatan peralatan dan aset di luar premis	*Kawalan* Keselamatan aset di luar premis hendaklah dipastikan dengan mengambil kira pelbagai risiko bekerja di luar premis organisasi.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.11.2.7	Pelupusan yang selamat atau penggunaan semula peralatan	*Kawalan* Semua bahagian peralatan yang mengandungi media penyimpanan hendaklah disahkan bagi memastikan sebarang data yang sensitif dan perisian berlesen telah dikeluarkan atau berjaya ditulis ganti sebelum dilupuskan atau diguna semula.
A.11.2.8	Peralatan pengguna tanpa jagaan	*Kawalan* Pengguna hendaklah memastikan peralatan yang dibiarkan tanpa jagaan mempunyai perlindungan sewajarnya.
A.11.2.9	Dasar meja bersih dan skrin kosong	*Kawalan* Dasar meja bersih untuk pengendalian kertas dan media penyimpanan boleh alih serta dasar skrin kosong untuk kemudahan pemprosesan maklumat hendaklah digunakan.
A.12 Keselamatan operasi		
A.12.1 Prosedur dan tanggungjawab operasi		
Objektif: Memastikan operasi kemudahan pemprosesan maklumat yang betul dan selamat.		
A.12.1.1	Prosedur operasi yang didokumenkan	*Kawalan* Prosedur operasi hendaklah didokumenkan dan disediakan untuk semua pengguna yang memerlukannya.
A.12.1.2	Pengurusan perubahan	*Kawalan* Perubahan dalam organisasi, proses perniagaan, kemudahan pemprosesan maklumat dan sistem yang menjejaskan keselamatan maklumat hendaklah dikawal.
A.12.1.3	Pengurusan kapasiti	*Kawalan* Penggunaan sumber hendaklah dipantau, disesuaikan dan unjuran hendaklah disediakan untuk keperluan kapasiti masa hadapan bagi memastikan prestasi sistem yang dikehendaki dicapai.
A.12.1.4	Pengasingan persekitaran pembangunan, pengujian dan operasi	*Kawalan* Persekitaran pembangunan, pengujian dan operasi hendaklah diasingkan bagi mengurangkan risiko akses tanpa izin atau perubahan kepada persekitaran operasi.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.12.2 Perlindungan daripada perisian hasad		
Objektif: Memastikan maklumat dan kemudahan pemprosesan maklumat dilindungi daripada perisian hasad.		
A.12.2.1	Kawalan daripada perisian hasad	*Kawalan* Kawalan pengesanan, pencegahan dan pemulihan untuk memberikan perlindungan daripada perisian hasad hendaklah dilaksanakan, digabungkan dengan kesedaran pengguna yang sewajarnya.
A.12.3 Sandaran		
Objektif: Melindungi kehilangan data.		
A.12.3.1	Sandaran maklumat	*Kawalan* Salinan sandaran maklumat, perisian dan imej sistem hendaklah diambil dan diuji secara tetap menurut dasar sandaran yang dipersetujui.
A.12.4 Pengelogan dan pemantauan		
Objektif: Merekodkan kejadian dan menghasilkan bukti.		
A.12.4.1	Pengelogan kejadian	*Kawalan* Log kejadian yang merekodkan aktiviti pengguna, pengecualian, ralat dan kejadian keselamatan maklumat hendaklah dihasilkan, disimpan dan dikaji semula secara tetap.
A.12.4.2	Perlindungan maklumat log	*Kawalan* Kemudahan pengelogan dan maklumat log hendaklah dilindungi daripada ubahan dan akses tanpa izin.
A.12.4.3	Log pentadbir dan pengendali	*Kawalan* Aktiviti pentadbir sistem dan pengendali sistem hendaklah direkodkan dan log tersebut hendaklah dilindungi dan dikaji semula secara tetap.
A.12.4.4	Penyegerakan jam	*Kawalan* Jam bagi semua sistem pemprosesan maklumat yang berkaitan dalam sesebuah domain organisasi atau domain keselamatan hendaklah disegerakkan mengikut satu sumber rujukan masa.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.12.5 Kawalan perisian yang beroperasi		
Objektif: Memastikan kewibawaan sistem yang beroperasi.		
