SNI

Standar Nasional Indonesia

SNI ISO/IEC 27001:2009

Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

Information technology – Security techniques – Information security management systems – Requirements
(*ISO/IEC 27001:2005, IDT*)

ICS 35.040

Badan Standardisasi Nasional

Daftar isi

Prakata iii
Pendahuluan iv
0.1 Umum iv
0.2 Pendekatan proses iv
0.3 Kesesuaian dengan sistem manajemen lainnya vi
1 Ruang lingkup 1
1.1 Umum 1
1.2 Penerapan 1
2 Acuan normatif 2
3 Istilah dan definisi 2
4 Sistem manajemen keamanan informasi 4
4.1 Persyaratan umum 4
4.2 Penetapan dan pengelolaan SMKI 4
4.2.1 Menetapkan SMKI 4
4.2.2 Menerapkan dan Mengoperasikan SMKI 6
4.2.3 Memantau dan Mengkaji SMKI 6
4.2.4 Memelihara dan Meningkatkan SMKI 7
4.3 Persyaratan dokumentasi 8
4.3.1 Umum 8
4.3.2 Pengendalian dokumen 8
4.3.3 Pengendalian rekaman 9
5 Tanggung jawab manajemen 9
5.1 Komitmen manajemen 9
5.2 Manajemen sumberdaya 10
5.2.1 Ketentuan sumberdaya 10
5.2.2 Pelatihan, kepedulian dan kompetensi 10
6 Audit internal SMKI 10
7 Kajian manajemen SMKI 11
7.1 Umum 11
7.2 Masukan Kajian 11
7.3 Luaran Kajian 12
8 Peningkatan SMKI 12

8.1 Peningkatan berkelanjutan 12
8.2 Tindakan korektif 12
8.3 Tindakan pencegahan 12
Lampiran A (normatif) Sasaran pengendalian dan pengendalian 14
Lampiran B (informatif)Prinsip-prinsip OECD dan ISO 27001 Prinsip OECD dan standar ini 35
Lampiran C (informatif) Kesesuaian antara SNI 19-9001-2001, SNI 19 – 14001 – 2005 dan Standar ini 37
Bibliografi 40

Prakata

Standar SNI ISO/IEC 27001:2009 "Teknologi informasi – Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan" disusun secara adopsi identik terhadap standar *ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements,* dengan metode terjemahan oleh Panitia Teknis PK 03-02 Sistem Manajemen Mutu yang dibentuk oleh BSN.

Penyusunan standar ini disepakati dalam rapat konsensus yang diselenggarakan pada tanggal 12 Agustus 2009 di Bogor dengan dihadiri oleh anggota Panitia Teknis Sistem Manajemen Mutu sebagai wakil dari pemangku kepentingan (stakeholder) dan narasumber.

Lampiran A dalam standar ini bersifat normatif sedangkan Lampiran B dan Lampiran C dalam standar ini hanya untuk informasi.

Pendahuluan

0.1 Umum

Standar ini dibuat sebagai model untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan Sistem Manajemen Keamanan Informasi (SMKI). Adopsi SMKI merupakan keputusan strategis organisasi. Desain dan penerapan SMKI dari suatu organisasi dipengaruhi oleh kebutuhan dan sasaran organisasi. Standar ini dan sistem pendukungnya diperkirakan akan berubah dari waktu ke waktu. Penerapan SMKI di sesuaikan dengan kebutuhan organisasi, misalnya situasi sederhana mensyaratkan penyelesaian SMKI yang sederhana.

Standar ini dapat digunakan untuk menilai kesesuaian oleh pihak terkait baik internal maupun eksternal.

0.2 Pendekatan proses

Standar ini mengadopsi pendekatan proses untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan perbaikan SMKI suatu organisasi.

Organisasi perlu mengidentifikasi dan mengatur seluruh kegiatannya agar berfungsi dengan efektif. Semua kegiatan yang menggunakan sumber daya dan dikelola untuk memudahkan transformasi masukan (input) ke dalam keluaran (output) dapat dianggap sebagai suatu proses. Seringkali keluaran dari satu proses secara langsung menjadi masukan untuk proses selanjutnya.

Penerapan dari suatu sistem proses dalam organisasi, bersama dengan identifikasi dan interaksi dalam proses tersebut dan manajemennya, dapat diacu sebagai suatu “pendekatan proses”.

Pendekatan proses untuk manajemen keamanan informasi yang dituangkan dalam Standar ini mendorong penggunanya untuk menekankan tentang pentingnya:

a) pemahaman persyaratan keamanan informasi dari suatu organisasi dan kebutuhan untuk membuat kebijakan dan sasaran untuk keamanan informasi;

b) penerapan dan pengoperasian kendali untuk mengatur risiko-risiko keamanan informasi dari suatu organisasi dalam konteks risiko bisnis dari organisasi secara keseluruhan;

c) pemantauan dan pengkajian kinerja dan keefektifan SMKI; dan

d) perbaikan berkesinambungan berdasarkan pengukuran sasaran.

Standar ini mengadopsi model *“Plan-Do-Check-Act” (PDCA)*, yang diterapkan untuk membentuk seluruh proses SMKI. Gambar 1 memperlihatkan persyaratan keamanan informasi dan harapan dari pihak terkait menjadi masukan bagi SMKI, serta melalui tindakan dan proses yang diperlukan akan menghasilkan keluaran keamanan informasi yang memenuhi persyaratan dan harapan tersebut. Gambar 1 juga memperlihatkan korelasi antara proses-proses yang dituangkan dalam klausul 4, 5, 6, 7 dan 8.

Adopsi dari model PDCA juga mencerminkan prinsip-prinsip dalam Panduan OECD (2002)[1)] yang mengatur keamanan sistem informasi dan jaringan. Standar ini memberikan model yang kokoh untuk menerapkan prinsip-prinsip yang ada dalam panduan tersebut yang mengatur asesmen risiko, desain keamanan dan penerapan, manajemen keamanan dan reasesmen.

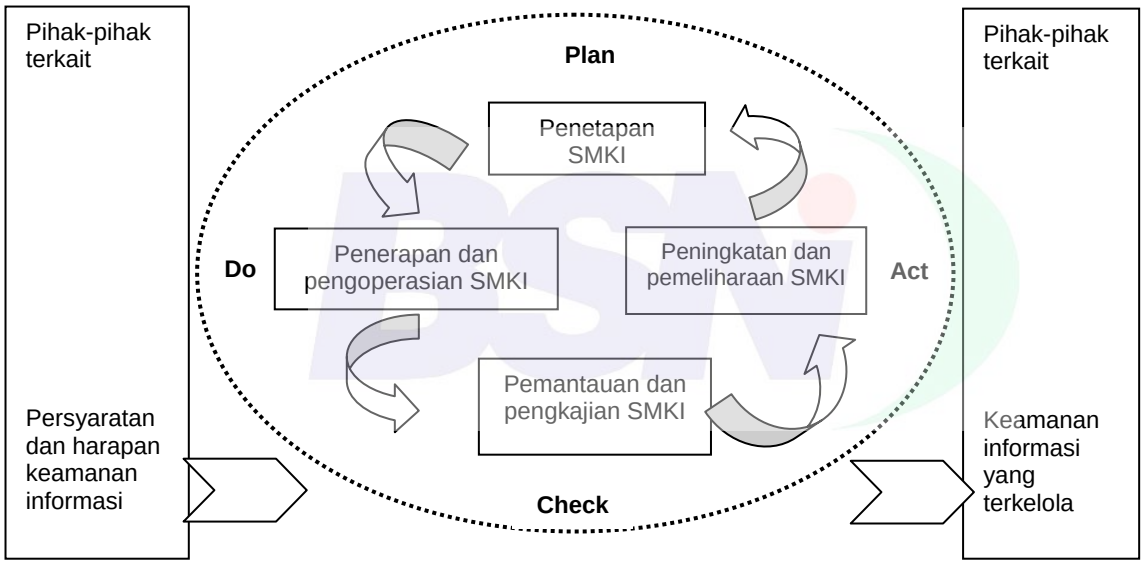
CONTOH 1

Salah satu contoh persyaratan adalah jika terjadi pelanggaran keamanan informasi tidak akan menyebabkan kerugian keuangan yang serius dan/atau menurunkan citra organisasi.

CONTOH 2

Contoh lainnya adalah jika terjadi insiden yang serius – misalnya gangguan (*hacking*) pada website suatu organisasi – sebaiknya ada orang yang cukup terlatih sesuai dengan prosedur untuk meminimalkan dampaknya.

.



Gambar 1 – Model PDCA yang diterapkan untuk proses SMKI

Plan **(penetapan SMKI)**	Menetapkan kebijakan, sasaran, proses dan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
Do **(penerapan dan pengoperasian SMKI)**	Menerapkan dan mengoperasikan kebijakan, pengendalian, proses dan prosedur SMKI.
Check **(pemantauan dan pengkajian SMKI)**	mengases dan, apabila berlaku, mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
Act **(peningkatan dan pemeliharaan SMKI)**	Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal audit SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

[1)] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org*

0.3 Kesesuaian dengan sistem manajemen lainnya

Standar ini diharmonisasikan dengan SNI 19-9001-2001 dan SNI 19-14001-2005 untuk mendukung penerapan dan operasi yang konsisten dan terintegrasi dengan standar manajemen terkait. Apabila satu sistem manajemen yang sesuai telah dibuat maka dapat memenuhi persyaratan dari seluruh standar tersebut. Tabel C.1 memperlihatkan korelasi antara klausul-klausul dari Standar ini, SNI 19-9001-2001, dan SNI 19-14001-2005.

Standar ini dibuat untuk memudahkan organisasi dalam mengharmonisasi atau mengintegrasi SMKI-nya dengan persyaratan sistem manajemen terkait.

Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan

PENTING – Publikasi ini tidak mencakup seluruh ketentuan yang diperlukan dalam suatu kontrak. Pengguna bertanggung jawab atas penerapannya secara benar. Kesesuaian dengan Standar internasional tidak secara otomatis kebal terhadap kewajiban hukum.

1 Ruang lingkup

1.1 Umum

Standar ini mencakup semua jenis organisasi (misalnya usaha komersial, pemerintah, organisasi nir-laba). Standar ini menetapkan persyaratan untuk penetapan, penerapan, pengoperasian, pemantauan, pengkajian, peningkatan dan pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI) yang terdokumentasi dalam konteks risiko bisnis organisasi secara keseluruhan. Standar ini menetapkan persyaratan penerapan pengendalian keamanan yang disesuaikan dengan kebutuhan masing-masing organisasi atau bagian organisasi.

SMKI didesain untuk memastikan pemilihan pengendalian keamanan yang memadai dan proposional untuk melindungi aset informasi dan memberikan kepercayaan kepada pihak terkait.

CATATAN 1 Acuan "bisnis" dalam Standar ini sebaiknya diinterpretasi secara luas yang berarti kegiatan yang merupakan inti dari tujuan keberadaan organisasi.

CATATAN 2 ISO/IEC 17799 memberikan panduan penerapan yang dapat digunakan saat mendesain pengendalian.

1.2 Penerapan

Persyaratan yang ditetapkan dalam Standar ini bersifat generik dan dimaksudkan agar dapat diterapkan untuk seluruh organisasi, tanpa melihat jenis, ukuran dan sifat organisasi. Pengecualian pada setiap persyaratan yang ditetapkan dalam klausul 4, 5, 6, 7 dan 8 tidak dapat diterima bila organisasi menyatakan kesesuaian terhadap Standar ini.

