SURAT PEKELILING ICT NO. 3/2012

DARIPADA: Setiausaha Kerajaan Negeri

KEPADA: Semua Setiausaha Tetap Kementerian
Semua Ketua Jabatan Negeri
Semua Residen dan Pegawai Daerah
Semua Pihak Berkuasa Tempatan
Semua Badan Berkanun Negeri

PERKARA: PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 (ISMS) DALAM SEKTOR AWAM NEGERI

RUJ. KAMI: JKM/ICTU/100-15.02 KLT.1(๒๒) **TARIKH:** 7 Disember 2012

---

1. TUJUAN

1.1 Surat Pekeliling ini bertujuan untuk memaklumkan bahawa Kerajaan Negeri mengambil maklum kepentingan pelaksanaan pensijilan MS ISO/IEC 27001:2007 dalam sektor awam. Oleh yang demikian, semua agensi Kerajaan Negeri digalakkan untuk melaksanakan pensijilan ini di agensi masing-masing dengan berpandukan kepada surat arahan yang dikeluarkan oleh Ketua Pengarah, Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU).

2. PELAKSANAAN

2.1 Surat Arahan dan Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam adalah dilampirkan bersama untuk rujukan dan tindakan selanjutnya.

2.2 Agensi Kerajaan yang bersedia untuk melaksanakan pensijilan ISMS dikehendaki berhubung dengan Unit ICT, Jabatan Ketua Menteri untuk maklumat lanjut berkenaan kaedah pelaksanaan.

3. TARIKH KUAT KUASA

3.1 Surat Pekeliling ini berkuat kuasa dari tarikh ia dikeluarkan. Surat Pekeliling ini diedarkan secara *online* di Berita SarawakNet dan juga di Laman Pekeliling Kerajaan Negeri.

Sekian, harap maklum.

"BERSATU BERUSAHA BERBAKTI"

"AN HONOUR TO SERVE"

(TAN SRI DATUK AMAR HAJI MOHAMAD MORSHIDI BIN ABDUL GHANI)
Setiausaha Kerajaan Sarawak

KERAJAAN MALAYSIA

PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

JABATAN PERDANA MENTERI MALAYSIA
24 NOVEMBER 2010

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

Telefon: 603 – 88723000
Faks : 603 – 88883721

Ruj. Kami : MAMPU.BPICT.700-4/3/5 Jld 2(5)
Tarikh : 24 November 2010

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun
Semua Pihak Berkuasa Tempatan

PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007DALAM SEKTOR AWAM

TUJUAN

Surat arahan ini bertujuan untuk menjelaskan kaedah pelaksanaan dan pensijilan standard MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (*Information Security Management System* - ISMS) di agensi-agensi Kerajaan.

LATAR BELAKANG

2. Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah mengambil maklum bahawa tahap keselamatan maklumat kritikal negara perlu memenuhi standard antarabangsa yang boleh dicapai melalui pelaksanaan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat.

3. Mesyuarat Jemaah Menteri juga telah bersetuju Sektor Awam yang merupakan sebahagian dari Prasarana Maklumat Kritikal Negara (*Critical National Information Infrastructure* – CNII) perlu mendapatkan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat dalam tempoh 3 tahun. Sebarang usaha untuk mendapatkan pensijilan tersebut dalam tempoh lebih awal adalah digalakkan.

4. Bagi tujuan ini, maksud Prasarana Maklumat Kritikal Negara adalah seperti yang ditakrif di bawah Dasar Keselamatan Siber Nasional yang merangkumi aset, sistem dan fungsi ICT yang amat penting kepada Negara di mana sekiranya

keupayaan beroperasi seperti biasa terganggu akan mengakibatkan kerugian besar dari segi:

a) Kekuatan ekonomi Negara;

b) Imej nasional;

c) Pertahanan dan keselamatan;

d) Keupayaan Kerajaan berfungsi; dan

e) Kesihatan awam.

5. Dalam pada itu, agensi awam yang di luar golongan Prasarana Maklumat Kritikal Negara adalah juga digalakkan untuk turut serta mencapai pensijilan bagi menjamin kepentingan sistem penyampaian perkhidmatan pelanggan.

PELAKSANAAN

6. Dalam melaksanakan keputusan ini, Ketua Jabatan hendaklah mengambil tindakan berikut:

a) Mengatur rancangan pematuhan pensijilan ISMS sebagaimana yang telah ditetapkan oleh Jemaah Menteri dan memberi maklum balas mengikut keperluan dari masa ke masa;

b) Mengenal pasti skop pelaksanaan dan pensijilan ISMS berdasarkan perkhidmatan kritikal agensi; dan

c) Merujuk kepada dokumen-dokumen berikut sebagai panduan pelaksanaan:

i) Malaysian Standard (MS ISO/IEC 27001:2007 *Information technology - Security techniques - Information Security Management Systems – Requirement);*

ii) International Standard (ISO/IEC 27003:2009 *Information technology - Security techniques - Information Security Management System Implementation Guidance); dan*

iii) International Standard (ISO/IEC 27004: 2009 *Information Technology-Security Techniques - Information Security Management Measurement).*

KHIDMAT NASIHAT

7. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) Jabatan Perdana Menteri menyediakan khidmat rundingan ISMS dalam lima (5) bidang khusus iaitu penentuan skop ISMS agensi, penggubalan dasar keselamatan ICT agensi, melaksanakan penilaian risiko, penyediaan pelan penguraian risiko (*Risk Treatment Plan*) serta pernyataan pemakaian (*Statement of Applicability*).

8. Sebarang pertanyaan berkaitan dengan surat arahan ini dan skop pelaksanaan pensijilan ISMS hendaklah dirujuk kepada:

Ketua Pengarah
Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 6, Blok B2, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya

KEPERLUAN TAMBAHAN AUDIT ISMS

9. Proses audit dan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat hendaklah dilaksanakan oleh badan pensijilan tempatan yang bertauliah dan telah diakreditasikan oleh Jabatan Standard Malaysia. Juru audit pensijilan hendaklah terdiri dari rakyat Malaysia dan mesti menandatangani Perakuan berkenaan Akta Rahsia Rasmi 1972.

PEMAKAIAN

10. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, surat arahan ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun dan Pihak Berkuasa Tempatan.