A.12.5.1	Pemasangan perisian pada sistem yang beroperasi	*Kawalan* Prosedur hendaklah dilaksanakan untuk mengawal pemasangan perisian pada sistem yang beroperasi.
A.12.6 Pengurusan kerentanan teknikal		
Objektif: Mencegah eksploitasi kerentanan teknikal.		
A.12.6.1	Pengurusan kerentanan teknikal	*Kawalan* Maklumat tentang kerentanan teknikal sistem maklumat yang digunakan hendaklah diperoleh pada masa yang tepat, pendedahan organisasi terhadap kerentanan tersebut hendaklah dinilai dan langkah-langkah yang sesuai hendaklah diambil untuk menangani risiko yang berkaitan.
A.12.6.2	Sekatan ke atas pemasangan perisian	*Kawalan* Peraturan yang mengawal pemasangan perisian oleh pengguna hendaklah disediakan dan dilaksanakan.
A.12.7 Pertimbangan tentang audit sistem maklumat		
Objektif: Meminimumkan kesan aktiviti audit ke atas sistem yang beroperasi.		
A.12.7.1	Kawalan audit sistem maklumat	*Kawalan* Keperluan dan aktiviti audit yang melibatkan penentusahan sistem yang beroperasi hendaklah dirancang dengan teliti dan dipersetujui bagi meminimumkan gangguan ke atas proses perniagaan.
A.13 Keselamatan komunikasi		
A.13.1 Pengurusan keselamatan rangkaian		
Objektif: Memastikan perlindungan maklumat dalam rangkaian dan dalam kemudahan sokongan pemprosesan maklumat dalam rangkaian.		
A.13.1.1	Kawalan rangkaian	*Kawalan* Rangkaian hendaklah diurus dan dikawal bagi melindungi maklumat dalam sistem dan aplikasi.
A.13.1.2	Keselamatan perkhidmatan rangkaian	*Kawalan* Mekanisme keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian hendaklah dikenal pasti dan dimasukkan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan ini disediakan secara dalaman atau oleh khidmat luaran.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.13.1.3	Pengasingan dalam rangkaian	*Kawalan* Kelompok perkhidmatan maklumat, pengguna dan sistem maklumat hendaklah diasingkan dalam rangkaian.
A.13.2 Pemindahan maklumat		
Objektif: Memelihara keselamatan maklumat yang dipindahkan dalam sesebuah organisasi dan dengan mana-mana entiti luaran.		
A.13.2.1	Dasar dan prosedur pemindahan maklumat	*Kawalan* Dasar, prosedur dan kawalan pemindahan formal hendaklah disediakan bagi melindungi pemindahan maklumat melalui penggunaan semua jenis kemudahan komunikasi.
A.13.2.2	Perjanjian tentang pemindahan maklumat	*Kawalan* Perjanjian hendaklah menangani aspek keselamatan dalam pemindahan maklumat perniagaan antara organisasi dengan pihak luaran.
A.13.2.3	Pesanan elektronik	*Kawalan* Maklumat yang terlibat dalam pesanan elektronik hendaklah dilindungi sewajarnya.
A.13.2.4	Perjanjian kerahsiaan atau ketakdedahan	*Kawalan* Keperluan untuk perjanjian kerahsiaan atau ketakdedahan yang menggambarkan keperluan organisasi terhadap perlindungan maklumat hendaklah dikenal pasti, dikaji semula dan didokumenkan secara tetap.
A.14 Pemerolehan, pembangunan dan penyenggaraan sistem		
A.14.1 Keperluan keselamatan sistem maklumat		
Objektif: Memastikan keselamatan maklumat dijadikan bahagian penting dalam sistem maklumat sepanjang kitar hayat. Ini juga termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan melalui rangkaian awam.		
A.14.1.1	Analisis dan spesifikasi keperluan keselamatan maklumat	*Kawalan* Keperluan berkaitan keselamatan maklumat hendaklah disertakan dalam keperluan untuk sistem maklumat baharu atau penambahbaikan pada sistem maklumat sedia ada.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.14.1.2	Melindungi perkhidmatan aplikasi dalam rangkaian awam	*Kawalan* Maklumat yang terlibat dalam perkhidmatan aplikasi yang disebarkan melalui rangkaian awam hendaklah dilindungi daripada aktiviti pemalsuan, pertikaian kontrak serta pendedahan dan pengubahsuaian yang tidak dibenarkan.