Setiap pengecualian pengendalian yang dianggap perlu untuk memenuhi kriteria risiko yang dapat diterima perlu dijustifikasi dan diperlukan bukti bahwa risiko tersebut telah diterima oleh orang yang bertanggung jawab. Jika pengendalian dikecualikan, pernyataan kesesuaian terhadap Standar ini tidak dapat diterima kecuali jika pengecualian tersebut tidak mempengaruhi kemampuan organisasi, dan/atau tanggung jawabnya, untuk menyediakan keamanan informasi yang memenuhi persyaratan keamanan sebagaimana ditetapkan melalui asesmen risiko dan persyaratan hukum atau perundang-undangan yang berlaku.

CATATAN Jika organisasi telah memiliki sistem manajemen proses bisnis yang telah berjalan (misalnya ISO 9001 atau ISO 14001), dalam berbagai kasus lebih disukai untuk menyesuaikan persyaratan Standar ini ke dalam sistem manajemen yang telah ada.

2 Acuan normatif

Dokumen acuan berikut sangat diperlukan untuk penerapan dokumen ini. Untuk acuan bertanggal, hanya berlaku edisi yang disebutkan. Untuk acuan tidak bertanggal, berlaku edisi terakhir dari dokumen acuan (termasuk setiap amandemen).

ISO/IEC 17799:2005, *Information Technology – Security techniques – Code of practice for information security management*

3 Istilah dan definisi

Untuk maksud dokumen ini, istilah dan definisi berikut digunakan.

3.1
aset
Apapun yang memiliki nilai untuk organisasi
[ISO/IEC 13335-1:2004]

3.2
ketersediaan
sifat/keadaan informasi yang dapat diakses dan digunakan sesuai permintaan lembaga yang berwenang
[ISO/IEC 13335-1:2004]

3.3
kerahasiaan
sifat/keadaan informasi yang tidak disediakan atau dibuka untuk perorangan, lembaga atau proses yang tidak berwenang
[ISO/IEC 13335-1:2004]

3.4
keamanan informasi
penjagaan kerahasiaan, integritas dan ketersediaan informasi; sebagai tambahan, sifat/keadaan informasi lainnya seperti keaslian, akuntabilitas, nirsangkal dan kehandalan dapat juga dimasukkan
[ISO/OEC 17799:2005]

3.5
kejadian keamanan informasi
keterulangan yang diidentifikasi dalam suatu sistem, jasa atau jaringan yang mengindikasikan kemungkinan pelanggaran terhadap kebijakan keamanan informasi atau kegagalan perlindungan, atau situasi yang tidak diketahui sebelumnya yang mungkin terkait dengan keamanan
[ISO/IEC TR 18044:2004]

3.6
insiden keamanan informasi
satu atau serangkaian kejadian keamanan informasi yang tidak diinginkan atau tidak diharapkan yang mempunyai kemungkinan secara signifikan dapat mengganggu operasi bisnis dan mengancam keamanan informasi
[ISO/IEC TR 18044:2004]

3.7
sistem manajemen keamanan informasi (SMKI)
bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi

CATATAN Sistem manajemen mencakup struktur, kebijakan, kegiatan perencanaan, tanggung jawab, praktek, prosedur, proses dan sumber daya organisasi.

3.8
integritas
Sifat/keadaan informasi yang melindungi keakuratan dan kelengkapan aset
[ISO/IEC 13335-1:2004]

3.9
risiko residu
risiko yang tersisa setelah perlakuan risiko
[ISO/IEC Guide 73:2002]

3.10
keberterimaan risiko
keputusan untuk menerima suatu risiko
[ISO/IEC Guide 73:2002]

3.11
analisis risiko
pengunaan informasi secara sistematik untuk mengidentifikasi sumber dan untuk memperkirakan risiko
(ISO/IEC Guide 73:2002)

3.12
asesmen risiko
proses analisis dan evaluasi risiko secara keseluruhan
[ISO/IEC Guide 73:2002]

3.13
evaluasi risiko
proses membandingkan risiko yang diperkirakan terhadap kriteria risiko yang ditetapkan untuk menentukan signifikansi risiko
[ISO/IEC Guide 73:2002]

3.14
manajemen risiko
kegiatan yang dikoordinasikan untuk mengarahkan dan mengendalikan organisasi terkait dengan risiko
[ISO/IEC Guide 73:2002]

3.15
perlakuan risiko
proses pemilihan dan penerapan tindakan untuk memodifikasi risiko
[ISO/IEC Guide 73:2002]

CATATAN Istilah ”pengendalian” dalam standar ini sama dengan ”tindakan”

3.16
pernyataan pemberlakuan
pernyataan terdokumentasi yang menjelaskan sasaran pengendalian dan pengendalian yang relevan dan berlaku untuk SMKI organisasi

CATATAN Sasaran pengendalian dan pengendalian didasarkan pada hasil dan kesimpulan dari proses asesmen risiko dan perlakuan risiko, persyaratan hukum atau perundang-undangan, kontrak dan persyaratan bisnis organisasi untuk keamanan informasi.

4 Sistem manajemen keamanan informasi

4.1 Persyaratan umum

Organisasi harus menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, memelihara dan meningkatkan SMKI terdokumentasi dalam konteks bisnis organisasi secara keseluruhan dan risiko yang dihadapinya. Untuk maksud Standar ini proses yang digunakan didasarkan pada model PDCA yang ditunjukkan dalam Gambar 1.

4.2 Penetapan dan pengelolaan SMKI

4.2.1 Menetapkan SMKI

Organisasi harus melakukan sebagai berikut:

a) Menetapkan ruang lingkup dan batasan SMKI sesuai dengan karakteristik bisnis, organisasi, lokasi, aset dan teknologi, dan termasuk rincian dari setiap pengecualian dan dasar justifikasi untuk setiap pengecualian dari ruang lingkup (lihat 1.2)

b) Menetapkan kebijakan SMKI sesuai dengan karakteristik bisnis, organisasi, lokasinya, asset dan teknologi yang:

   1) Mencakup kerangka kerja untuk menyusun sasaran dan menetapkan arahan dan prinsip tindakan secara menyeluruh berkenaan keamanan informasi;

   2) Mempertimbangkan persyaratan bisnis dan hukum atau regulator, dan kewajiban keamanan sesuai kontrak;

   3) Selaras dengan manajemen risiko strategis organisasi dalam konteks penetapan dan pemeliharaan SMKI yang akan dilaksanakan;

   4) Menetapkan kriteria terhadap risiko yang akan dievaluasi (lihat 4.2.1c)); dan

   5) Telah disetujui oleh manajemen.

   CATATAN Untuk maksud standar ini kebijakan SMKI sebagai suatu kesatuan dalam kebijakan SMKI. Kebijakan ini dapat diuraikan dalam satu dokumen.

c) Menetapkan pendekatan asesmen risiko pada organisasi

   1) Mengidentifikasi suatu metodologi asesmen risiko yang sesuai dengan SMKI, dan keamanan informasi bisnis yang teridentifikasi, dan persyaratan hukum dan perundang-undangan.

   2) Mengembangkan kriteria untuk menerima risiko dan mengidentifikasi tingkat risiko yang dapat diterima (lihat 5.1f)).

   Metodologi asesmen risiko yang dipilih harus memastikan bahwa asesmen risiko memberikan hasil yang dapat dibandingkan dan direproduksi.

CATATAN Terdapat metodologi asesmen risiko yang berbeda. Contoh dari metodologi asesmen risiko adalah sebagaimana didiskusikan dalam ISO/IEC TR 13335-3, *Information Technology – Guidelines for The Management of IT security – Techniques for the management of IT security.*

d) Mengidentifikasi risiko

1) Mengidentifikasi aset dalam ruang lingkup SMKI dan pemilik[2)] aset.

2) Mengidentifikasi ancaman-ancaman terhadap aset

3) Mengidentifikasi kelemahan yang mungkin dieksploitasi oleh ancaman

4) Mengidentifikasi dampak hilangnya kerahasiaan, integritas dan ketersediaan dari aset.

e) Menganalisis dan mengevaluasi risiko.

1) Mengases dampak bisnis bagi organisasi yang mungkin berasal dari kegagalan keamanan, yang mempertimbangkan konsekuensi hilangnya kerahasiaan, integritas atau ketersediaan aset

2) Mengases kemungkinan terjadinya kegagalan keamanan yang realistik, berkenaan dengan ancaman dan kelemahan, dan dampak yang terkait dengan aset serta pengendalian yang diterapkan saat ini.

3) Memperkirakan tingkat risiko.

4) Menetapkan apakah risiko dapat diterima atau memerlukan perlakuan dengan menggunakan kriteria untuk risiko yang dapat diterima sebagaiman ditetapkan dalam 4.2.1c)2).

f) Mengidentifikasi dan mengevaluasi pilihan perlakuan risiko

Tindakan yang mungkin mencakup:

1) penerapan pengendalian yang tepat;

2) penerimaan risiko secara sadar dan objektif, jika risiko tersebut memenuhi kebijakan organisasi dan kriteria risiko yang dapat diterima(lihat 4.2.1c)2));

3) pencegahan risiko; dan

4) pengalihan risiko bisnis terkait kepada pihak lainnya seperti pihak asuransi, pemasok.

g) Memilih sasaran pengendalian dan pengendalian untuk perlakuan risiko.

Sasaran pengendalian dan pengendalian harus dipilih dan diterapkan untuk memenuhi persyaratan yang diidentifikasi melalui proses asesmen risiko dan proses perlakuan risiko. Pemilihan ini harus mempertimbangkan kriteria risiko yang dapat diterima (lihat 4.2.1c)2)) dan juga persyaratan hukum, perundang-undangan dan persyaratan kontrak.

Sasaran pengendalian dan pengendalian dari Lampiran A harus dipilih sebagai bagian dari proses ini sesuai dengan cakupan persyaratan yang diidentifikasi.

Sasaran pengendalian dan pengendalian yang terdaftar dalam Lampiran A tidak lengkap dan sasaran pengendalian dan pengendalian tambahan mungkin dapat dipilih.

[2)] Istilah pemilik mengidentifikasi suatu individu atau lembaga yang telah menyetujui tanggung jawab manajemen untuk mengendalikan produksi, pengembangan, pemeliharaan, penggunaan dan keamanan aset. Istilah pemilik tidak berarti bahwa seseorang secara aktual memiliki hak properti terhadap aset

CATATAN Lampiran A memuat daftar sasaran pengendalian dan pengendalian yang komprehensif, yang secara umum digunakan oleh organisasi. Pengguna Standar ini diarahkan ke Lampiran A sebagai langkah awal untuk pemilihan pengendalian untuk memastikan bahwa tidak ada pilihan pengendalian penting yang terlewatkan.

h) Memperoleh persetujuan manajemen terhadap risiko residu yang diajukan.

i) Memperoleh kewenangan manajemen untuk menerapkan dan mengoperasikan SMKI.

j) Menyiapkan pernyataan pemberlakuan.

Pernyataan pemberlakuan harus disiapkan yang mencakup sebagai berikut:

1) Sasaran pengendalian dan pengendalian yang dipilih dalam 4.2.1g) dan alasan-alasan pemilihannya;

2) Sasaran pengendalian dan pengendalian yang diterapkan saat ini (lihat 4.2.1e)2)); dan

3) Pengecualian setiap sasaran pengendalian dan pengendalian dalam Lampiran A dan dasar justifikasi untuk pengecualiannya.