KUAT KUASA

11. Surat arahan ini berkuatkuasa mula tarikh ia dikeluarkan.

"BERKHIDMAT UNTUK NEGARA"

(DATO' MOHAMAD ZABIDI ZAINAL)
Ketua Pengarah
Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia (MAMPU)

KERAJAAN MALAYSIA

PANDUAN KEPERLUAN DAN PERSEDIAAN PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

JABATAN PERDANA MENTERI MALAYSIA
24 NOVEMBER 2010

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 603 – 8872 0000
Faks : 603 – 8888 3721

Ruj. Kami : MAMPU.BPICT.700-4/3/5 Jld. 2 (6)
Tarikh : 24 November 2010

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun
Semua Pihak Berkuasa Tempatan

PANDUAN KEPERLUAN DAN PERSEDIAAN
PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

TUJUAN

1. Panduan ini bertujuan untuk memberi kefahaman mengenai keperluan dan persediaan pensijilan dalam melaksanakan Pengurusan Sistem Keselamatan Maklumat (ISMS) berasaskan MS ISO/IEC 27001:2007 *Information Technology- Security Techniques – Information Security Management Systems-Requirements* yang dikeluarkan oleh Jabatan Standard Malaysia.

LATAR BELAKANG

2. Kerajaan Malaysia telah membuat pelaburan yang banyak ke atas aset Teknologi Maklumat dan Komunikasi (ICT) sama ada dalam bentuk infrastruktur, teknologi, aplikasi dan proses. Demi memastikan bahawa aset ICT Kerajaan digunakan dengan optimum dalam keadaan selamat untuk menyokong penyampaian perkhidmatan yang berkesan kepada pelanggan, maka perlu digerakkan inisiatif ke arah jaminan kualiti pengurusan sistem keselamatan aset ICT Kerajaan.

3. Bagi memastikan keberkesanan pembangunan infrastruktur keselamatan ICT sektor awam, Kerajaan telah memperkenalkan instrumen strategik penggubalan dasar keselamatan seperti Rangka Dasar Keselamatan ICT, *Malaysian Public Sector Management of ICT Security Handbook* (MyMIS), Mekanisme Pelaporan Insiden

Keselamatan ICT, Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik Di Agensi-Agensi Kerajaan, Garis Panduan Penilaian Risiko Maklumat Sektor Awam, Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT dan Pengurusan Kesinambungan Perkhidmatan.

4. Walaupun pelaksanaan program ICT di agensi agak memberangsangkan, namun banyak usaha yang perlu dilaksanakan termasuk memperkukuh dan memastikan keselamatan aset ICT. Dalam hal ini, Kerajaan harus mengambil initiatif untuk mengamalkan pengurusan sistem keselamatan ICT yang berlandaskan kepada standard antarabangsa.

PANDUAN PELAKSANAAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

5. Panduan ini menjelaskan tindakan yang perlu diambil oleh semua kementerian, jabatan dan agensi Kerajaan Malaysia supaya mencapai taraf MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat.

6. Panduan ini mengandungi dua (2) bahagian berikut:

i) Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam; dan

ii) Panduan Pelaksanaan Audit Dalam ISMS Sektor Awam.

TARIKH BERKUAT KUASA

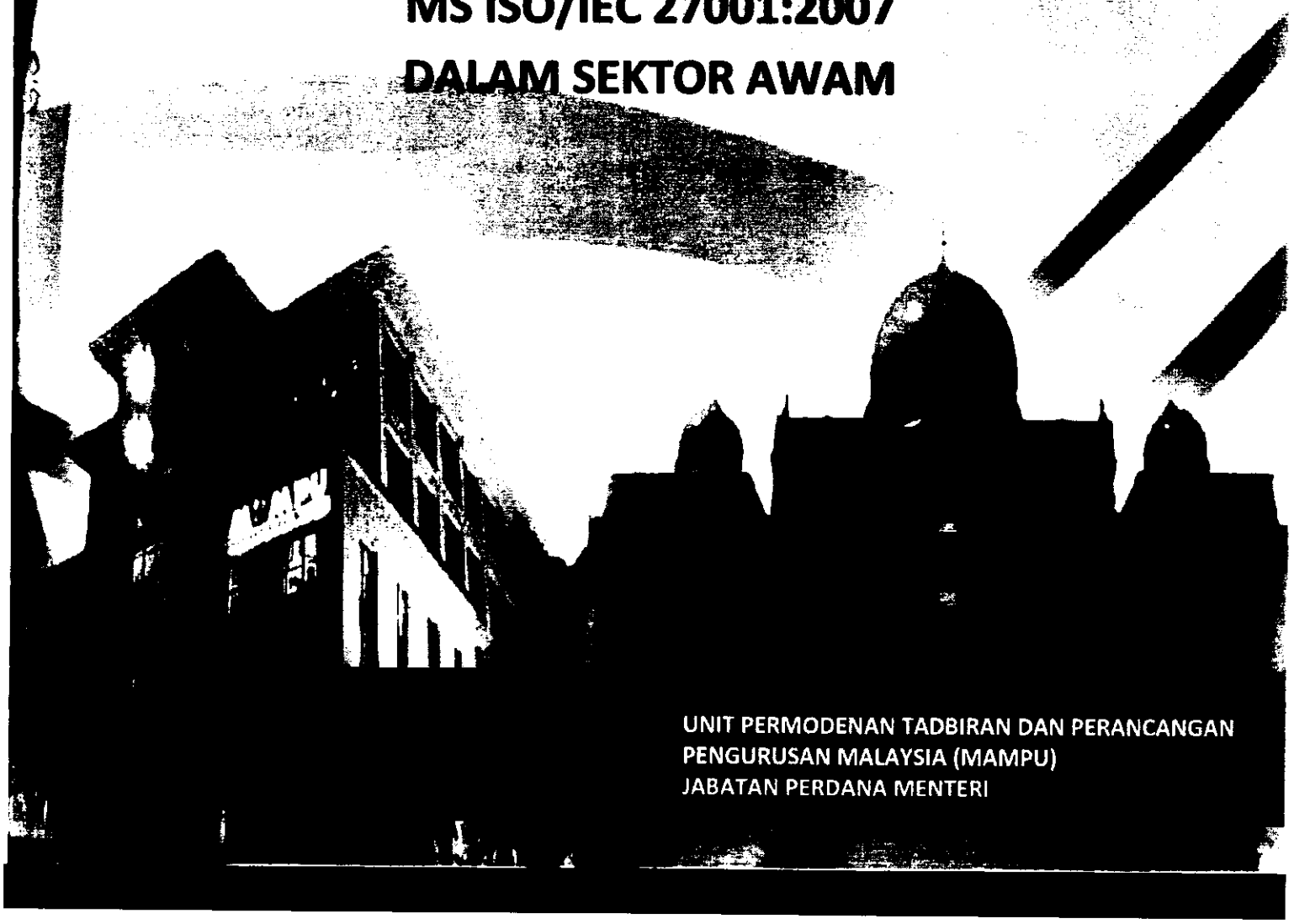
7. Panduan ini berkuat kuasa mulai tarikh ia dikeluarkan.

