



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 Kesyinambungan 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 inisiatif 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.

KANDUNGAN

PERKARA	MUKA SURAT
1. PENGENALAN	
1.1. Tujuan	1
1.2. Skop Panduan	1
1.3. Definisi	2
1.4. Singkatan	5
1.5. Dokumen Rujukan	5
2. KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)	
2.1. Pernyataan Dasar Keselamatan ICT	6
3. PENGURUSAN SISTEM KESELAMATAN MAKLUMAT	
3.1. Konsep Pengurusan Kualiti dan Keselamatan Maklumat	8
3.2. Prinsip-prinsip Pengurusan Sistem Keselamatan Maklumat	9
3.3. Keselamatan Maklumat Yang Berkesan	10
3.4. Proses Berterusan	10
4. MODEL PDCA DALAM MS ISO/IEC 27001:2007	
4.1. Fasa PDCA dalam proses pelaksanaan MS ISO/IEC 27001:2007	11
5. PANDUAN PELAKSANAAN MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM	
5.1. Keperluan ISMS	13
5.2. Penjelasan Standard di Bawah Seksyen 4: Pengurusan Sistem Keselamatan Maklumat	18
5.2.1. Keperluan Am	18



PERKARA	MUKA SURAT
5.2.2. Mewujud dan Mengurus ISMS	19
5.2.3. Keperluan Dokumentasi	36
5.3. Penjelasan Standard di Bawah Seksyen 5: Tanggungjawab Pengurusan	38
5.3.1. Komitmen Pengurusan	38
5.3.2. Pengurusan Sumber	39
5.4. Penjelasan Standard di Bawah Seksyen 6: Audit Dalam ISMS	40
5.5. Penjelasan Standard di Bawah Seksyen 7: Kajian Semula ISMS	41
5.6. Penjelasan Standard di Bawah Seksyen 8: Penambahbaikan Berterusan	42
6. PENSIJILAN	
6.1. Persediaan Pensijilan	43
6.1.1. Penilaian Pematuhan	43
6.1.2. Bukti Auditan	44
6.1.3. Pengecualian dan Penerimaan Risiko	44
6.1.4. Dokumentasi Pengurusan Sistem	45
6.2. Metodologi Audit	45
6.2.1. Audit Peringkat I	45
6.2.2. Audit Peringkat II	46
6.2.3. Audit Pemantauan	46
6.2.4. Audit Penilaian Semula	46

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.

1.1 TUJUAN

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.

1.2 SKOP PANDUAN

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.

1.3 DEFINISI

ISTILAH	MAKSUD
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.

ISTILAH	MAKSUD
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 mewujudkan, melaksana, memantau, menyemak, menyelenggara dan

ISTILAH	MAKSUD
Maklumat	menambah baik keselamatan maklumat.
Pelan Penguraian Risiko <i>(Risk Treatment Plan-RTP)</i>	Bermaksud strategi untuk menangani risiko keselamatan ICT.
Proses	Bermaksud proses yang mengguna pakai model <i>Plan-Do-Check-Act</i> (PDCA). Setiap proses hendaklah dirancang (<i>Plan</i>); dilaksana dan diselenggara (<i>Do</i>); dipantau, dinilai dan dikaji semula (<i>Check</i>) dan ditambah baik (<i>Act</i>)
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 <i>(Statement of Applicability- SoA)</i>	Bermaksud menyenaraikan justifikasi pemilihan kawalan, <i>Annex A</i> 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.

1.4 SINGKATAN

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

1.5 DOKUMEN RUJUKAN

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 ICT

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

2.1 PENYATAAN DASAR KESELAMATAN 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

CIRI – CIRI UTAMA KESELAMATAN MAKLUMAT		KERAHSIAAN Maklumat <u>tidak boleh didedahkan</u> sewenang-wenangnya atau dibiarkan <u>diakses tanpa kebenaran</u>
		INTEGRITI Data dan maklumat hendaklah <u>tepat, lengkap dan kemaskini</u> . Ia hanya boleh diubah dengan cara yang dibenarkan
		TIDAK BOLEH DISANGKAL Punca data dan maklumat hendaklah dari <u>punca yang sah</u> dan tidak boleh disangkal
		KESAHIHAN Data dan maklumat hendaklah <u>dijamin kesahihan</u>
		KEBOLEHSEDIAAN Data dan maklumat hendaklah <u>boleh diakses pada bila-bila masa</u>

3.

PENGURUSAN SISTEM KESELAMATAN MAKLUMAT

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

3.1 KONSEP PENGURUSAN KUALITI DAN KESELAMATAN MAKLUMAT

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.