A.14.1.3	Melindungi transaksi perkhidmatan aplikasi	*Kawalan* Maklumat yang terlibat dalam transaksi perkhidmatan aplikasi hendaklah dilindungi bagi mengelakkan penghantaran tidak sempurna, salah hala, pindaan mesej tanpa kebenaran, pendedahan tanpa kebenaran, duplikasi atau ulang tayang mesej tanpa kebenaran.
A.14.2 Keselamatan dalam proses pembangunan dan sokongan		
Objektif: Memastikan keselamatan maklumat direka bentuk dan dilaksanakan dalam kitar hayat pembangunan sistem maklumat.		
A.14.2.1	Dasar pembangunan selamat	*Kawalan* Peraturan bagi pembangunan perisian dan sistem hendaklah disediakan dan digunakan untuk pembangunan dalam organisasi.
A.14.2.2	Prosedur kawalan perubahan sistem	*Kawalan* Perubahan pada sistem dalam kitar hayat pembangunan hendaklah dikawal dengan menggunakan prosedur kawalan perubahan formal.
A.14.2.3	Kajian semula teknikal bagi aplikasi selepas perubahan platform operasi	*Kawalan* Apabila platform operasi berubah, aplikasi penting perniagaan hendaklah dikaji semula dan diuji bagi memastikan tiada impak yang menjejaskan ke atas operasi atau keselamatan organisasi.
A.14.2.4	Sekatan ke atas perubahan dalam pakej perisian	*Kawalan* Pengubahsuaian ke atas pakej perisian adalah tidak digalakkan, terhad kepada perubahan yang perlu dan semua perubahan hendaklah dikawal dengan ketat.
A.14.2.5	Prinsip kejuruteraan sistem yang selamat	*Kawalan* Prinsip kejuruteraan bagi sistem yang selamat hendaklah diwujudkan, didokumenkan, disenggara dan digunakan untuk sebarang usaha pelaksanaan sistem maklumat.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.14.2.6	Persekitaran pembangunan selamat	*Kawalan* Organisasi hendaklah mewujudkan dan melindungi sewajarnya persekitaran pembangunan selamat untuk pembangunan sistem dan usaha integrasi yang meliputi seluruh kitar hayat pembangunan sistem.
A.14.2.7	Pembangunan oleh khidmat luaran	*Kawalan* Organisasi hendaklah menyelia dan memantau aktiviti pembangunan sistem yang dijalankan oleh khidmat luaran.
A.14.2.8	Pengujian keselamatan sistem	*Kawalan* Pengujian fungsian keselamatan hendaklah dijalankan semasa pembangunan.
A.14.2.9	Pengujian penerimaan sistem	*Kawalan* Program pengujian penerimaan dan kriteria yang berkaitan hendaklah disediakan untuk sistem maklumat yang baharu, yang ditambah baik dan versi baharu.
A.14.3 Data ujian		
Objektif: Memastikan perlindungan bagi data yang digunakan untuk pengujian.		
A.14.3.1	Perlindungan data ujian	*Kawalan* Data ujian hendaklah dipilih dengan teliti, dilindungi dan dikawal.
A.15 Hubungan pembekal		
A.15.1 Keselamatan maklumat dalam hubungan pembekal		
Objektif: Memastikan perlindungan aset organisasi yang boleh diakses oleh pembekal.		
A.15.1.1	Dasar keselamatan maklumat untuk hubungan pembekal	*Kawalan* Keperluan keselamatan maklumat untuk mengurangkan risiko yang dikaitkan dengan akses pembekal kepada aset organisasi hendaklah dipersetujui dengan pembekal dan didokumenkan.
A.15.1.2	Menangani keselamatan dalam perjanjian pembekal	*Kawalan* Semua keperluan keselamatan maklumat yang berkaitan hendaklah diwujudkan dan dipersetujui dengan setiap pembekal yang boleh mengakses, memproses, menyimpan, menyampaikan, atau menyediakan komponen infrastruktur IT untuk maklumat organisasi.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.15.1.3	Rantaian bekalan teknologi maklumat dan komunikasi	*Kawalan* Perjanjian dengan pembekal hendaklah mengandungi keperluan untuk menangani risiko keselamatan maklumat yang dikaitkan dengan perkhidmatan teknologi maklumat dan komunikasi serta rantaian bekalan produk.