"BERKHIDMAT UNTUK NEGARA"

(DATO' MOHAMAD ZABIDI ZAINAL)
Ketua Pengarah
Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia (MAMPU)

(Lampiran Kepada Surat Ketua Pengarah MAMPU)
Rujukan MAMPU: MAMPU.BPICT.700-4/3/5 Jld. 2 (6)
Tarikh: 24 November 2010

PANDUAN KEPERLUAN DAN PERSEDIAAN PELAKSANAAN PENSIJILAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM



UNIT PERMODENAN TADBIRAN DAN PERANCANGAN
PENGURUSAN MALAYSIA (MAMPU)
JABATAN PERDANA MENTERI

Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 6, Blok B2
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA

Telefon: 603-8872 3000
Telefaks: 603-8888 3721
Laman web: www.mampu.gov.my
Versi: 1
Pada: 2010
Penulis: MAMPU

Hak Cipta Terpelihara

Semua hak cipta terpelihara. Tiada mana-mana bahagian jua daripada ini yang boleh diterbitkan semula atau disimpan di dalam bentuk yang boleh dipinda semula atau disiarkan dalam sebarang bentuk dengan apa jua cara elektronik, mekanikal, fotokopi, rakaman dan/atau sebaliknya tanpa mendapat keizinan daripada MAMPU

Kerajaan Malaysia berhak untuk mengubah atau menggubal mana-mana bahagian dalam dokumen ini pada bila-bila masa tanpa pemberitahuan awal. Kerajaan Malaysia tidak bertanggungjawab terhadap sebarang kesalahan cetak dan kesulitan cetak akibat daripada dokumen ini.

1. [redacted]

Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam ini menerangkan keperluan asas serta penerangan ringkas mengenai persediaan pelaksanaan pensijilan ISMS. Antaranya tujuan pelaksanaan, skop panduan yang terlibat, definisi istilah yang diguna pakai dalam dokumen panduan, singkatan nama atau istilah dan senarai dokumen rujukan yang diperlukan sebagai rujukan kepada panduan ini.

[redacted]

Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam bertujuan untuk memberi kefahaman mengenai keperluan standard dalam melaksanakan pensijilan Pengurusan Sistem Keselamatan Maklumat (ISMS) berasaskan *Malaysian Standard* (MS), MS ISO/IEC 27001:2007 *Information Technology- Security Techniques – Information Security Management Systems-Requirements* yang dikeluarkan oleh Jabatan Standard Malaysia.

[redacted]

Panduan ini mengandungi enam (6) aspek berikut:

a. **Pengenalan**

   Tujuan dan skop dokumen Panduan Keperluan dan Persediaan Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam.

b. **Keselamatan Teknologi Maklumat dan Komunikasi (ICT)**

   Menerangkan dasar keselamatan yang perlu diambil perhatian oleh semua agensi Kerajaan dalam melindungi aset ICT Kerajaan.

c. **Pengurusan Sistem Keselamatan Maklumat**

   Panduan pengurusan sistem keselamatan maklumat yang merangkumi rangka kerja, reka bentuk, pelaksanaan, pengurusan, penyelenggaraan, penguatkuasaan proses keselamatan maklumat dalam organisasi secara keseluruhan.

d. **Model PDCA Dalam MS ISO/IEC 27001:2007**

MS ISO/IEC 27001:2007 menggunakan model PDCA dalam proses ISMS

e. **Panduan Pelaksanaan MS ISO/IEC 27001:2007 Dalam Sektor Awam**

Menerangkan perkara-perkara yang perlu diambil tindakan untuk memenuhi keperluan MS ISO/IEC 27001:2007.

f. **Pensijilan**

Menerangkan persediaan pensijilan dan metodologi audit yang diguna pakai oleh badan pensijilan tempatan dalam menjayakan proses pensijilan MS ISO/IEC 27001:2007 di agensi kerajaan.

Aset	**Bermaksud semua aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia yang mempunyai nilai kepada agensi**
Ancaman	Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Dasar Keselamatan ICT	**Bermaksud dokumen yang mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT). Dasar hendaklah juga menerangkan kepada semua pengguna mengenai peranan dan tanggungjawab dalam melindungi aset ICT.**
Integriti	Bermaksud data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.

Insiden keselamatan	**Bermaksud musibah yang berlaku ke atas sistem maklumat dan komunikasi (ICT) atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT samada yang ditetapkan secara tersurat atau tersirat.**
Kerahsiaan	Bermaksud maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
Kebolehsediaan	**Bermaksud data dan maklumat hendaklah boleh diakses pada bila-bila masa.**
Kawalan	Bermaksud langkah-langkah pengukuhan yang diguna pakai untuk mengurus risiko.
Keselamatan maklumat	**Bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.**
Kawalan Rekod	Bermaksud peraturan bagi memastikan rekod sentiasa diselenggara dan disimpan dengan teratur supaya mudah dikesan apabila diperlukan untuk rujukan
Keterdedahan (*vulnerability*)	**Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman**
Kajian Semula	Bermaksud langkah-langkah untuk mengendalikan kajian semula ke atas pengurusan keselamatan maklumat bagi menilai keberkesanannya serta peluang penambahbaikan secara berterusan
Pengurusan Sistem Keselamatan	**Bermaksud perkara-perkara yang perlu diberikan tumpuan untuk mewujud, melaksana, memantau, menyemak, menyelenggara dan**