CATATAN Pernyataan pemberlakuan memberikan ringkasan keputusan yang berkaitan dengan perlakuan risiko. Dasar justifikasi pengecualian menyediakan acuan silang bahwa tidak ada pengendalian yang sengaja diabaikan.

4.2.2 Menerapkan dan mengoperasikan SMKI

Organisasi harus melakukan hal-hal sebagai berikut:

a) Merumuskan rencana perlakuan risiko yang mengidentifikasi tindakan manajemen sumber daya, tanggung jawab dan prioritas secara tepat untuk mengelola risiko keamanan informasi (lihat 5).

b) Menerapkan rencana perlakuan risiko untuk mencapai sasaran pengendalian yang teridentifikasi, yang mencakup pertimbangan pendanaan dan alokasi peran dan tanggung jawab.

c) Menerapkan pengendalian yang dipilih dalam 4.2.1g) untuk memenuhi sasaran pengendalian.

d) Menetapkan bagaimana mengukur keefektifan pengendalian atau kelompok pengendalian yang dipilih dan menerangkan bagaimana pengukuran tersebut digunakan untuk mengakses keefektifan pengendalian untuk memperoleh hasil yang dapat dibandingkan dan direproduksi (lihat 4.2.3c)).

CATATAN Pengukuran keefektifan pengendalian memperbolehkan manajer dan staf untuk menentukan bagaimana pengendalian tersebut berjalan baik dalam mencapai sasaran pengendalian yang direncanakan.

e) Menerapkan program pelatihan dan kepedulian (lihat 5.2.2).

f) Mengelola operasi SMKI

g) Mengelola sumberdaya untuk SMKI (lihat 5.2.2).

h) Menerapkan prosedur dan pengendalian lainnya yang mampu melakukan deteksi secara cepat kejadian keamanan dan menanggapi insiden keamanan (lihat 4.2.3a)).

4.2.3 Memantau dan mengkaji SMKI

Organisasi harus melakukan hal-hal berikut:

a) Melaksanakan prosedur pemantauan, pengkajian dan pengendalian lainnya untuk:

1) Mendeteksi kesalahan hasil pengolahan secara cepat;

2) Mengidentifikasi secara cepat terhadap pelanggaran dan insiden keamanan baik dalam bentuk upaya maupun yang telah berhasil;

3) Memungkinkan manajemen untuk menentukan apakah kegiatan keamanan didelegasikan kepada orang atau diterapkan dengan teknologi informasi yang dilaksanakan sebagaimana diharapkan;

4) Membantu mendeteksi kejadian keamanan sehingga mencegah insiden keamanan dengan menggunakan indikator; dan

5) Menentukan apakah tindakan-tindakan yang diambil untuk memecahkan masalah pelanggaran keamanan telah efektif.

b) Melaksanakan tinjauan keefektifan SMKI secara reguler (termasuk pemenuhan kebijakan dan sasaran SMKI dan mengkaji pengendalian keamanan) dengan mempertimbangkan hasil audit keamanan, insiden, hasil pengukuran keefektifan, pendapat dan umpan balik dari semua pihak terkait.

c) Mengukur keefektifan pengendalian untuk memverifikasi bahwa persyaratan keamanan telah dipenuhi.

d) Mengkaji asesmen risiko pada interval yang direncanakan dan mengkaji risiko residu, dan tingkat risiko yang dapat diterima dan telah diidentifikasi, dengan mempertimbangkan perubahan terhadap:

1) organisasi;

2) teknologi;

3) sasaran dan proses bisnis ;

4) ancaman yang diidentifikasi;

5) keefektifan dari pengendalian yang diterapkan; dan

6) kejadian eksternal seperti perubahan terhadap lingkungan hukum dan regulator, kewajiban kontrak yang berubah dan perubahan lingkungan sosial.

e) Melaksanakan audit internal SMKI pada interval yang direncanakan (lihat 6).

CATATAN Audit internal, kadang-kadang disebut audit pihak pertama, dilaksanakan oleh atau atas nama organisasi itu sendiri untuk tujuan internal.

f) Melaksanakan kajian manajemen SMKI secara reguler untuk memastikan bahwa ruang lingkup masih mencukupi dan peningkatan proses SMKI diidentifikasi (lihat 7.1).

g) Memutakhirkan rencana keamanan dengan mempertimbangkan temuan dari kegiatan pemantauan dan pengkajian .

h) Merekam tindakan dan kejadian yang dapat mempunyai dampak terhadap keefektifan atau kinerja SMKI (lihat 4.3.3).

4.2.4 Meningkatkan dan memelihara SMKI

Organisasi harus melakukan secara reguler hal berikut:

a) Menerapkan peningkatan yang diidentifikasi dalam SMKI

b) Mengambil tindakan korektif dan pencegahan yang tepat sesuai dengan 8.2 dan 8.3. Mengambil pelajaran dari pengalaman keamanan organisasi lain dan dari organisasi itu sendiri.

c) Mengkomunikasikan tindakan dan peningkatan kepada semua pihak yang terkait dengan tingkat rincian sesuai situasi dan kondisi, dan jika relevan, menyetujui tindak lanjutnya.

d) Memastikan bahwa peningkatan tersebut mencapai sasaran yang dimaksudkan.

4.3 Persyaratan dokumentasi

4.3.1 Umum

Dokumentasi harus mencakup rekaman keputusan manajemen, memastikan bahwa tindakan dapat ditelusur terhadap keputusan dan kebijakan manajemen, dan memastikan bahwa hasil yang direkam dapat direproduksi.

Penting untuk mampu menunjukkan hubungan dari pengendalian yang dipilih kembali ke hasil dari asesmen risiko dan proses perlakuan risiko, serta selanjutnya kembali ke kebijakan dan sasaran SMKI.

Dokumentasi SMKI harus mencakup:

a) Pernyataan terdokumentasi tentang kebijakan (lihat 4.2.1b)) dan sasaran SMKI;

b) Ruang lingkup SMKI (lihat 4.2.1a));

c) Prosedur dan pengendalian dalam mendukung SMKI;

d) Deskripsi tentang metodologi asesmen risiko (lihat 4.2.1c));

e) Laporan asesmen risiko (lihat 4.2.1c) sampai 4.2.1g));

f) Rencana perlakuan risiko (lihat 4.2.2b));

g) Prosedur terdokumentasi yang dibutuhkan oleh organisasi untuk memastikan perencanaan, pelaksanaan dan pengendalian yang efektif dari proses keamanan informasinya dan menguraikan bagaimana mengukur keefektifan pengendalian (lihat 4.2.3c));

h) Rekaman yang dipersyaratkan oleh Standar ini (lihat 4.3.3); dan

i) Pernyataan Pemberlakuan.

CATATAN 1 Apabila istilah “prosedur terdokumentasi” muncul dalam Standar ini, hal ini berarti bahwa prosedur tersebut dibuat, didokumentasikan, diterapkan dan dipelihara.

CATATAN 2 Cakupan dari dokumentasi SMKI dapat berbeda satu organisasi dengan yang lainnya tergantung pada:
- ukuran organisasi dan jenis kegiatannya; dan
- ruang lingkup dan kompleksitas persyaratan keamanan dan sistem yang dikelola

CATATAN 3 Dokumen dan rekaman dapat berupa dalam bentuk atau media apapun.

4.3.2 Pengendalian dokumen

Dokumen yang dipersyaratkan oleh SMKI harus dilindungi dan dikendalikan. Prosedur terdokumentasi harus ditetapkan untuk mendefinisikan tindakan manajemen yang dibutuhkan untuk:

a) Menyetujui kecukupan dokumen sebelum diterbitkan;

b) Mengkaji dan memutakhirkan dokumen jika diperlukan dan menyetujui kembali dokumen;

c) Memastikan bahwa perubahan dan status revisi terkini dari dokumen diidentifikasi;

d) Memastikan bahwa versi yang relevan dari dokumen yang berlaku tersedia di tempat penggunaan;

e) Memastikan bahwa dokumen dapat dibaca dengan mudah dan mudah diidentifikasi;

f) Memastikan bahwa dokumen tersedia untuk orang yang membutuhkannya, serta ditransfer, disimpan dan akhirnya dimusnahkan sesuai dengan prosedur yang berlaku sesuai dengan klasifikasinya;

g) Memastikan bahwa dokumen yang berasal dari luar diidentifikasi;

h) Memastikan bahwa distribusi dokumen dikendalikan;

i) Mencegah penggunaan yang tidak diinginkan terhadap dokumen yang kadaluarsa; dan

j) Menerapkan identifikasi yang sesuai untuk dokumen yang disimpan untuk berbagai tujuan.

4.3.3 Pengendalian rekaman

Rekaman harus ditetapkan dan dipelihara untuk menyediakan bukti kesesuaian terhadap persyaratan dan operasi SMKI yang efektif. Rekaman harus dilindungi dan dikendalikan. SMKI harus mempertimbangkan setiap persyaratan hukum atau peraturan perundang-undangan yang relevan dan kewajiban kontrak. Rekaman harus mudah dibaca, mudah diidentifikasi dan mudah diambil. Pengendalian yang dibutuhkan untuk identifikasi, penyimpanan, perlindungan, pengambilan kembali, waktu penyimpanan dan pemusnahan rekaman, harus didokumentasikan dan diterapkan.

Rekaman yang berisi kinerja proses sebagaimana dijelaskan dalam 4.2 dan seluruh kejadian dari insiden keamanan yang signifikan terkait dengan SMKI harus dipelihara.

CONTOH

Contoh rekaman adalah buku tamu, laporan audit dan formulir otorisasi akses yang telah diisi lengkap.

5 Tanggung jawab manajemen

5.1 Komitmen manajemen

Manajemen harus menyediakan bukti komitmennya terhadap penetapan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharaan dan peningkatan SMKI dengan:

a) Menetapkan kebijakan SMKI;

b) Memastikan sasaran dan rencana SMKI telah ditetapkan;

c) Menetapkan peran dan tanggung jawab untuk keamanan informasi;

d) Mengkomunikasikan kepada organisasi tentang pentingnya memenuhi sasaran keamanan informasi dan kesesuaian terhadap kebijakan keamanan informasi, tanggung jawabnya berdasarkan hukum dan kebutuhan untuk peningkatan berkelanjutan;

e) Menyediakan sumberdaya yang cukup untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI (lihat 5.2.1);

f) Memutuskan kriteria risiko yang dapat diterima dan tingkat keberterimaan risiko;

g) Memastikan bahwa audit internal SMKI dilaksanakan (lihat 6); dan

h) Melaksanakan kajian manajemen SMKI (lihat 7).

5.2 Manajemen sumberdaya

5.2.1 Ketentuan sumberdaya

Organisasi harus menetapkan dan menyediakan sumberdaya yang dibutuhkan untuk:

a) Menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara SMKI;

b) Memastikan bahwa prosedur keamanan informasi mendukung persyaratan bisnis;

c) Mengidentifikasi dan memenuhi persyaratan hukum dan perundang-undangan serta kewajiban keamanan kontrak;

d) Memelihara keamanan secara memadai dengan penerapan yang tepat dari semua pengendalian yang diterapkan;

e) Melaksanakan kajian jika diperlukan, dan menindaklanjuti hasil kajian secara tepat; dan

f) Apabila dipersyaratkan, meningkatkan keefektifan SMKI.