A.15.2 Pengurusan penyampaian perkhidmatan pembekal		
Objektif: Mengekalkan tahap keselamatan maklumat dan penyampaian perkhidmatan yang dipersetujui selaras dengan perjanjian pembekal.		
A.15.2.1	Memantau dan mengkaji semula perkhidmatan pembekal	*Kawalan* Organisasi hendaklah memantau, mengkaji semula dan mengaudit penyampaian perkhidmatan pembekal secara tetap.
A.15.2.2	Menguruskan perubahan kepada perkhidmatan pembekal	*Kawalan* Perubahan kepada perolehan perkhidmatan daripada pembekal, termasuk mengekalkan dan menambah baik dasar keselamatan maklumat sedia ada, prosedur dan kawalan, hendaklah diuruskan, dengan mengambil kira kegentingan maklumat, sistem dan proses perniagaan yang terlibat dan pentaksiran semula risiko.
A.16 Pengurusan insiden keselamatan maklumat		
A.16.1 Pengurusan insiden keselamatan maklumat dan penambahbaikan		
Objektif: Memastikan pendekatan yang konsisten dan berkesan dalam pengurusan insiden keselamatan maklumat, termasuk komunikasi tentang kejadian dan kelemahan keselamatan.		
A.16.1.1	Tanggungjawab dan prosedur	*Kawalan* Tanggungjawab pengurusan dan prosedur hendaklah diwujudkan bagi memastikan tindak balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat.
A.16.1.2	Pelaporan kejadian keselamatan maklumat	*Kawalan* Kejadian keselamatan maklumat hendaklah dilaporkan melalui saluran pengurusan yang bersesuaian dengan secepat mungkin.
A.16.1.3	Pelaporan kelemahan keselamatan maklumat	*Kawalan* Kakitangan dan kontraktor yang menggunakan sistem dan perkhidmatan maklumat organisasi adalah dikehendaki mencatatkan dan melaporkan sebarang kelemahan keselamatan maklumat yang diperhatikan atau disyaki dalam sistem atau perkhidmatan.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.16.1.4	Penilaian dan keputusan tentang kejadian keselamatan maklumat	*Kawalan* Kejadian keselamatan maklumat hendaklah dinilai dan ditentukan jika ia perlu dikelaskan sebagai insiden keselamatan maklumat.
A.16.1.5	Tindak balas terhadap insiden keselamatan maklumat	*Kawalan* Insiden keselamatan maklumat hendaklah ditangani menurut prosedur yang didokumenkan.
A.16.1.6	Mempelajari daripada insiden keselamatan maklumat	*Kawalan* Pengetahuan yang diperoleh daripada analisis dan penyelesaian insiden keselamatan maklumat hendaklah digunakan bagi mengurangkan kemungkinan berlakunya insiden atau impak insiden mendatang.
A.16.1.7	Pengumpulan bahan bukti	*Kawalan* Organisasi hendaklah mentakrifkan dan menggunakan prosedur untuk mengenal pasti, mengumpul, memperoleh dan memelihara maklumat yang boleh digunakan sebagai bahan bukti.
A.17 Aspek keselamatan maklumat bagi pengurusan kesinambungan perniagaan		
A.17.1 Kesinambungan keselamatan maklumat		
Objektif: Kesinambungan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perniagaan organisasi.		
A.17.1.1	Perancangan kesinambungan keselamatan maklumat	*Kawalan* Organisasi hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat dalam keadaan yang menjejaskan, contohnya, semasa krisis atau bencana.
A.17.1.2	Pelaksanaan kesinambungan keselamatan maklumat	*Kawalan* Organisasi hendaklah mewujudkan, mendokumenkan, melaksanakan dan menyenggarakan proses, prosedur dan kawalan bagi memastikan keperluan tahap kesinambungan keselamatan maklumat ketika berada dalam keadaan yang menjejaskan.