Maklumat	menambah baik keselamatan maklumat.
Pelan Penguraian Risiko*(Risk Treatment Plan-RTP)*	Bermaksud strategi untuk menangani risiko keselamatan ICT.
Proses	Bermaksud proses yang mengguna pakai model *Plan-Do-Check-Act* (PDCA). Setiap proses hendaklah dirancang *(Plan)*; dilaksana dan diselenggara (*Do*); dipantau, dinilai dan dikaji semula (*Check*) dan ditambah baik (*Act)*
Prosedur	Bermaksud peranan dan tanggungjawab serta langkah-langkah yang perlu dilaksanakan dalam sesuatu proses atau aktiviti.
Penilaian Risiko	Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Penyataan Pemakaian (*Statement of Applicability- SoA)*	Bermaksud menyenaraikan justifikasi pemilihan kawalan, *Annex A* dalam MS ISO/IEC 27001:2007 dan sebarang rujukan dalam melindungi keselamatan aset ICT.
Rekod	Bermaksud data/maklumat yang bertulis/elektronik hasil daripada aktiviti ISMS sebagai bukti pelaksanaan.
Risiko	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan keraguan
Tindakan Pembetulan	Bermaksud tindakan segera bagi mengelak kejadian berulang yang boleh menjejaskan sistem keselamatan maklumat.
Tindakan Pencegahan	Bermaksud tumpuan untuk menghapuskan sebab-sebab sesuatu kesilapan mungkin berlaku supaya ianya tidak akan berlaku.

MS	***Malaysian Standard***
ISO	*International Organization for Standardization*
IEC	***International Electrotechnical Commission***
ISMS	*Information Security Management System*
MyRAM	***The Malaysian Public Sector Risk Assessment Methodology***
ICT	*Information and Communications Technology*
PDCA	***Plan-Do-Check-Act***
RTP	*Risk Treatment Plan*
SoA	***Statement of Applicability***

Antara dokumen yang berkaitan adalah:

1. MS ISO/IEC 27001:2007 *Information Technology- Security Techniques- Information Security Management Systems-Requirements;*
2. Surat Arahan Ketua Pengarah MAMPU bertarikh 24 November 2010: Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 Dalam Sektor Awam;
3. Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
4. MS ISO/IEC 27002:2005 *Code of Practise- Information Techniques – Security Techniques-Code of Practice For Information Security Management System;*
5. Pekeliling Am Bilangan 1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); dan
6. Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.

2.

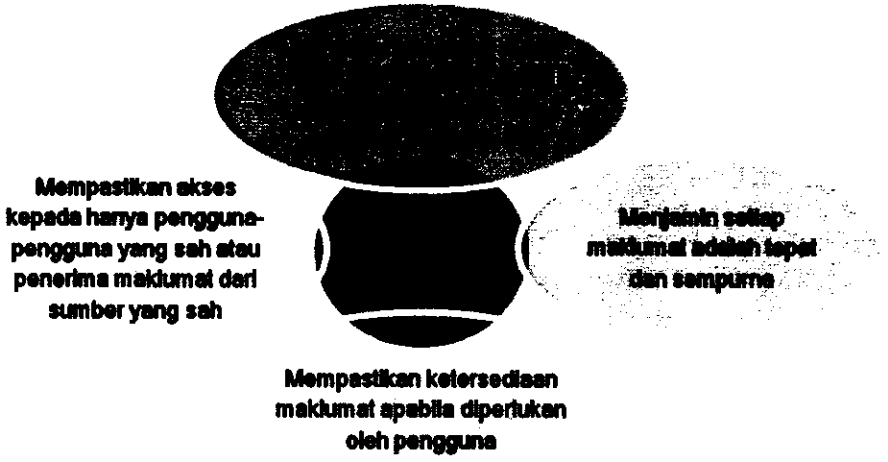
Keselamatan aset teknologi maklumat dan komunikasi (*Information and Communications Technology*), ringkasnya ICT, berkait rapat dengan perlindungan maklumat yang terkandung dalam aset ICT.

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

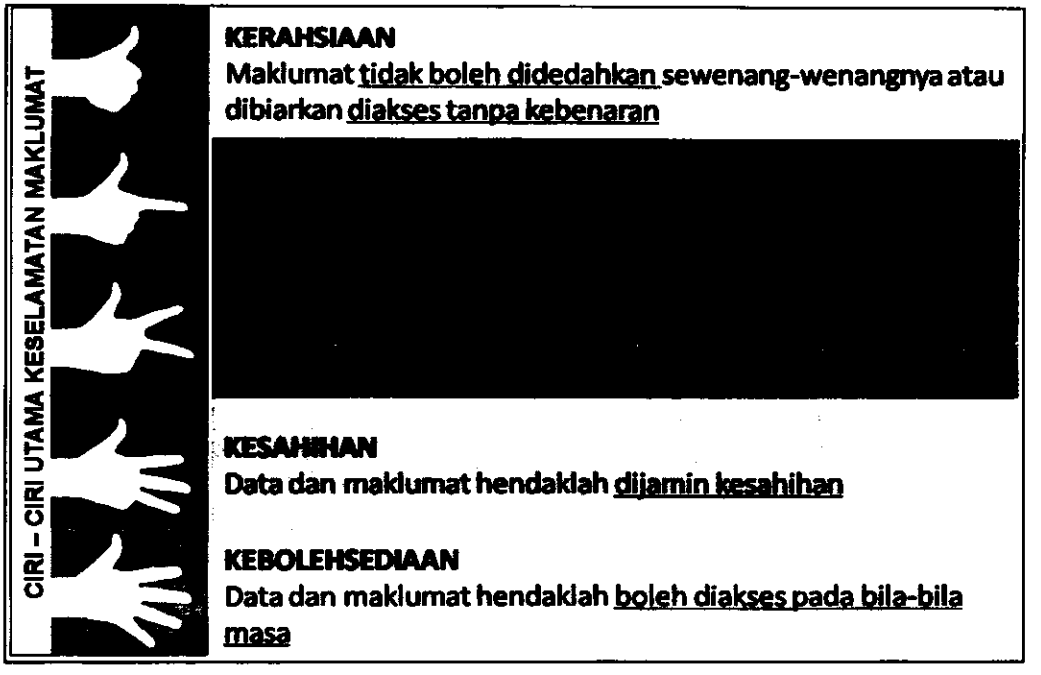
Merujuk kepada Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan, terdapat empat (4) komponen asas keselamatan seperti dalam Rajah 1.

Rajah 1: Komponen Asas Keselamatan ICT



Keselamatan ICT Kerajaan merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan berdasarkan ciri-ciri utama keselamatan maklumat seperti dalam Rajah 2.

Rajah 2: Ciri Utama Keselamatan Maklumat



3.