5.2.2 Pelatihan, kepedulian dan kompetensi

Organisasi harus memastikan bahwa semua personel yang diberikan tanggung jawab yang ditetapkan dalam SMKI kompeten untuk melaksanakan tugas yang dipersyaratkan dengan:

a) Menetapkan kompetensi yang perlu untuk personel yang melaksanakan pekerjaan yang mempengaruhi SMKI;

b) Menyediakan pelatihan atau mengambil tindakan lainnya (misalnya mempekerjakan personel yang kompeten) untuk memenuhi kebutuhan tersebut;

c) Mengevaluasi keefektifan tindakan yang diambil; dan

d) Memelihara rekaman pendidikan, pelatihan, ketrampilan, pengalaman dan kualifikasi (lihat 4.3.3).

Organisasi juga harus memastikan bahwa semua personel terkait peduli akan relevansi dan pentingnya kegiatan keamanan informasinya dan bagaimana mereka memberikan kontribusi terhadap pencapaian sasaran SMKI.

6 Audit internal SMKI

Organisasi harus melaksanakan audit internal SMKI pada interval yang terencana untuk menetapkan apakah sasaran pengendalian, pengendalian, proses dan prosedur SMKI tersebut:

a) Sesuai dengan persyaratan Standar ini dan persyaratan hukum atau peraturan perundang-undangan yang relevan;

b) Sesuai dengan persyaratan keamanan informasi yang diidentifikasi;

c) Dilaksanakan dan dipelihara secara efektif; dan

d) Dilaksanakan sesuai yang diharapkan.

Program audit harus direncanakan, mempertimbangkan status dan pentingnya proses dan area yang akan diaudit, serta hasil dari audit sebelumnya. Kriteria, ruang lingkup, frekuensi dan metode audit harus ditetapkan. Pemilihan auditor dan pelaksanaan audit harus memastikan objektifitas dan ketidakberpihakan proses audit. Auditor tidak boleh mengaudit pekerjaannya sendiri.

Tanggung jawab dan persyaratan untuk perencanaan dan pelaksanaan audit serta pelaporan dan pemeliharaan rekaman (lihat 4.3.3) harus ditetapkan dalam prosedur terdokumentasi.

Tanggung jawab manajemen terhadap bidang yang diaudit harus memastikan bahwa tindakan yang diambil tidak boleh ditunda untuk menghilangkan ketidaksesuaian yang terdeteksi dan penyebabnya. Kegiatan tindak lanjut harus mencakup verifikasi dari tindakan yang diambil dan laporan hasil verifikasi (lihat 8).

CATATAN SNI 19-19011-2005, Panduan untuk audit sistem manajemen mutu dan/atau lingkungan, mungkin dapat memberikan panduan untuk melaksanakan audit internal SMKI.

7 Kajian manajemen SMKI

7.1 Umum

Manajemen harus mengkaji SMKI organisasi pada interval yang terencana (minimal setahun sekali) untuk memastikan kesesuaian, kecukupan dan keefektifannya secara berkesinambungan. Kajian ini harus mencakup asesmen peluang peningkatan dan kebutuhan terhadap perubahan SMKI, termasuk kebijakan keamanan informasi dan sasaran keamanan informasi. Hasil dari kajian ini harus didokumentasikan dengan jelas dan rekaman harus dipelihara (lihat 4.3.3).

7.2 Masukan kajian

Masukan untuk kajian manajemen harus mencakup:

a) Hasil audit dan kajian SMKI;

b) Umpan balik dari pihak yang berkepentingan;

c) Teknik, produk atau prosedur, yang dapat digunakan dalam organisasi untuk meningkatkan kinerja dan keefektifan SMKI;

d) Status tindakan korektif dan tindakan pencegahan;

e) Kelemahan atau ancaman yang tidak ditangani secara memadai dalam asesmen risiko sebelumnya;

f) Hasil dari pengukuran keefektifan;

g) Tindak lanjut dari kajian manajemen sebelumnya;

h) Setiap perubahan yang dapat mempengaruhi SMKI; dan

i) Rekomendasi untuk peningkatan.

7.3 Keluaran Kajian

Keluaran dari kajian manajemen harus mencakup setiap keputusan dan tindakan yang terkait hal-hal berikut:

a) Peningkatan keefektifan SMKI.

b) Pemutakhiran asesmen risiko dan rencana perlakuan risiko.

c) Modifikasi prosedur dan pengendalian yang mempengaruhi keamanan informasi, jika perlu, untuk menanggapi kejadian internal dan eksternal yang dapat berdampak pada SMKI, termasuk perubahan terhadap:

   1) persyaratan bisnis;

   2) persyaratan keamanan;

   3) proses bisnis yang mempengaruhi persyaratan bisnis yang ada;

   4) persyaratan peraturan perundang-undangan atau hukum;

   5) kewajiban kontrak; dan

   6) tingkat risiko dan/atau kriteria risiko yang dapat diterima.

d) Kebutuhan sumberdaya.

e) Peningkatan atas keefektifan pengukuran pengendalian .

8 Peningkatan SMKI

8.1 Peningkatan berkelanjutan

Organisasi harus meningkatkan keefektifan SMKI secara berkelanjutan melalui kebijakan keamanan informasi, sasaran keamanan informasi, hasil audit, analisis kejadian yang dipantau, tindakan korektif dan pencegahan, dan kajian manajemen (lihat 7).

8.2 Tindakan korektif

Organisasi harus mengambil tindakan untuk menghilangkan penyebab ketidaksesuaian dengan persyaratan SMKI untuk mencegah terulangnya kembali ketidaksesuaian tersebut. Prosedur terdokumentasi untuk tindakan korektif harus menetapkan persyaratan untuk:

   a) Mengidentifikasi ketidaksesuaian;

   b) Menetapkan penyebab ketidaksesuaian;

   c) Mengevaluasi kebutuhan tindakan untuk memastikan bahwa ketidaksesuaian tidak terulang;

   d) Menetapkan dan menerapkan tindakan korektif yang diperlukan;

   e) Merekam hasil tindakan yang diambil (lihat 4.3.3); dan

   f) Mengkaji tindakan korektif yang diambil.

8.3 Tindakan pencegahan

Organisasi harus menetapkan tindakan untuk menghilangkan penyebab ketidaksesuaian yang potensial dengan persyaratan SMKI untuk mencegah ketidaksesuaian tersebut terulang. Tindakan pencegahan yang diambil harus sesuai dengan dampak masalah yang potensial. Prosedur terdokumentasi untuk tindakan pencegahan harus menetapkan persyaratan untuk:

a) Mengidentifikasi ketidaksesuaian potensial dan penyebabnya;

b) Mengevaluasi kebutuhan tindakan untuk mencegah terulangnya ketidaksesuaian;

c) Menetapkan dan menerapkan tindakan pencegahan yang diperlukan;

d) Merekam hasil tindakan yang diambil (lihat 4.3.3); dan

e) Mengkaji tindakan pencegahan yang diambil.

Organisasi harus mengidentifikasi risiko yang berubah dan mengidentifikasi persyaratan tindakan pencegahan yang memfokuskan pada risiko yang berubah secara signifikan.

Prioritas tindakan pencegahan harus ditetapkan berdasarkan hasil asesmen risiko.

CATATAN Tindakan untuk mencegah ketidaksesuaian seringkali lebih efektif dari segi biaya dibandingkan dengan tindakan korektif .

Lampiran A
(normatif)

Sasaran pengendalian dan pengendalian

Sasaran pengendalian dan pengendalian yang terdaftar dalam Tabel A.1 djabarkan dan diselaraskan dengan ISO/IEC 17799:2005 Klausul 5 sampai Klausul 15. Daftar dalam Tabel A.1 tidak mencakup semua sasaran pengendalian dan pengendalian dan organisasi dapat mempertimbangkan untuk menambahkannya. Sasaran pengendalian dan pengendalian dalam tabel tersebut disesuaikan dengan proses SMKI seperti yang ditetapkan dalam 4.2.1.

ISO/IEC 17799:2005 Klausul 5 sampai Klausul 15 memberikan saran penerapan dan panduan tentang praktek terbaik dalam mendukung pengendalian sebagaimana ditetapkan dalam A.5 sampai A. 15.

Table A.1 – Sasaran pengendalian dan pengendalian

A.5 Kebijakan keamanan		
A.5.1. Kebijakan keamanan informasi *Sasaran:* untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi menurut persyaratan bisnis dan hukum dan regulasi yang relevan		
A.5.1.1.	Dokumen kebijakan keamanan informasi	*Pengendalian* Dokumen kebijakan keamanan informasi harus disetujui oleh manajemen, dan dipublikasikan serta dikomunikasikan kepada semua pekerja dan pihak-pihak luar terkait.
A. 5.1.2	Kajian kebijakan keamanan informasi	*Pengendalian* Kebijakan keamanan informasi harus dikaji pada interval yang terencana atau jika terjadi perubahan signifikan untuk memastikan kesesuaian, kecukupan dan keefektifan yang berkelanjutan .
A.6. Organisasi keamanan informasi		
A.6.1 Organisasi internal Sasaran:untuk mengelola keamanan informasi dalam organisasi		
A.6.1.1	Komitmen manajemen terhadap keamanan informasi	*Pengendalian* Manajemen harus mendukung secara aktif keamanan dalam organisasi dengan arahan yang jelas, komitmen nyata, penugasan eksplisit dan bertanggung jawab atas keamanan informasi

A.6.1.2	Koordinasi keamanan informasi	*Pengendalian* Kegiatan keamanan informasi harus dikoordinasikan oleh wakil-wakil dari bagian organisasi yang sesuai dengan peran dan fungsi kerjanya masing-masing.
A.6.1.3	Alokasi tanggung jawab keamanan informasi	*Pengendalian* Seluruh tanggung jawab keamanan informasi harus ditetapkan dengan jelas
A.6.1.4	Proses otorisasi untuk fasilitas pengolahan informasi	*Pengendalian* Proses otorisasi manajemen untuk fasilitas pengolahan informasi terkini harus ditetapkan dan dilaksanakan.
A.6.1.5	Perjanjian kerahasiaan	*Pengendalian* Persyaratan perjanjian kerahasiaan atau *non-disclosure* yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi dan dikaji secara regular.
A.6.1.6	Kontak dengan pihak berwenang	*Pengendalian* Kontak dengan pihak berwenang yang relevan harus dipelihara
A.6.1.7	Kontak dengan kelompok khusus (*special interest*)	*Pengendalian* Kontak dengan kelompok khusus (*special interest*)atau forum ahli keamanan dan asosiasi profesi harus dipelihara.
A.6.1.8	Kajian independen terhadap keamanan informasi	*Pengendalian* Pendekatan organisasi untuk mengelola keamanan informasi dan penerapannya (yaitu sasaran pengendalian, pengendalian, kebijakan, proses, dan prosedur untuk keamanan informasi) harus dikaji secara independen pada interval terencana, atau ketika terjadi perubahan signifikan terhadap penerapan keamanan.
A.6.2 Pihak eksternal Sasaran: untuk memelihara keamanan informasi organisasi dan fasilitas pengolahan informasi yang diakses, diolah, dikomunikasikan kepada atau dikelola oleh pihak eksternal.		
A.6.2.1	Identifikasi risiko terkait pihak	Pengendalian

	ekternal	Risiko terhadap informasi organisasi dan fasilitas pengolahan informasi dari proses bisnis yang melibatkan pihak-pihak eksternal harus diidentifikasi dan pengendalian yang sesuai dilaksanakan sebelum pemberian akses.
A.6.2.2	Penekanan keamanan ketika berhubungan dengan pelanggan	Pengendalian Seluruh persyaratan keamanan yang diidentifikasi harus ditekankan sebelum memberikan akses kepada pelanggan terhadap informasi atau aset organisasi.
A.6.2.3	Penekanan keamanan perjanjian dengan pihak ketiga	*Pengendalian* Perjanjian dengan pihak ketiga yang meliputi pengaksesan, pengolahan, pengkomunikasian atau pengelolaan informasi organisasi atau fasilitas pengolahan informasi, atau penambahan produk atau jasa ke dalam fasilitas pengolahan informasi harus mencakup seluruh persyaratan keamanan yang relevan.
A.7 Pengelolaan aset		
A.7.1 Tanggung jawab terhadap aset Sasaran: untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi.		
A.7.1.1	Inventaris aset	*Pengendalian* Semua aset harus diidentifikasi dengan jelas dan inventaris dari semua aset penting dicatat dan dipelihara.
A.7.1.2	Kepemilikan aset	*Pengendalian* Semua informasi dan aset yang terkait dengan fasilitas pengolahan informasi harus "dimiliki"[3)] oleh bagian dari organisasi yang ditunjuk.
A.7.1.3	Penggunaan aset yang dapat diterima	*Pengendalian* Aturan untuk penggunaan informasi dan aset yang dapat diterima terkait dengan fasilitas pengolahan informasi harus diidentifikasi, didokumentasikan dan diterapkan.