3.2 PRINSIP-PRINSIP PENGURUSAN SISTEM KESELAMATAN MAKLUMAT

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.

3.3 KESELAMATAN MAKLUMAT YANG BERKESAN

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.

3.4 PROSES BERTERUSAN

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) Meningkatkan indeks pencapaian Kerajaan di peringkat antarabangsa.

4.

MODEL PDCA DALAM MS ISO/IEC 27001:2007

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.

4.1 FASA PDCA DALAM PROSES PELAKSANAAN MS ISO/IEC 27001:2007

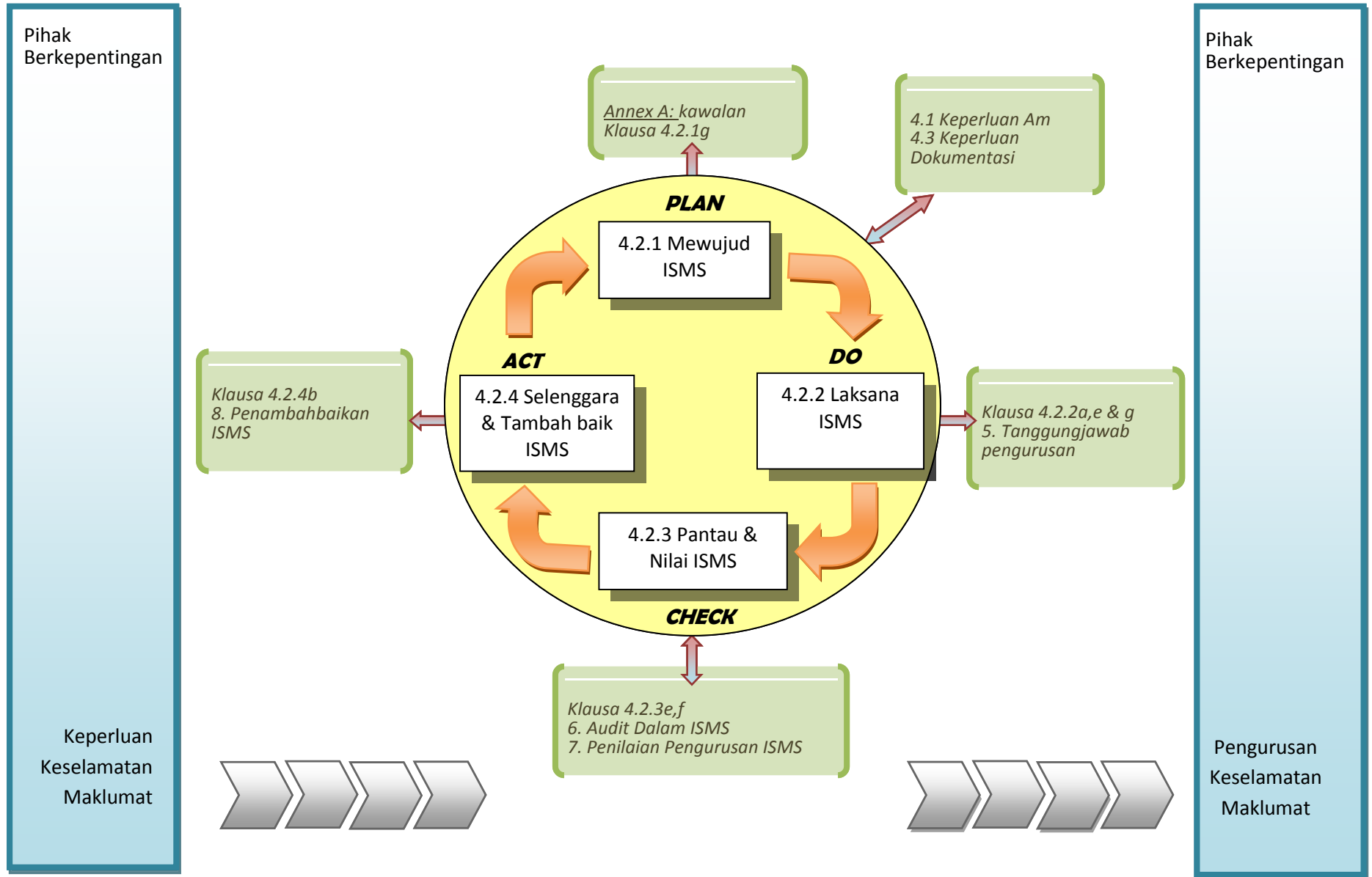
Rajah 3 menunjukkan empat (4) fasa utama dalam proses ISMS merangkumi *Plan* (mewujud ISMS), *Do* (melaksana ISMS), *Check* (memantau dan menilai ISMS) dan *Act* (menyelenggara dan menambah baik ISMS).