Semua agensi Kerajaan digalakkan untuk melaksanakan amalan baik dalam pengurusan sistem keselamatan maklumat. Penggunaan amalan baik tersebut akan mendorong agensi ke arah menguruskan keselamatan maklumat yang cemerlang menerusi pengiktirafan pensijilan MS ISO/IEC 27001:2007

Pemakaian standard bagi sesebuah sistem pengurusan dapat membantu agensi dalam melaksanakan sistem penyampaian mereka. Melalui standard tersebut, agensi secara konsisten dapat menyediakan sebuah rangka kerja ke arah memenuhi keperluan-keperluan yang ditetapkan oleh standard dan *industry best practise*. Standard MS ISO 9001:2008 menyatakan keperluan ke atas sistem pengurusan kualiti yang mana agensi dapat menunjukkan keupayaannya menyampaikan perkhidmatan yang memenuhi tuntutan serta kepuasan pelanggan dan peraturan-peraturan semasa.

Manakala standard MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (*Information Security Management System*, ISMS) pula adalah pelengkap kepada sistem pengurusan kualiti di mana standard ini menyediakan spesifikasi dan kawalan-kawalan bagi melindungi keselamatan aset maklumat dan seterusnya meningkatkan integriti dan keyakinan pelanggan kepada agensi berkenaan. Melalui pengauditan ke atas aset ICT, tindakan pembetulan dan penambahbaikan dapat diambil ke atas sebarang kelemahan, ketidakpatuhan atau kekurangan kepada sistem

pengurusan keselamatan ICT sedia ada demi memantapkan perlindungan kepada prinsip-prinsip kerahsiaan, integriti dan ketersediaan.

Program pengurusan sistem keselamatan maklumat berdasarkan standard MS ISO/IEC 27001:2007 adalah program pensijilan yang telah mendapat pengiktirafan di peringkat antarabangsa. Oleh itu, adalah penting pensijilan tersebut diperkenalkan untuk diguna pakai oleh agensi-agensi Kerajaan di mana penggunaan ICT telah menjadi komponen penting untuk penyampaian perkhidmatan Kerajaan masa kini.

Pensijilan MS ISO/IEC 27001:2007 dapat dijadikan sebagai tanda aras mengenai tahap pengurusan sistem keselamatan maklumat sesebuah agensi. Secara tidak langsung pensijilan ini mampu mendorong agensi ke arah pengurusan keselamatan ICT yang cemerlang.

Prinsip-prinsip asas standard MS ISO/IEC 27001:2007 adalah untuk melindungi kerahsiaan, integriti dan kebolehsediaan maklumat. Prinsip ini bermaksud:

a) Maklumat hendaklah dilindungi dari pihak lain yang tidak diberi kuasa menggunakan maklumat;

b) Maklumat hendaklah sentiasa tepat, lengkap dan kemas kini semasa ianya diproses; dan

c) Maklumat hendaklah sentiasa tersedia jika diperlukan oleh pihak lain yang diberi kuasa mencapai maklumat tersebut.

[redacted]

Program ISMS harus direka bentuk bagi memastikan pengurusan sistem keselamatan maklumat adalah mencukupi dan berkesan untuk melindungi aset ICT agensi serta dapat memberi keyakinan dan jaminan kepada pihak yang berkepentingan.

Perkara berikut harus diambil kira dalam menjayakan ISMS:

a) Menyediakan program kesedaran keselamatan maklumat
b) Melaksanakan peranan dan tanggungjawab dalam mencapai objektif keselamatan maklumat
c) Melaksanakan penilaian risiko supaya langkah-langkah perlindungan paling berkesan dikenal pasti
d) Mengambil kira keperluan stakeholder dan komitmen pengurusan
e) Mencegah dan mengesan insiden keselamatan maklumat
f) Menilai keselamatan maklumat secara berterusan dan mengambil tindakan pembetulan atau penambahbaikan.

[redacted]

ISMS merupakan proses penambahbaikan pengurusan sistem keselamatan yang berterusan. Sokongan dan komitmen pengurusan kementerian, jabatan dan agensi Kerajaan amat penting dalam mencapai kejayaan pelaksanaan ISMS bagi memperoleh faedah-faedah berikut:

a) Mengukur dan menilai tahap keselamatan maklumat berdasarkan pensijilan sebagai penanda aras;
b) Meminimumkan masalah kegagalan sistem, serta insiden-insiden siber bagi menjamin aspek kesinambungan perkhidmatan Kerajaan;
c) Meminimumkan kadar risiko dan keterdedahan (*vulnerability*) dan kelemahan sistem keselamatan maklumat Kerajaan ;
d) Meningkatkan keyakinan masyarakat terhadap tahap keselamatan maklumat Kerajaan; dan
e) Meningkat indeks pencapaian Kerajaan di peringkat antarabangsa.

4. [redacted]

Pelaksanaan pensijilan ISMS mengguna pakai model *Plan-Do-Check-Act* dalam setiap fasa pelaksanaannya. Model ini merangkumi aktiviti pewujudan, pelaksanaan, operasi, pemantauan, penyelenggaraan dan penambahbaikan dalam ISMS.

[redacted]