[3)] Penjelasan : Istilah pemilik mengidentifikasi suatu individu atau lembaga yang telah menyetujui tanggung jawab manajemen untuk mengendalikan produksi, pengembangan, pemeliharaan, penggunaan dan keamanan aset. Istilah pemilik tidak berarti bahwa seseorang secara aktual memiliki hak kepemilikan terhadap aset.

A.7.2 Klasifikasi informasi Sasaran: untuk memastikan bahwa informasi menerima tingkat perlindungan yang tepat		
A.7.2.1	Pedoman klasifikasi	*Pengendalian* Informasi harus diklasifikasikan sesuai dengan nilai, persyaratan hukum, sensitivitas dan tingkat kritisnya terhadap organisasi
A.7.2.2	Pelabelan dan penanganan informasi	*Pengendalian* Sekumpulan prosedur yang memadai untuk pelabelan dan penanganan informasi harus dikembangkan dan diterapkan menurut skema klasifikasi yang diadopsi oleh organisasi.
A.8 Keamanan sumberdaya manusia		
A.8.1 Sebelum dipekerjakan[4)] Sasaran: untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga memahami tanggung jawab sesuai dengan perannya, dan untuk mengurangi risiko pencurian, kecurangan atau penyalahgunaan fasilitas.		
A.8.1.1	Peran dan tanggung jawab	*Pengendalian* Peran dan tanggung jawab dari pegawai, kontraktor dan pengguna pihak ketiga terhadap keamanan harus ditetapkan dan didokumentasikan sesuai dengan kebijakan keamanan informasi organisasi.
A.8.1.2	Penyaringan (*Screening*)	*Pengendalian* Verifikasi latar belakang terhadap semua calon pegawai, kontraktor, dan pengguna pihak ketiga harus dilaksanakan menurut hukum dan undang-undang serta etika yang berlaku dan proporsional terhadap persyaratan bisnis, klasifikasi informasi yang diakses dan risiko yang dipersepsikan.
A.8.1.3	Syarat dan aturan kepegawaian	*Pengendalian* Sebagai bagian dari kewajiban kontrak, pegawai, kontraktor dan pengguna pihak ketiga harus menyetujui dan menandatangani syarat dan aturan kontrak kepegawaian yang harus menyatakan tanggung jawab mereka dan organisasi terhadap keamanan informasi.

[4)] Penjelasan : Kata “Dipekerjakan” disini berarti mencakup semua situasi yang berbeda yaitu : mempekerjakan orang (sementara atau permanen), penunjukan peran pekerjaan, perubahan peran pekerjaan, penugasan kontrak dan pengakhiran dari semua pengaturan ini.

A.8.2 Selama bekerja Sasaran: untuk memastikan bahwa semua pegawai, kontraktor dan pengguna pihak ketiga telah peduli terhadap ancaman dan masalah keamanan informasi, tanggung jawab dan pertanggung-gugatan mereka, dan disediakan perlengkapan yang memadai untuk mendukung kebijakan keamanan organisasi selama bekerja dan untuk mengurangi risiko kesalahan manusia.		
A.8.2.1	Tanggung jawab manajemen	*Pengendalian* Manajemen harus mensyaratkan pegawai, kontraktor dan pengguna pihak ketiga untuk menerapkan keamanan menurut kebijakan dan prosedur organisasi yang ditetapkan.
A.8.2.2	Kepedulian, pendidikan dan pelatihan keamanan informasi	*Pengendalian* Semua pegawai organisasi dan, jika relevan, kontraktor dan pengguna pihak ketiga harus menerima pelatihan kepedulian dan kebijakan serta prosedur organisasi yang mutakhir secara regular sesuai dengan fungsi kerjanya.
A.8.2.3	Proses pendisiplinan	*Pengendalian* Harus ada proses pendisiplinan yang resmi untuk pegawai yang melakukan pelanggaran keamanan.
A.8.3 Pengakhiran atau perubahan pekerjaan Sasaran: untuk memastikan bahwa pegawai, kontraktor dan pengguna pihak ketiga keluar dari organisasi atau adanya perubahan pekerjaan dengan cara yang sesuai.		
A.8.3.1	Tanggung jawab pengakhiran pekerjaan	*Pengendalian* Tanggung jawab untuk melaksanakan pengakhiran pekerjaan atau perubahan pekerjaan harus ditetapkan dan diberikan dengan jelas.
A.8.3.2	Pengembalian aset	*Pengendalian* Semua pegawai, kontraktor dan pengguna pihak ketiga harus mengembalikan semua aset organisasi yang digunakannya ketika pekerjaan, kontrak atau perjanjian.berakhir.
A.8.3.3	Penghapusan hak akses	*Pengendalian* Hak akses semua pegawai, kontraktor dan pengguna pihak ketiga terhadap informasi dan fasilitas pengolahan informasi harus dihapuskan ketika pekerjaan, kontrak atau perjanjian .berakhir ., atau disesuaikan dengan

		perubahan.
A.9 Keamanan fisik dan lingkungan		
A.9.1 Area yang aman Sasaran: untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interferensi terhadap lokasi dan informasi organisasi.		
A.9.1.1	Perimeter keamanan fisik	*Pengendalian* Perimeter keamanan (batasan seperti dinding, pintu masuk yang dikendalikan dengan kartu atau meja resepsionis yang dijaga) harus digunakan untuk melindungi area yang berisi informasi dan fasilitas pengolahan informasi.
A.9.1.2	Pengendalian entri yang bersifat fisik	*Pengendalian* Area yang aman harus dilindungi dengan pengendalian entri yang sesuai untuk memastikan bahwa hanya personel yang berwenang diperbolehkan untuk mengakses.
A.9.1.3	Mengamankan kantor, ruangan dan fasilitas	*Pengendalian* Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.
A.9.1.4	Perlindungan terhadap ancaman eksternal dan lingkungan	*Pengendalian* Perlindungan fisik terhadap kerusakan akibat dari kebakaran, banjir, gempa bumi, ledakan, kerusuhan dan bentuk lain bencana alam atau buatan manusia harus dirancang dan diterapkan.
A.9.1.5	Bekerja di area yang aman	*Pengendalian* Perlindungan fisik dan pedoman kerja dalam area yang aman harus dirancang dan diterapkan
A.9.1.6	Area akses publik, dan bongkar muat	*Pengendalian* Titik akses seperti area bongkar muat dan titik lainnya dimana orang yang tidak berwenang dapat masuk kedalam lokasi harus dikendalikan dan, jika mungkin, dipisahkan dari fasilitas pengolahan informasi untuk mencegah akses yang tidak berwenang.
A.9.2 Keamanan peralatan Sasaran: untuk mencegah kehilangan, kerusakan, pencurian atau gangguan aset dan interupsi terhadap kegiatan organisasi		

A.9.2.1	Penempatan dan perlindungan peralatan	*Pengendalian* Peralatan harus ditempatkan atau dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan dan peluang untuk akses oleh pihak yang tidak berwenang.
A.9.2.2	Sarana pendukung	*Pengendalian* Peralatan harus dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan oleh kegagalan sarana pendukung.
A.9.2.3	Keamanan kabel	*Pengendalian* Kabel daya dan telekomunikasi yang membawa data atau jasa informasi pendukung harus dilindungi dari intersepsi atau kerusakan.
A.9.2.4	Pemeliharaan peralatan	*Pengendalian* Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya.
A.9.2.5	Keamanan peralatan di luar lokasi	*Pengendalian* Keamanan harus diterapkan pada peralatan di luar lokasi dengan mempertimbangkan risiko yang berbeda pada saat bekerja di luar lokasi organisasi.
A.9.2.6	Pembuangan atau penggunaan kembali peralatan secara aman	*Pengendalian* Seluruh *item* atau peralatan yang memuat media penyimpanan harus diperiksa untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa (overwritten) secara aman sebelum dibuang.
A.9.2.7	Pemindahan barang	*Pengendalian* Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa ijin yang berwenang.
A.10 Manajemen komunikasi dan operasi		
A.10.1 Prosedur operasional dan tanggung jawab Sasaran: untuk memastikan pengoperasian fasilitas pengolahan informasi secara benar dan aman		
A.10.1.1	Prosedur operasi terdokumentasi	*Pengendalian* Prosedur pengoperasian harus

		didokumentasikan, dipelihara dan tersedia untuk semua pengguna yang memerlukannya.
A.10.1.2.	Manajemen perubahan	*Pengendalian* Perubahan terhadap fasilitas dan sistem pengolahan informasi harus dikendalikan.
A.10.1.3	Pemisahan tugas	*Pengendalian* Tugas dan lingkup tanggung jawab harus dipisahkan untuk mengurangi peluang bagi modifikasi yang tidak sengaja atau tidak sah atau penyalahgunaan terhadap aset organisasi.
A.10.1.4	Pemisahan fasilitas pengembangan, pengujian dan operasional	*Pengendalian* Fasilitas pengembangan, pengujian dan operasional harus dipisahkan untuk mengurangi risiko akses atau perubahan yang tidak sah terhadap sistem operasional.
A.10.2 Manajemen pelayanan jasa pihak ketiga Sasaran: untuk menerapkan dan memelihara tingkat keamanan informasi dan pelayanan jasa yang sesuai dengan perjanjian pelayanan jasa pihak ketiga.		
A.10.2.1	Pelayanan jasa	*Pengendalian* Harus dipastikan bahwa pengendalian keamanan, definisi jasa dan tingkat layanan yang dicakup dalam perjanjian pelayanan jasa pihak ketiga diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga.
A.10.2.2	Pemantauan dan pengkajian jasa pihak ketiga	*Pengendalian* Jasa, laporan dan rekaman yang diberikan oleh pihak ketiga harus dipantau, dikaji dan diaudit secara regular
A.10.2.3	Pengelolaan perubahan terhadap jasa pihak ketiga	*Pengendalian* Perubahan terhadap ketentuan jasa, termasuk pemeliharaan dan peningkatan kebijakan , prosedur dan pengendalian keamanan informasi yang ada, harus dikelola dengan mempertimbangkan tingkat kritikal sistem dan proses bisnis terkait dan asesmen ulang dari risiko.
A.10.3 Perencanaan dan keberterimaan sistem Sasaran: untuk mengurangi risiko kegagalan sistem		