Jadual A.1 – Objektif kawalan dan kawalan *(sambungan)*

A.17.1.3	Menentusahkan, mengkaji semula dan menilai kesinambungan keselamatan maklumat	*Kawalan* Organisasi hendaklah menentusahkan kawalan kesinambungan keselamatan maklumat yang diwujudkan dan dilaksanakan pada sela masa tetap bagi memastikan ianya sahih dan berkesan semasa keadaan yang menjejaskan.
A.17.2 Lewahan		
Objektif: Memastikan ketersediaan kemudahan pemprosesan maklumat.		
A.17.2.1	Ketersediaan kemudahan pemprosesan maklumat	*Kawalan* Kemudahan pemprosesan maklumat hendaklah dilaksanakan dengan lewahan yang mencukupi bagi memenuhi keperluan ketersediaan.
A.18 Pematuhan		
A.18.1 Pematuhan kepada keperluan undang-undang dan kontrak		
Objektif: Mengelakkan pelanggaran obligasi undang-undang, statutori, kawal selia atau kontrak yang berkaitan dengan keselamatan maklumat dan sebarang keperluan keselamatan.		
A.18.1.1	Pengenalpastian keperluan undang-undang dan kontrak yang terpakai	*Kawalan* Semua keperluan perundangan, statutori, kawal selia, kontrak yang berkaitan dan pendekatan organisasi bagi memenuhi keperluan ini hendaklah dikenal pasti dengan jelas, didokumenkan dan dikemas kini bagi setiap sistem maklumat dan organisasi.
A.18.1.2	Hak harta intelek	*Kawalan* Prosedur yang sesuai hendaklah dilaksanakan bagi memastikan keperluan pematuhan perundangan, kawal selia dan kontrak yang berkaitan dengan hak harta intelek dan penggunaan produk perisian proprietari.
A.18.1.3	Perlindungan rekod	*Kawalan* Rekod perlu dilindungi daripada kehilangan, kemusnahan, pemalsuan, akses tanpa izin dan pengeluaran tanpa kebenaran, mengikut keperluan undang-undang, kawal selia, kontrak dan perniagaan.
A.18.1.4	Privasi dan perlindungan maklumat peribadi	*Kawalan* Privasi dan perlindungan maklumat peribadi hendaklah dipastikan seperti yang dikehendaki dalam undang-undang dan peraturan yang relevan jika berkenaan.

Jadual A.1 – Objektif kawalan dan kawalan *(penyudahan)*

A.18.1.5	Peraturan kawalan kriptografi	*Kawalan* Kawalan kriptografi hendaklah digunakan bagi mematuhi semua perjanjian, undang-undang dan peraturan yang relevan.
A.18.2 Kajian semula keselamatan maklumat		
Objektif: Memastikan keselamatan maklumat dilaksanakan dan dikendalikan menurut dasar dan prosedur organisasi.		
A.18.2.1	Kajian semula keselamatan maklumat secara berkecuali	*Kawalan* Pendekatan organisasi dalam menguruskan keselamatan maklumat dan pelaksanaannya (iaitu, objektif kawalan, kawalan, dasar, proses dan prosedur untuk keselamatan maklumat) hendaklah dikaji semula secara berkecuali pada sela masa yang dirancang atau apabila berlaku perubahan yang ketara.
A.18.2.2	Pematuhan dasar dan standard keselamatan	*Kawalan* Pengurus hendaklah mengkaji semula secara tetap pematuhan pemprosesan maklumat dan prosedur dalam bidang tanggungjawabnya terhadap dasar keselamatan yang bersesuaian, standard dan sebarang keperluan keselamatan yang lain.
A.18.2.3	Kajian semula pematuhan teknikal	*Kawalan* Sistem maklumat hendaklah dikaji semula secara tetap bagi mematuhi dasar dan standard keselamatan maklumat organisasi.