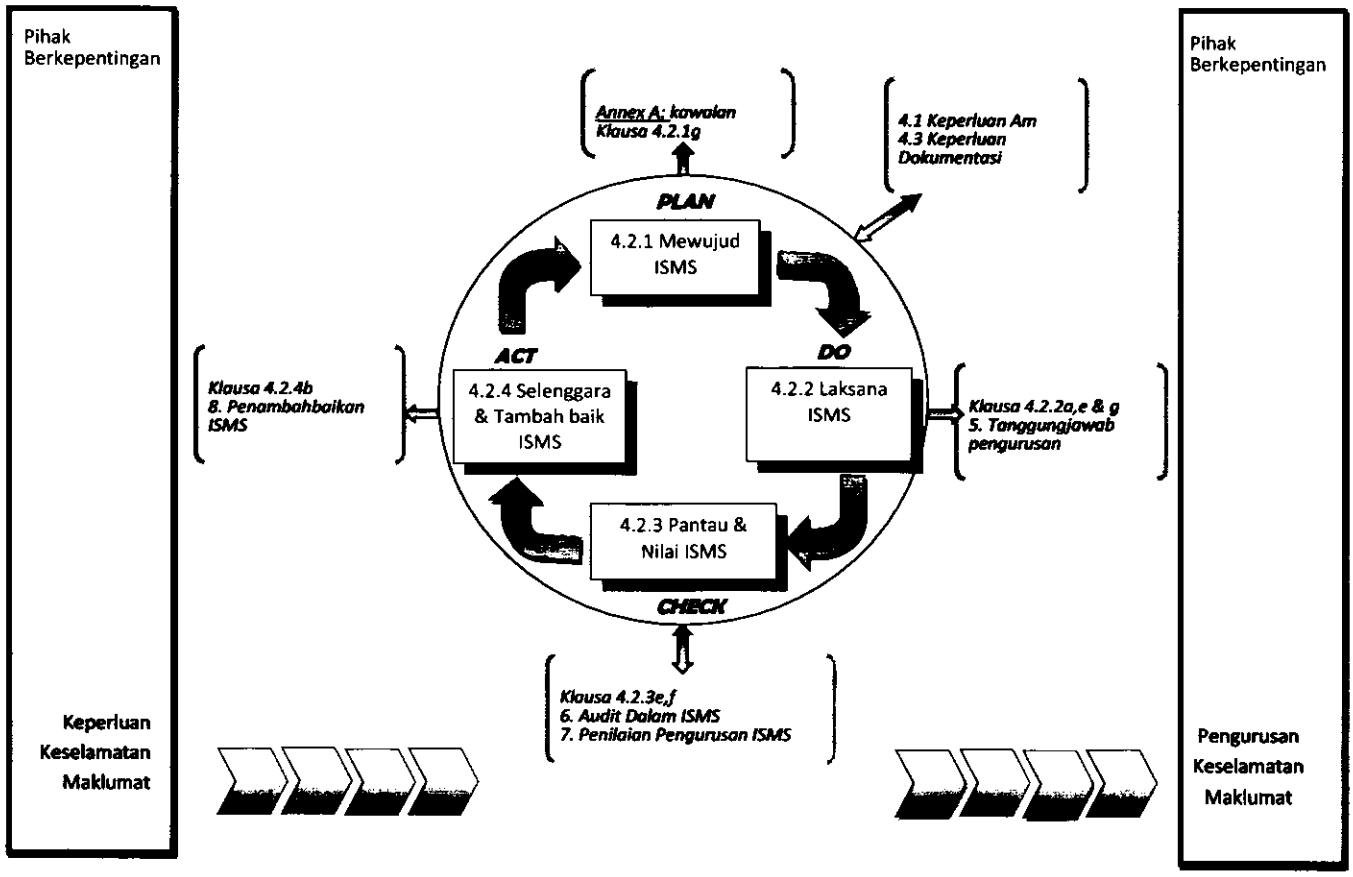
Rajah 3 menunjukkan empat (4) fasa utama dalam proses ISMS merangkumi *Plan* (mewujud ISMS), *Do* (melaksana ISMS), *Check* (memantau dan menilai ISMS) dan *Act* (menyelenggara dan menambah baik ISMS).

Rajah 3: Fasa PDCA dan Proses ISMS

***Plan* (Mewujud ISMS)**	**Mewujud dasar ISMS, objektif, proses dan prosedur yang relevan untuk mengurus risiko bagi menjamin keselamatan maklumat.**
***Do* (Melaksana ISMS)**	Melaksana dasar ISMS, objektif, proses dan prosedur
***Check* (Memantau dan menilai ISMS)**	**Memantau dan menilai ISMS. Jika perlu ukur prestasi proses dan kawalan ISMS. Lapor hasilnya kepada pihak pengurusan untuk pertimbangan.**
***Act* (Menyelenggara dan menambah baik ISMS)**	Mengambil tindakan pembetulan/pencegahan berdasarkan penemuan Audit Dalam ISMS dan menyemak semula pelaksanaan ISMS oleh pihak pengurusan bagi menambah baik ISMS secara berterusan.

Proses ISMS adalah secara berterusan dan saling berkaitan. Rajah 4 menunjukkan pelaksanaan ISMS serta hubung kait antara proses yang terlibat dalam setiap fasa dalam model PDCA.

Rajah 4: Fasa PDCA dalam Proses ISMS



5.

Panduan pelaksanaan ISMS merangkumi keperluan-keperluan pengurusan sistem keselamatan maklumat dengan merujuk kepada seksyen 4 hingga 8 dalam MS ISO/IEC 27001:2007. Penerangan di bawah bab ini menumpukan kepada keperluan ISMS seperti *roadmap*, fasa pelaksanaan ISMS dan ringkasan setiap seksyen serta penjelasan satu persatu keperluan standard yang meliputi pengurusan sistem keselamatan maklumat, tanggungjawab pengurusan, audit dalam ISMS, kajian semula ISMS dan penambahbaikan berterusan.

MS ISO/IEC 27001:2007 adalah standard yang menetapkan satu set keperluan bagi memenuhi keperluan pengurusan sistem keselamatan maklumat. Istilah maklumat, merangkumi koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif agensi contohnya sistem dokumentasi, prosedur operasi, rekod-rekod agensi, profil pelanggan, pangkalan data dan fail data, maklumat arkib dan lain-lain.