A.10.3.1	Manajemen kapasitas	*Pengendalian* Penggunaan sumberdaya harus dipantau, disesuaikan dan diproyeksikan untuk pemenuhan kapasitas mendatang, guna memastikan kinerja sistem yang dipersyaratkan.
A.10.3.2	Keberterimaan sistem	*Pengendalian* Kriteria keberterimaan sistem informasi yang baru, *upgrade*, dan versi baru harus ditetapkan dan dilakukan pengujian sistem yang sesuai selama pengembangan dan sebelum diterima.
A.10.4 Perlindungan terhadap *malicious and mobile code* Sasaran: untuk melindungi integritas perangkat lunak dan informasi		
A.10.4.1	Pengendalian terhadap *malicious code*	*Pengendalian* Pengendalian yang bersifat pendeteksian, pencegahan dan pemulihan untuk melindungi dari *malicious code,* dan prosedur kepedulian pengguna yang memadai harus diterapkan.
A.10.4.2	Pengendalian terhadap ***mobile code***	*Pengendalian* Apabila penggunaan ***mobile code*** diijinkan, konfigurasi tersebut harus memastikan bahwa ***mobile code*** yang sah beroperasi sesuai dengan kebijakan keamanan yang ditetapkan secara jelas, dan penggunaan ***mobile code*** yang tidak sah harus dicegah.
A.10.5 *Back-up* Sasaran: untuk memelihara integritas dan ketersediaan informasi dan fasilitas pengolahan informasi.		
A.10.5.1	*Back-up* informasi	*Pengendalian* Salinan *back-up* informasi dan perangkat lunak harus diambil dan diuji secara regular sesuai dengan kebijakan *back-up* yang disetujui.
A.10.6 Manajemen keamanan jaringan Sasaran: untuk memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung.		
A.10.6.1	Pengendalian jaringan	*Pengendalian* Jaringan harus dikelola dan dikendalikan secara memadai, agar terlindung dari ancaman, dan untuk memelihara keamanan dari sistem

		dan aplikasi yang menggunakan jaringan, termasuk informasi dalam transit.
A.10.6.2	Keamanan layanan jaringan	*Pengendalian* Fitur keamanan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dicakup dalam setiap perjanjian layanan jaringan, baik diberikan secara *in-house* atau dialihdayakan.
A.10.7 Penanganan media Sasaran: untuk mencegah pengungkapan, modifikasi, pemindahan atau pemusnahan aset yang tidak sah, dan gangguan kegiatan bisnis.		
A.10.7.1	Manajemen media yang dapat dipindahkan	*Pengendalian* Harus tersedia prosedur untuk manajemen media yang dapat dipindahkan.
A.10.7.2	Pemusnahan media	*Pengendalian* Media harus dimusnahkan secara aman dan terjamin apabila tidak lagi diperlukan dengan menggunakan prosedur formal.
A.10.7.3	Prosedur penanganan informasi	*Pengendalian* Prosedur untuk penanganan dan penyimpanan informasi harus ditetapkan untuk melindungi informasi dari pengungkapan yang tidak sah atau penyalahgunaan.
A.10.7.4	Keamanan dokumentasi sistem	*Pengendalian* Dokumentasi sistem harus dilindungi terhadap akses yang tidak sah.
A.10.8 Pertukaran informasi Sasaran: untuk memelihara keamanan informasi dan perangkat lunak yang dipertukarkan dalam suatu organisasi dan dengan setiap entitas eksternal.		
A.10.8.1	Kebijakan dan prosedur pertukaran informasi	*Pengendalian* Kebijakan prosedur dan pengendalian secara formal harus tersedia untuk melindungi pertukaran informasi dengan menggunakan semua jenis fasilitas komunikasi.
A.10.8.2	Perjanjian pertukaran	*Pengendalian* Perjanjian harus ditetapkan untuk pertukaran informasi dan perangkat

		lunak antara organisasi dan pihak eksternal.
A.10.8.3	Media fisik dalam transit	*Pengendalian* Media yang memuat informasi harus dilindungi terhadap akses yang tidak sah, penyalahgunaan atau kerusakan selama transportasi diluar batas fisik organisasi.
A.10.8.4	Pesan elektronik	*Pengendalian* Informasi dalam bentuk pesan elektronik harus dilindungi dengan tepat.
A.10.8.5	Sistem informasi bisnis	*Pengendalian* Kebijakan dan prosedur harus dikembangkan dan diterapkan untuk melindungi informasi yang berkaitan dengan interkoneksi sistem informasi bisnis.
A.10.9 Layanan *electronic commerce* Sasaran: untuk memastikan keamanan layanan *electronic commerce* dan keamanan penggunaannya.		
A.10.9.1	*Electronic commerce*	*Pengendalian* Informasi yang termasuk dalam layanan *electronic commerce* yang melalui jaringan publik harus dilindungi dari tindak kecurangan, perselisihan kontrak dan pengungkapan serta modifikasi yang tidak sah.
A.10.9.2	Transaksi *on-line*	*Pengendalian* Informasi yang termasuk dalam transaksi *on-line* harus dilindungi untuk mencegah transmisi yang tidak lengkap, salah jalur, perubahan pesan, pengungkapan, duplikasi atau pengulangan proses yang tidak sah.
A.10.9.3	Informasi yang tersedia untuk umum	*Pengendalian* Integritas informasi yang tersedia pada sistem yang digunakan untuk umum harus dilindungi untuk mencegah modifikasi yang tidak sah.
A.10.10 Pemantauan Sasaran: untuk mendeteksi kegiatan pengolahan informasi yang tidak sah.		
A.10.10.1	*Log* audit	*Pengendalian* *Log* audit yang merekam kegiatan

		pengguna, pengecualian dan kejadian keamanan informasi harus dihasilkan dan dijaga pada periode yang disetujui untuk membantu investigasi di masa yang akan datang dan pemantauan pengendalian akses.
A.10.10.2	Pemantauan penggunaan sistem	*Pengendalian* Prosedur untuk pemantauan penggunaan fasilitas pengolahan informasi harus ditetapkan dan hasil kegiatan pemantauan ditinjau secara regular.
A.10.10.3	Perlindungan informasi *log*	*Pengendalian* Fasilitas *log* dan informasi *log* harus dilindungi terhadap gangguan dan akses tidak sah.
A.10.10.4	*Log* administrator dan operator	*Pengendalian* Kegiatan administrator sistem dan operator sistem harus dicatat dalam *log*.
A.10.10.5	*Log* atas kesalahan yang terjadi (Fault logging)	*Pengendalian* Kesalahan harus dicatat dalam log, dianalisis dan diambil tindakan yang sesuai.
A.10.10.6	Sinkronisasi penunjuk waktu	*Pengendalian* Penunjuk waktu dari seluruh sistem pengolahan informasi relevan dalam organisasi atau *domain* keamanan harus disinkronisasikan dengan sumber penunjuk waktu akurat yang disepakati.
A.11 Pengendalian akses		
A.11.1 Persyaratan bisnis untuk pengendalian akses Sasaran: untuk mengendalikan akses kepada informasi		
A.11.1.1	Kebijakan pengendalian akses	*Pengendalian* Kebijakan pengendalian akses harus ditetapkan, didokumentasikan dan dikaji berdasarkan persyaratan bisnis dan keamanan untuk akses.
A.11.2 Manajemen akses pengguna Sasaran: untuk memastikan akses oleh pengguna yang sah dan untuk mencegah pihak yang tidak sah pada sistem informasi		
A.11.2.1	Pendaftaran pengguna	*Pengendalian* Harus ada prosedur pendaftaran

		dan pembatalan pendaftaran pengguna secara formal untuk pemberian dan pencabutan akses terhadap seluruh layanan dan sistem informasi.
A.11.2.2	Manajemen hak khusus	*Pengendalian* Alokasi penggunaan hak khusus harus dibatasi dan dikendalikan.
A.11.2.3	Manajemen *password* pengguna	*Pengendalian* Alokasi *password* harus dikendalikan dengan proses manajemen formal.
A.11.2.4	Tinjauan terhadap hak akses pengguna	*Pengendalian* Manajemen harus meninjau hak akses pengguna secara regular dengan menggunakan proses formal.
A.11.3 Tanggung jawab pengguna Sasaran: untuk mencegah akses pengguna yang tidak sah dan gangguan atau pencurian atas informasi dan fasilitas pengolahan informasi		
A.11.3.1	Penggunaan *password*	*Pengendalian* Pengguna harus disyaratkan untuk mengikuti pedoman pengamanan yang baik dalam pemilihan dan penggunaan *password*.
A.11.3.2	Peralatan yang ditinggal oleh penggunanya (unattended)	*Pengendalian* Peralatan yang ditinggalkan oleh penggunanya (unattended) harus dipastikan terlindungi dengan tepat.
A.11.3.3	Kebijakan *clear desk* dan *clear screen*	*Pengendalian* Kebijakan *clear desk* terhadap kertas dan media penyimpanan yang dapat dipindahkan dan kebijakan *clear screen* untuk fasilitas pengolahan informasi harus ditetapkan.
A.11.4 Pengendalian akses jaringan Sasaran: untuk mencegah akses yang tidak sah ke dalam layanan jaringan		
A.11.4.1	Kebijakan penggunaan layanan jaringan	*Pengendalian* Pengguna hanya diberikan akses terhadap layanan yang telah diberikan kewenangan penggunaannya secara spesifik.

A.11.4.2	Otentikasi pengguna untuk koneksi eksternal	*Pengendalian* Metode otentikasi yang tepat harus digunakan untuk mengendalikan akses oleh pengguna *remote*.
A.11.4.3	Identifikasi peralatan dalam jaringan	*Pengendalian* Identifikasi peralatan secara otomatis harus dipertimbangkan sebagai cara untuk mengotentikasi koneksi lokasi dan peralatan spesifik.
A.11.4.4	Perlindungan terhadap *remote diagnostic* dan *configuration port*	*Pengendalian* Akses secara fisik dan *logical* terhadap *diagnostic* dan *configuration port* harus dikendalikan.
A.11.4.5	Segregasi dalam jaringan	*Pengendalian* Pengelompokan terhadap layanan informasi, pengguna dan sistem informasi di dalam jaringan harus disegregasikan.
A.11.4.6	Pengendalian koneksi jaringan	*Pengendalian* Untuk jaringan yang digunakan bersama, khususnya perluasan jaringan yang melewati batas perusahaan, kapabilitas pengguna untuk terhubung dengan jaringan harus dibatasi, sejalan dengan kebijakan pengendalian akses dan persyaratan dalam aplikasi bisnis.
A.11.4.7	Pengendalian *routing* jaringan	*Pengendalian* Pengendalian *routing* harus diterapkan ke dalam jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan pengendalian akses dari aplikasi bisnis.
A.11.5 Pengendalian akses sistem operasi Sasaran: untuk mencegah akses tidak sah ke dalam sistem operasi		
A.11.5.1	Prosedur *log-on* yang aman	*Pengendalian* Akses ke dalam sistem operasi harus dikendalikan dengan prosedur *log-on* yang aman.
A.11.5.2	Identifikasi dan otentikasi pengguna	*Pengendalian* Semua pengguna harus memiliki identifikasi unik (user id) yang hanya digunakan secara personal

		dan teknik otentikasi yang sesuai harus dipilih untuk membuktikan identitas pengguna.
A.11.5.3	Sistem manajemen *password*	*Pengendalian* Sistem untuk mengelola *password* harus interaktif dan memastikan kualitas *password*.
A.11.5.4	Penggunaan *system utilities*	*Pengendalian* Penggunaan program *utility* yang kemungkinan mampu mengesampingkan (*overriding*) pengendalian sistem dan aplikasi harus dibatasi dan dikendalikan secara ketat.
A.11.5.5	Sesi *time-out*	*Pengendalian* Sesi yang tidak aktif dalam jangka waktu tertentu harus mati. .
A.11.5.6	Pembatasan waktu koneksi	*Pengendalian* Pembatasan terhadap waktu koneksi harus digunakan untuk menyediakan keamanan tambahan untuk aplikasi yang berisiko tinggi.
A.11.6 Pengendalian akses aplikasi dan informasi Sasaran: untuk mencegah akses yang tidak sah terhadap informasi pada sistem aplikasi		
A.11.6.1.	Pembatasan akses informasi	*Pengendalian* Akses terhadap informasi dan fungsi sistem aplikasi oleh pengguna dan personel pendukung harus dibatasi sesuai dengan kebijakan pengendalian akses yang ditetapkan.
A.11.6.2	Isolasi sistem yang sensitif	*Pengendalian* Sistem yang sensitif harus memiliki lingkungan komputasi yang diisolasi.
A.11.7 *Mobile computing* dan kerja jarak jauh (teleworking) Sasaran: untuk memastikan keamanan informasi ketika menggunakan fasilitas *mobile computing* dan kerja jarak jauh (teleworking)		
A.11.7.1	*Mobile computing* dan komunikasi	*Pengendalian* Kebijakan formal harus tersedia dan tindakan pengamanan yang tepat harus digunakan untuk melindungi terhadap risiko penggunaan fasilitas *mobile computing* dan komunikasi.