Bibliografi

[1] ISO/IEC 27002:2013, *Information technology - Security techniques - Code of practice for information security controls*

[2] ISO/IEC 27003, *Information technology - Security techniques - Information security management system implementation guidance*

[3] ISO/IEC 27004, *Information technology - Security techniques - Information security management - Measurement*

[4] ISO/IEC 27005, *Information technology - Security techniques - Information security risk management*

[5] ISO 31000:2009, *Risk management - Principles and guidelines*

[6] ISO/IEC Directives, Part 1, *Consolidated ISO Supplement - Procedures specific to ISO*, 2012

Penghargaan

Ahli Jawatankuasa Teknikal mengenai Keselamatan Maklumat

Encik Thaib Mustafa (Pengerusi)	TM Applied Business Sdn Bhd
Dr Solahuddin Shamsuddin (Timbalan Pengerusi)	CyberSecurity Malaysia
Cik Salwa Denan (Setiausaha)	SIRIM Berhad
Lt Kol (B) Sazali Sukardi	CyberSecurity Malaysia
Encik Tan Chuan Ou	Kementerian Sains, Teknologi dan Inovasi
Encik Tan Tze Meng	Malaysia Digital Economy Corporation Sdn Bhd
Encik Ng Kang Siong	MIMOS Berhad
Puan Julaila Engan	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Dr Dzaharudin Mansor	Persatuan Industri Komputer dan Multimedia Malaysia
Encik Abd Rahman Abas	POS Malaysia Berhad
Puan Ong Ai Lin/ Encik Tan Cheng Yeong/ Encik Ismail Awang	PricewaterhouseCoopers Risk Services Sdn Bhd
Puan Sazlin Alias	SIRIM QAS International Sdn Bhd
Puan Azleyna Arifin	Suruhanjaya Komunikasi dan Multimedia Malaysia
Puan Sophia Hashim/ Puan Nur Hidayah Abdullah	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia

Penghargaan (*sambungan*)

Ahli Kumpulan Kerja mengenai Sistem Pengurusan Keselamatan Maklumat

Puan Raja Azrina Raja Othman (Pengerusi)	VADS Berhad
Puan Azleyna Arifin (Timbalan Pengerusi)	Suruhanjaya Komunikasi dan Multimedia Malaysia
Cik Salwa Denan (Setiausaha)	SIRIM Berhad
Puan Maslina Daud/ Puan Wan Nasra Wan Fairuz	CyberSecurity Malaysia
Puan Juliaty Abdul Rahman	Malaysian Electronic Payment System Sdn Bhd
Puan Nor Aza Ramli	Pakar bebas
Encik Ismail Awang	PricewaterhouseCoopers Risk Services Sdn Bhd
Puan Fatin Nabiha Abdul Aziz	Suruhanjaya Komunikasi dan Multimedia Malaysia
Encik Thaib Mustafa/ Puan Azrina Ibramsha	TM Applied Business Sdn Bhd
Puan Aaishah Dato' Abu Bakar/ Puan Ita Nurazlin Mohd Sahlan	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
Dr Normaziah Abdul Aziz	Universiti Islam Antarabangsa Malaysia
Dr Azah Anir Norman	Universiti Malaya
Prof Madya Dr Omar Zakaria	Universiti Pertahanan Nasional Malaysia

Ahli ambilan

Encik Shamsul Baharin Deraman/ Encik Noorhisam Rusmani	RHB Bank Berhad