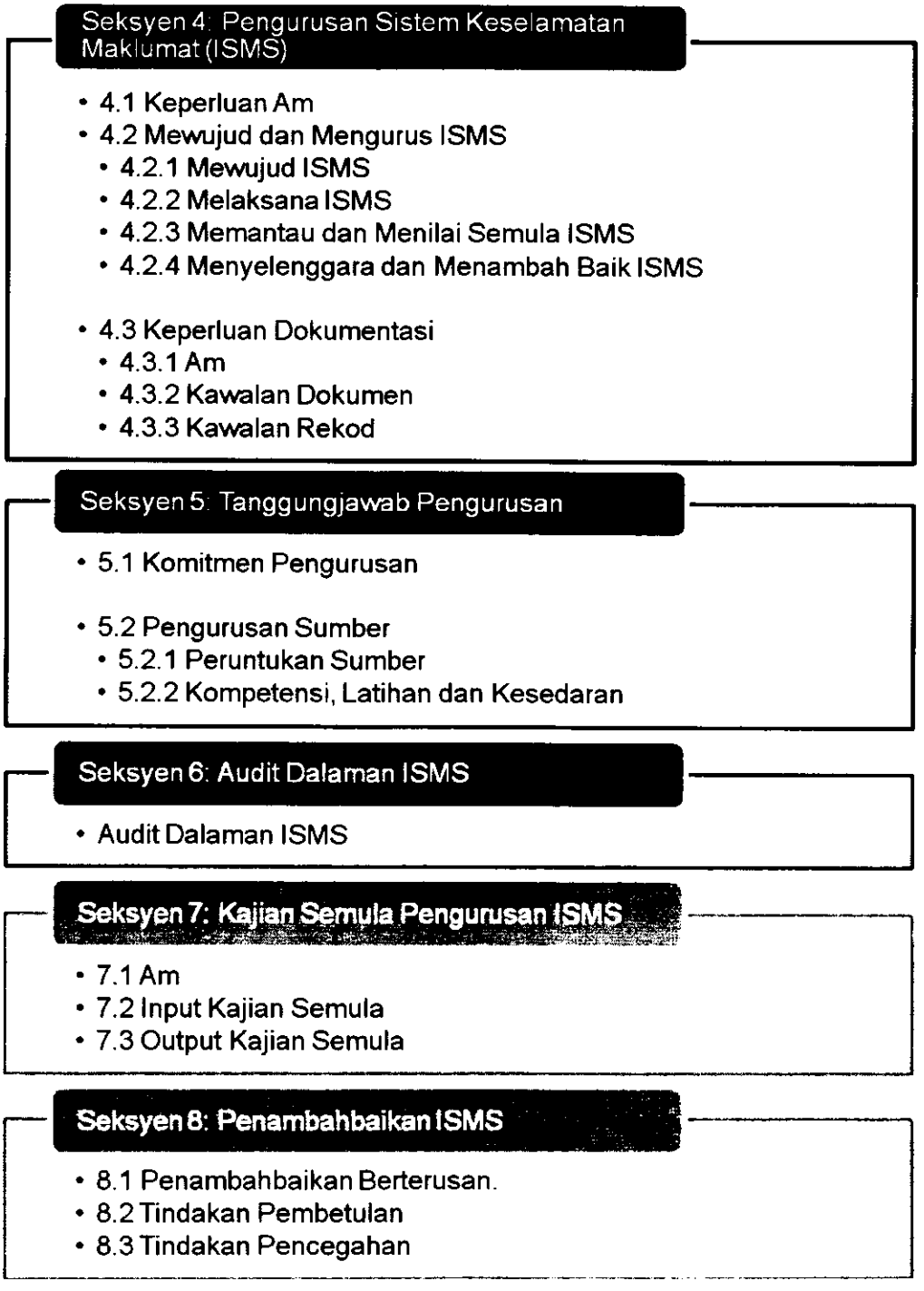
Semua keperluan dinyatakan dalam seksyen 4 hingga seksyen 8 dalam standard tersebut dengan menggunakan perkataan *shall* dan ini menunjukkan semua keperluan proses dalam MS ISO/IEC 27001:2007 adalah wajib. Rajah 5 menerangkan berkenaan struktur standard MS ISO/IEC 27001:2007 mengikut seksyen beserta penerangan ringkas bagi setiap seksyen.

Rajah 5: Struktur Standard MS ISO/IEC 27001:2007

LAPAN (8) SEKSYEN DALAM STANDARD MS ISO/IEC 27001:2007	
Seksyen 1	**Menerangkan bahawa standard MS ISO/IEC 27001:2007 merupakan keperluan generik dan sebarang pengecualian pemakaian seksyen 4 sehingga 8 tidak diterima. Standard ini berupaya memenuhi keperluan pelbagai jenis, saiz dan perkhidmatan.**
Seksyen 2	Menetapkan bahawa dokumen yang perlu dirujuk dalam melaksanakan Pengurusan Sistem Keselamatan Maklumat adalah dokumen ISO/IEC 17799:2005
Seksyen 3	**Menjelaskan definisi yang diguna pakai dalam standard MS ISO/IEC 27001:2007**
Seksyen 4	Menerangkan keperluan untuk merancang pembentukan ISMS.
Seksyen 5	**Menerangkan tanggungjawab dan peranan pengurusan dalam melaksana, memantau dan menilai ISMS.**
Seksyen 6	Menerangkan keperluan untuk melaksanakan audit bagi proses dan kawalan ISMS.
Seksyen 7	**Menerangkan keperluan menilai semula ISMS berdasarkan hasil laporan pengauditan dan pemantauan.**
Seksyen 8	Menerangkan keperluan untuk mengambil tindakan pembetulan dan pencegahan bagi menambah baik pengurusan sistem keselamatan maklumat secara berterusan.

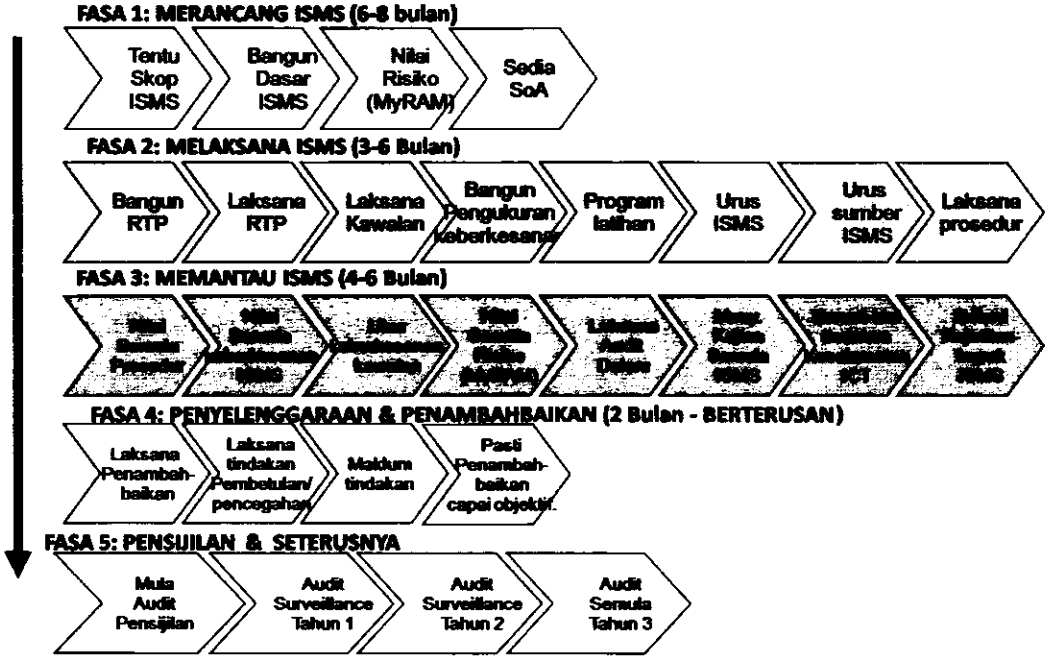
Agensi-agensi Kerajaan yang melaksanakan pensijilan MS ISO/IEC 27001:2007 hendaklah mematuhi semua keperluan standard yang dijelaskan di dalam seksyen 4 hingga seksyen 8 seperti dalam Rajah 6.