A.11.7.2	Kerja jarak jauh	*Pengendalian* Kebijakan, rencana operasional dan prosedur harus dikembangkan dan diterapkan untuk kegiatan kerja jarak jauh.
A.12 Akuisisi, pengembangan dan pemeliharaan sistem informasi		
A.12.1 Persyaratan keamanan dari sistem informasi Sasaran: untuk memastikan bahwa keamanan merupakan bagian yang utuh dari sistem informasi		
A.12.1.1	Analisis dan spesifikasi persyaratan keamanan	*Pengendalian* Pernyataan persyaratan bisnis untuk sistem informasi yang baru, atau peningkatan terhadap sistem informasi yang ada harus menetapkan persyaratan untuk pengendalian keamanan.
A.12.2 Pengolahan yang benar dalam aplikasi Sasaran: Untuk mencegah kesalahan, kehilangan, modifikasi yang tidak sah atau penyalahgunaan informasi dalam aplikasi		
A.12.2.1	Validasi data masukan	*Pengendalian* Masukan data ke dalam aplikasi harus divalidasi untuk memastikan bahwa data tersebut benar dan tepat.
A.12.2.2	Pengendalian pengolahan internal	*Pengendalian* Pengecekan validasi harus di gabungkan ke dalam aplikasi untuk mendeteksi setiap kerusakan informasi karena kesalahan pengolahan atau tindakan yang disengaja.
A.12.2.3	Integritas pesan	*Pengendalian* Persyaratan untuk memastikan keaslian dan perlindungan integritas pesan dalam aplikasi harus diidentifikasi, dan pengendalian yang tepat harus diidentifikasi dan diterapkan.
A.12.2.4	Validasi data keluaran	*Pengendalian* Keluaran data dari aplikasi harus divalidasi untuk memastikan bahwa pengolahan informasi yang disimpan adalah benar dan tepat sesuai dengan keadaan.
A.12.3 Pengendalian dengan cara kriptografi Sasaran: untuk melindungi kerahasiaan, keasliaan atau integritas informasi dengan cara kriptografi		

A.12.3.1	Kebijakan tentang penggunaan pengendalian kriptografi	*Pengendalian* Kebijakan tentang penggunaan pengendalian kriptografi untuk melindungi informasi harus dikembangkan dan diterapkan.
A.12.3.2	Manajemen kunci	*Pengendalian* Manajemen kunci harus tersedia untuk mendukung penggunaan teknik kriptografi oleh organisasi.
A.12.4 Keamanan *system files* Sasaran: untuk memastikan keamanan *system files*		
A.12.4.1	Pengendalian perangkat lunak yang operasional	*Pengendalian* Harus tersedia prosedur untuk mengendalikan instalasi perangkat lunak pada sistem yang operasional.
A.12.4.2	Perlindungan data uji sistem	*Pengendalian* Data uji harus dipilih secara hati-hati, dan dilindungi serta dikendalikan.
A.12.4.3	Pengendalian akses terhadap kode sumber program	*Pengendalian* Akses ke kode sumber program harus dibatasi.
A.12.5 Keamanan dalam proses pengembangan dan pendukung Sasaran: untuk memelihara keamanan perangkat lunak sistem aplikasi dan informasi		
A.12.5.1	Prosedur pengendalian perubahan	*Pengendalian* Penerapan perubahan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.
A.12.5.2	Tinjauan teknis dari aplikasi setelah perubahan sistem operasi	*Pengendalian* Bila sistem operasi diubah, aplikasi kritis bisnis harus ditinjau dan diuji untuk memastikan tidak ada dampak yang merugikan terhadap organisasi atau keamanan.
A.12.5.3	Pembatasan atas perubahan terhadap paket perangkat lunak	*Pengendalian* Modifikasi untuk paket perangkat lunak harus dihindari, dibatasi hanya pada perubahan yang perlu, dan seluruh perubahan harus dikendalikan dengan ketat.

A.12.5.4	Kebocoran informasi	*Pengendalian* Peluang untuk kebocoran informasi harus dicegah.
A.12.5.5	Pengembangan perangkat lunak yang dialihdayakan	*Pengendalian* Pengembangan perangkat lunak yang dialihdayakan harus disupervisi dan dipantau oleh organisasi.
A.12.6 Manajemen kerawanan teknis Sasaran: untuk mengurangi risiko terhadap ekploitasi kerawanan teknis yang dipublikasikan.		
A.12.6.1	Pengendalian kerawanan teknis	*Pengendalian* Informasi tepat waktu tentang kerawanan teknis dari sistem informasi yang digunakan harus diperoleh, eksposur organisasi terhadap kerawanan tersebut dievaluasi, dan diambil tindakan yang tepat untuk menangani risiko terkait.
A.13 Manajemen insiden keamanan informasi **A.13.1 Pelaporan kejadian dan kelemahan keamanan informasi** Sasaran: untuk memastikan kejadian dan kelemahan keamanan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa sehingga memungkinkan tindakan koreksi dilakukan tepat waktu.		
A.13.1.1	Pelaporan kejadian keamanan informasi	*Pengendalian* Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin.
A.13.1.2	Pelaporan kelemahan keamanan	*Pengendalian* Semua pegawai, kontraktor dan pengguna pihak ketiga dari sistem informasi dan layanan harus disyaratkan untuk mencatat dan melaporkan setiap kelemahan keamanan yang diamati dan dicurigai dalam sistem atau layanan
A.13.2 Manajemen insiden keamanan informasi dan perbaikan Sasaran: untuk memastikan pendekatan yang konsisten dan efektif diterapkan untuk manajemen insiden keamanan informasi.		
A.13.2.1	Tanggung jawab dan prosedur	*Pengendalian* Tanggung jawab manajemen dan prosedur harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan sesuai terhadap insiden keamanan informasi.

A.13.2.2	Pembelajaran dari insiden keamanan informasi	*Pengendalian* Harus tersedia mekanisme yang memungkinkan jenis, volume, dan biaya insiden keamanan informasi diukur dan dipantau.
A.13.2.3	Pengumpulan bukti	*Pengendalian* Apabila tindak lanjut terhadap orang atau organisasi setelah insiden keamanan informasi melibatkan tindakan hukum (baik perdata atau pidana), bukti harus dikumpulkan, disimpan, dan disajikan sesuai aturan berkenaan dengan bukti yang ditetapkan dalam wilayah hukum yang relevan.
A.14 Manajemen keberlanjutan bisnis (Business continuity management)		
A.14.1 Aspek keamanan informasi dari manajemen keberlanjutan bisnis Sasaran: untuk menghadapi gangguan kegiatan bisnis dan untuk melindungi proses bisnis kritis dari efek kegagalan utama sistem informasi atau bencana dan untuk memastikan keberlanjutannya secara tepat waktu.		
A.14.1.1	Memasukkan keamanan informasi dalam proses manajemen keberlanjutan bisnis	*Pengendalian* Proses yang dikelola harus dikembangkan dan dipelihara untuk keberlanjutan bisnis organisasi secara menyeluruh, yang menekankan penggunaan persyaratan keamanan informasi yang dibutuhkan untuk keberlanjutan bisnis organisasi.
A.14.1.2	Keberlanjutan bisnis dan asesmen risiko	*Pengendalian* Kejadian yang dapat menyebabkan gangguan terhadap proses bisnis harus diidentifikasi, bersamaan dengan kemungkinan dan dampak dari gangguan tersebut serta konsekuensinya terhadap keamanan informasi.
A.14.1.3	Pengembangan dan penerapan rencana keberlanjutan termasuk keamanan informasi	*Pengendalian* Rencana harus dikembangkan dan diterapkan untuk memelihara atau mengembalikan operasi dan memastikan ketersediaan informasi pada tingkat dan dalam jangka waktu yang disyaratkan setelah terjadinya gangguan atau kegagalan dari proses bisnis kritis.
A.14.1.4	Kerangka kerja perencanaan keberlanjutan bisnis	*Pengendalian* Kerangka kerja tunggal dari rencana keberlanjutan bisnis harus dipelihara untuk memastikan semua rencana konsisten, dan

		menekankan persyaratan keamanan informasi dan untuk mengidentifikasi prioritas untuk pengujian dan pemeliharaan .
A.14.1.5	Pengujian, pemeliharaan dan asesmen ulang rencana keberlanjutan bisnis	*Pengendalian* Rencana keberlanjutan bisnis harus diuji dan dimutakhirkan secara reguler untuk memastikan bahwa rencana tersebut mutakhir dan efektif.