Rajah 6: Keperluan Standard dalam seksyen 4 hingga seksyen 8



Ringkasan keperluan bagi seksyen 4 hingga seksyen 8 mengikut cadangan penjadualan dalam tempoh masa tiga (3) tahun digariskan melalui roadmap adalah seperti di Rajah 7

Rajah 7: *Roadmap* ISMS Dalam Sektor Awam



Bagi memastikan kejayaan pelaksanaan dan pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat, lima (5) fasa dicadangkan mengandungi langkah-langkah pelaksanaan ISMS dan perlu diambil tindakan oleh agensi-agensi Kerajaan.

Fasa 1: Merancang ISMS

Jangka masa yang dicadangkan adalah enam (6) hingga lapan (8) bulan. Aktiviti yang perlu dilaksanakan dalam fasa ini adalah menentukan skop ISMS, membangunkan dasar ISMS, melaksanakan penilaian risiko dengan menggunakan pendekatan MyRAM dan menyediakan penyataan pemakaian *(SoA).*

Fasa 2: Melaksana ISMS

Jangka masa yang dicadangkan bagi Fasa 2 pula adalah antara tiga (3) hingga enam (6) bulan. Aktiviti yang perlu dilaksanakan adalah membangunkan pelan penguraian

risiko (RTP) berdasarkan *output* daripada penilaian risiko yang telah dilaksanakan dalam Fasa 1 dan melaksanakan pelan tersebut. Selain itu, agensi juga perlu melaksanakan kawalan ke atas kawalan-kawalan yang telah ditetapkan pada SoA di Fasa 1. Seterusnya membangunkan prosedur untuk mengukur keberkesanan, merancang dan melaksana program latihan kepada semua warga di agensi, menguruskan ISMS, menguruskan semua sumber yang terlibat dengan ISMS serta melaksanakan prosedur yang telah ditetapkan.

Fasa 3: Memantau ISMS

Bagi Fasa 3, jangka masa yang dicadangkan adalah empat (4) hingga enam (6) bulan yang melibatkan beberapa aktiviti iaitu menilai semula prosedur, menilai semula keberkesanan ISMS, mengukur keberkesanan kawalan, menilai semula risiko (MyRAM), melaksanakan audit dalam, mengadakan mesyuarat dengan pengurusan bagi mengkaji semula pelaksanaan ISMS, mengemas kini tindakan keselamatan ICT dan merekod kejadian/ impak ISMS ke atas agensi.

Fasa 4: Penyelenggaraan dan Penambahbaikan

Bagi Fasa 4, pelaksanaannya dicadangkan dalam masa dua (2) bulan dan dilakukan secara berterusan. Aktiviti yang perlu dilaksanakan dalam fasa ini adalah melaksana penambahbaikan, melaksana tindakan pencegahan dan pembetulan, memaklumkan tindakan yang diambil kepada pengurusan dan memastikan penambahbaikan yang dilakukan menepati objektif yang ditetapkan.

Fasa 5: Pensijilan dan Seterusnya

Agensi perlu menjalani audit permulaan pensijilan yang melibatkan Audit Pensijilan Peringkat I dan Audit Pensijilan Peringkat II untuk mendapatkan pensijilan ISMS. Tempoh sah laku pensijilan adalah tiga (3) tahun. Sekiranya agensi berjaya mendapat pensijilan ISMS dalam Audit Pensijilan Peringkat II, agensi perlu menjalani Audit Pemantauan (*Surveillance*) Tahun 1 dan Audit Pemantauan (*Surveillance)* Tahun 2. Seterusnya, agensi perlu menjalani audit penilaian semula bagi tahun ketiga untuk memperbaharui pensijilan ISMS tersebut.

Seksyen 4 menjelaskan keperluan agensi untuk mewujud, melaksana, memantau, menyemak, menyelenggara dan menambah baik suatu pengurusan sistem keselamatan maklumat. Agensi juga dikehendaki menyediakan prosedur untuk mengawal dan merekod semua dokumen ISMS yang telah ditetapkan.

5.2.1 Keperluan Am

Agensi perlu melaksanakan keperluan am ISMS berdasarkan seksyen 4.1 dokumen MS ISO/IEC 27001:2007 melibatkan tujuh (7) keperluan seperti dalam Rajah 8.

Rajah 8: Tujuh Keperluan Am ISMS
merujuk kepada Seksyen 4.1 MS ISO/IEC 27001:2007

✓	**Mewujud**
✓	Melaksana
✓	**Mengoperasi**
✓	Memantau
✓	**Menyemak**
✓	Menyelenggara
✓	**Menambah baik**

5.2.2 Mewujud dan Mengurus ISMS

a) Mewujud ISMS (rujuk kepada Seksyen 4.2.1)

i. **Menetapkan skop ISMS**

Agensi hendaklah memilih skop ISMS yang bersesuaian dengan fungsi-fungsi utama agensi. Agensi boleh menetapkan skop ISMS merangkumi keseluruhan agensi atau bahagian di agensi atau sistem aplikasi dan sempadan skop hendaklah juga ditakrifkan dengan sempurna.

Skop perlu mengambil kira pihak ketiga yang terlibat seperti bahagian-bahagian lain dalam agensi (jika bukan dalam skop ISMS), agensi lain, pembekal dan entiti lain. Keterangan setiap pengecualian dari skop ISMS harus didokumentasikan.

ii. **Menetapkan dasar ISMS**

Dasar ISMS hendaklah dibangunkan dengan menetapkan peraturan-peraturan yang mesti dipatuhi dalam menggunakan aset ICT. Dasar tersebut hendaklah menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Kerajaan.

Agensi boleh merujuk kepada tatacara pembangunan Dasar Keselamatan ICT (DKICT) seperti di Rajah 9.

Perkara-perkara yang perlu diambil kira semasa penggubalan DKICT hendaklah merangkumi bidang-bidang keselamatan berikut:

- **Bidang 01: Pembangunan dan Penyelanggaraan Dasar**

  Bidang ini menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan agensi dan perundangan yang berkaitan.