A.15 Kesesuaian		
A.15.1 Kesesuaian dengan persyaratan hukum Sasaran: untuk mencegah pelanggaran terhadap undang-undang, peraturan perundang-undangan atau kewajiban kontrak dan setiap persyaratan keamanan.		
A.15.1.1	Identifikasi peraturan hukum yang berlaku	*Pengendalian* Seluruh statuta, peraturan perundang-undangan dan persyaratan kontrak serta pendekatan organisasi untuk memenuhi persyaratan tersebut harus ditetapkan secara ekplisit, didokumentasikan, dan dijaga pemutakhirannya untuk masing-masing sistem informasi dan organisasi
A.15.1.2	Hak kekayaan intelektual (HAKI)	*Pengendalian* Prosedur yang sesuai harus diterapkan untuk memastikan kesesuaian dengan peraturan hukum, peraturan perundang-undangan dan persyaratan kontrak tentang penggunaan materi berkenaan dimana mungkin terdapat hak kekayaan intelektual dan tentang penggunaan produk perangkat lunak yang memiliki hak paten.
A.15.1.3	Perlindungan rekaman organisasi	*Pengendalian* Rekaman penting harus dilindungi dari kehilangan, penghancuran dan pemalsuan sesuai dengan statuta, peraturan perundang-undangan, persyaratan kontrak dan persyaratan bisnis.
A.15.1.4	Perlindungan data dan rahasia informasi pribadi	*Pengendalian* Perlindungan data dan kerahasiaan harus dijamin seperti yang dipersyaratkan dalam legislasi, regulasi yang relevan, dan klausul

		kontrak, jika diperlukan.
A.15.1.5	Pencegahan penyalahgunaan fasilitas pengolahan informasi	*Pengendalian* Pengguna harus dicegah dari penggunaan fasilitas pengolahan informasi untuk tujuan yang tidak sah
A.15.1.6	Regulasi pengendalian kriptografi	*Pengendalian* Pengendalian kriptografi harus digunakan sesuai dengan seluruh perjanjian, undang-undang dan regulasi yang relevan.
A.15.2 Pemenuhan terhadap kebijakan keamanan dan standar, dan pemenuhan teknis Sasaran: untuk memastikan pemenuhan sistem terhadap kebijakan dan standar keamanan organisasi		
A.15.2.1	Pemenuhan terhadap kebijakan keamanan dan standar	*Pengendalian* Manajer harus memastikan bahwa seluruh prosedur dalam lingkup tanggungjawabnya dilakukan secara benar untuk mencapai pemenuhan terhadap kebijakan keamanan dan standar .
A.15.2.2	Pengecekan pemenuhan teknis	*Pengendalian* Sistem informasi harus secara regular dicek pemenuhan teknis terhadap standar penerapan keamanan.
A.15.3 Pertimbangan audit sistem informasi Sasaran: untuk memaksimalkan keefektifan dari dan untuk meminimalkan interferensi kepada/dari proses audit sistem informasi.		
A.15.3.1	Pengendalian audit sistem informasi	*Pengendalian* Persyaratan audit dan kegiatan yang melibatkan pengecekan pada sistem operasional harus direncanakan secara hati-hati dan disetujui untuk meminimalisasi risiko dari gangguan terhadap proses bisnis.
A.15.3.2	Perlindungan terhadap alat audit informasi	*Pengendalian* Akses terhadap alat audit sistem informasi harus dilindungi untuk mencegah setiap kemungkinan penyalahgunaan atau gangguan (compromise)

Lampiran B
(informatif)

Prinsip-prinsip OECD dan ISO 27001
Prinsip OECD dan Standar ini

Prinsip yang terdapat dalam Pedoman OECD untuk Keamanan Sistem Informasi dan Jaringan diterapkan untuk seluruh kebijakan dan tingkatan operasional sistem informasi dan jaringan. Standar ini menyediakan kerangka kerja sistem manajemen keamanan informasi yang dilandasi prinsip OECD dengan menggunakan model PDCA dan proses yang diuraikan dalam Klausul 4,5,6, dan 8 sebagaimana diindikasikan dalam Tabel B.1.

Tabel B.1 – Prinsip OECD dan model PDCA

Prinsip OECD	Kesesuaian dengan proses SMKI dan tahap PDCA
Kepedulian Peserta sebaiknya peduli terhadap kebutuhan keamanan sistem informasi dan jaringan dan apa yang mereka dapat lakukan untuk meningkatkan keamanan	Kegiatan ini merupakan bagian dari tahap ***Do*** (lihat 4.2.2 dan 5.2.2)
Tanggung jawab Seluruh peserta bertanggung jawab atas keamanan sistem informasi dan jaringan	Kegiatan ini merupakan bagian dari tahap ***Do*** (lihat 4.2.2 dan 5.1)
Tanggapan Peserta sebaiknya bertindak tepat waktu dan kooperatif untuk mencegah, mendeteksi dan menanggapi terhadap insiden keamanan	Hal ini merupakan kegiatan pemantauan bagian dari tahap ***Check*** (lihat 4.2.3 dan 6 sampai 7.3) dan kegiatan yang ditanggapi merupakan bagian dari tahap ***Act*** (lihat 4.2.4 dan 8.1 sampai 8.3). Hal ini juga dicakup oleh beberapa aspek dari tahap ***Plan*** dan ***Check***.
Asesmen risiko Peserta sebaiknya melaksanakan asesmen risiko	Kegiatan ini merupakan bagian dari tahap ***Plan*** (lihat 4.2.1) dan asesmen ulang risiko merupakan bagian dari tahap ***Check*** (lihat 4.2.3 dan 6 sampai 7.3).
Desain dan penerapan keamanan Peserta sebaiknya menggabungkan keamanan sebagai elemen esensial dari sistem informasi dan jaringan.	Ketika asesmen risiko telah dilengkapi, pengendalian yang dipilih untuk perlakuan risiko sebagai bagian dari tahap ***Plan*** (lihat 4.2.1). Tahap ***Do*** (lihat 4.2.2 dan 5.2) mencakup penerapan dan penggunaan operasional dari pengendalian ini.
Manajemen keamanan Peserta sebaiknya mengadopsi pendekatan komprehensif untuk manajemen keamanan.	Manajemen risiko merupakan suatu proses yang mencakup pencegahan, deteksi dan tanggapan terhadap insiden, pemeliharaan yang sedang berlangsung, kajian dan audit. Seluruh aspek tersebut dicakup dalam tahap ***Plan, Do, Check dan Act.***
Asesmen ulang Peserta sebaiknya mengkaji dan mengases ulang keamanan sistem informasi dan jaringan,	Asesmen ulang keamanan informasi merupakan bagian dari tahap ***Check*** (lihat 4.2.3 dan 6 sampai 7.3) dimana kajian regular sebaiknya

Prinsip OECD	Kesesuaian dengan proses SMKI dan tahap PDCA
dan membuat modifikasi yang sesuai terhadap kebijakan keamanan, praktek, tindakan dan prosedur.	dilaksanakan untuk memeriksa keefektifan sistem manajemen keamanan informasi dan peningkatan keamanan merupakan bagian dari tahap ***Act*** (lihat 4.2.4 dan 8.2 sampai 8.3).

Lampiran C
(informatif)

Kesesuaian antara SNI 19-9001-2001, SNI 19 – 14001 – 2005 dan Standar ini

Tabel C.1 menunjukkan kesesuaian antara SNI 19-9001-2001, SNI 19 – 14001 – 2005 dan Standar ini.

Tabel C.1 - Kesesuaian antara SNI 19-9001-2001, SNI 19–14001–2005 dan Standar ini

Standar ini	SNI 19-9001-2001	SNI 19–14001–2005
0 Pendahuluan	**0 Pendahuluan**	**Pendahuluan**
0.1 Umum	0.1 Umum	
0.2 Pendekatan proses	0.2 Pendekatan proses	
	0.3 Hubungan dengan ISO 9004	
0.3 Kesesuaian dengan sistem manajemen lainnya	0.4 Kesesuaian dengan sistem manajemen lainnya	
1 Ruang lingkup	**1 Ruang lingkup**	**1 Ruang lingkup**
1.1. Umum	1.1. Umum	
1.2. Penerapan	1.2. Penerapan	
2 Acuan normatif	**2 Acuan normatif**	**2 Acuan normatif**
3 Istilah dan definisi	**3 Istilah dan definisi**	**3 Istilah definisi**
4 Sistem manajemen keamanan informasi	**4 Sistem manajemen mutu**	**4 Sistem Manajemen Lingkungan**
4.1. Persyaratan umum	4.1. Persyaratan umum	4.1. Persyaratan umum
4.2. Penetapan dan pengelolaan SMKI		
4.2.1. Penetapan SMKI		
4.2.2 Penerapan dan pengoperasian SMKI		4.4. Penerapan dan operasi
4.2.3 Pemantauan dan pengkajian SMKI	8.2.3 Pemantauan dan pengukuran proses	4.5.1 Pemantauan dan pengukuran
	8.2.4 Pemantauan dan pengukuran produk	
4.2.4 Pemeliharaan dan peningkatan SMKI		

Standar ini	SNI 19-9001-2001	SNI 19–14001–2005
4.3 Persyaratan dokumentasi	4.2. Persyaratan dokumentasi	
4.3.1 Umum	4.2.1. Umum	
	4.2.2 Panduan mutu	
4.3.2 Pengendalian dokumen	4.2.3 Pengendalian dokumen	4.4.5 Pengendalian dokumentasi
4.3.3 Pengendalian rekaman	4.2.4 Pengendalian rekaman	4.5.4 Pengendalian rekaman
5 Tanggung jawab manajemen	**5 Tanggung jawab manajemen**	
5.1. Komitmen manajemen	5.1 Komitmen manajemen	
	5.2 Fokus pelanggan	
	5.3 Kebijakan mutu	4.2 Kebijakan lingkungan
	5.4 Perencanaan	4.3 Perencanaan
	5.5 Tanggung jawab, wewenang dan komunikasi	
5.2 Manajemen sumberdaya	**6 Manajemen sumberdaya**	
5.2.1 Ketentuan sumberdaya	6.1 Ketentuan sumberdaya	
	6.2 Sumberdaya manusia	
5.2.2 Pelatihan, kepedulian dan kompetensi	6.2.2 Kompetensi, kepedulian dan pelatihan	4.4.2 Kompetensi, pelatihan dan kepedulian
	6.3 Infrastruktur	
	6.4 Lingkungan kerja	
6 Audit internal SMKI	8.2.2 Audit internal	4.4.5 Audit internal
7 Kajian manajemen SMKI	**5.6 Tinjauan manajemen**	**4.6 Tinjauan manajemen**
7.1 Umum	5.6.1 Umum	
7.2 Masukan kajian	5.6.2 Masukan tinjauan	
7.3 Keluaran kajian	5.6.3 Keluaran tinjauan	
8 Peningkatan SMKI	**8.5 Peningkatan**	
8.1 Peningkatan berkelanjutan	8.5.1 Peningkatan berkelanjutan	
8.2 Tindakan korektif	8.5.3 Tindakan korektif	4.5.3 Ketidaksesuaian, tindakan korektif dan tindakan pencegahan

Standar ini	SNI 19-9001-2001	SNI 19–14001–2005
8.3 Tindakan pencegahan	8.5.3 Tindakan pencegahan	
Lampiran A Sasaran pengendalian dan pengendalian		**Lampiran A Panduan tentang penggunaan Standar ini**
Lampiran B Prinsip OECD dan Standar ini		
Lampiran C Kesesuaian antara SNI 19-9001-2001, SNI 19-14001-2005 dan Standar ini	**Lampiran A Kesesuaian antara SNI 19-9001-2001 dan SNI 19-14001-2005**	**Lampiran B Kesesuaian antara SNI 19-14001-2005 dan SNI 19-9001-2001**

Bibliografi

Standards publications

[1] ISO 9001:2000*, Quality management systems — Requirements*

[2] ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of informationand communications technology security — Part 1: Concepts and models for information and communications technology security management*

[3] ISO/IEC TR 13335-3:1998, *Information technology — Guidelines for the management of IT Security —Part 3: Techniques for the management of IT security*

[4] ISO/IEC TR 13335-4:2000, *Information technology — Guidelines for the management of IT Security —Part 4: Selection of safeguards*

[5] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*

[6] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*

[7] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*

[8] ISO/IEC Guide 62:1996, *General requirements for bodies operating assessment and certification/registration of quality systems*

[9] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

Other publications

[1] OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July 2002. www.oecd.org*

[2] NIST SP 800-30, *Risk Management Guide for Information Technology Systems*

[3] Deming W.E., Out *of the Crisis, Cambridge, Mass: MIT, Center for Advanced Engineering Study, 198*

BADAN STANDARDISASI NASIONAL - BSN
Gedung Manggala Wanabakti Blok IV Lt. 3-4
Jl. Jend. Gatot Subroto, Senayan Jakarta 10270
Telp: 021- 574 7043; Faks: 021- 5747045; e-mail : bsn@bsn.go.id