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. Laporan 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 MS ISO/IEC 27001:2007 DALAM SEKTOR AWAM

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.

5.1 KEPERLUAN ISMS

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.

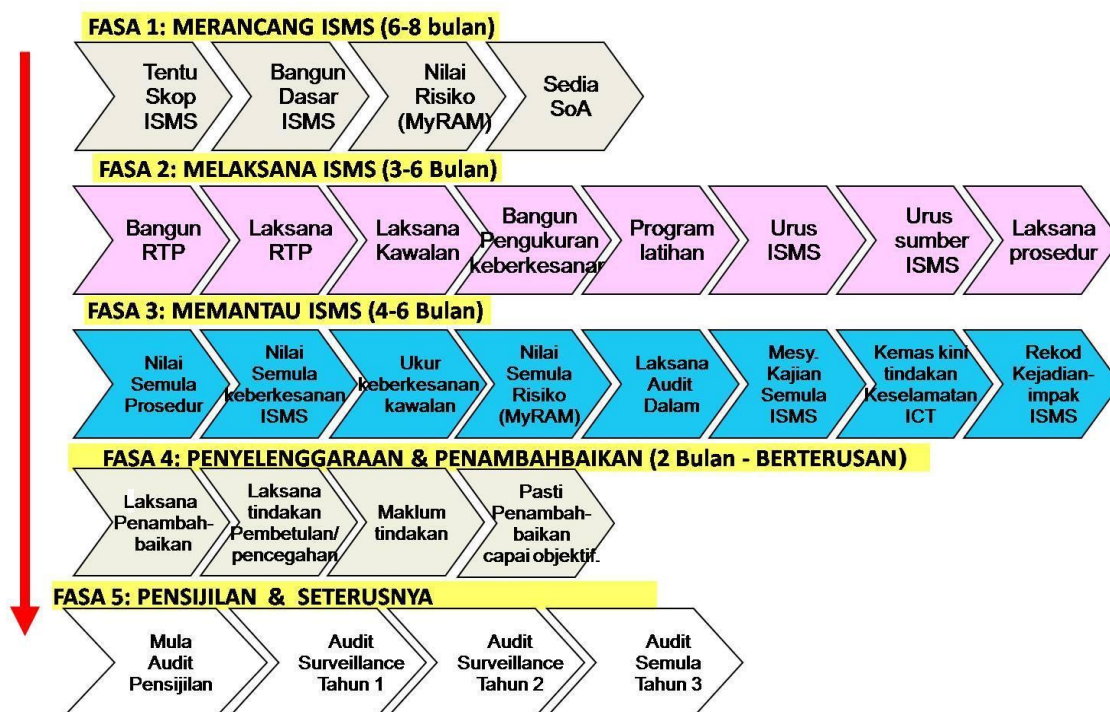
Agensi-agensi Kerajaan yang melaksanakan pensijilan MS ISO/IEC 27001:2007 hendaklah mematuhi semua keperluan standard yang dijelaskan di dalam seksyen 4 hingga seksyen 8 seperti dalam Rajah 6.

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 pernyataan 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.

5.2 PENJELASAN STANDARD DI BAWAH SEKSYEN 4: PENGURUSAN SISTEM KESELAMATAN MAKLUMAT

Seksyen 4 menjelaskan keperluan agensi untuk mewujudkan, 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 Penyelenggaraan Dasar**

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



- **Bidang 02: Organisasi Keselamatan**

Bidang ini menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT serta menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, pakar runding dan lain-lain).

- **Bidang 03: Pengurusan Aset**

Bidang ini menerangkan bagaimana aset ICT diuruskan dan disokong serta memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

- **Bidang 04: Keselamatan Sumber Manusia**

Bidang ini menerangkan kawalan untuk memastikan semua sumber manusia yang terlibat (termasuk pegawai dan kakitangan agensi, pembekal, pakar runding dan pihak-pihak yang berkepentingan) memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT.

Semua warga agensi hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

- **Bidang 05: Keselamatan Fizikal dan Persekitaran**

Bidang ini menerangkan kawalan bagi melindungi aset ICT daripada sebarang bentuk pencerobohan, ancaman, kecurian, kehilangan, kesilapan, kecuiaan, kemalangan, gangguan, kerosakan dan bencana alam serta akses yang tidak dibenarkan

- **Bidang 06: Pengurusan Operasi dan Komunikasi**

Bidang ini merangkumi beberapa pecahan bidang yang menerangkan kawalan bagi memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan. Selain itu, memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

Bidang ini juga menerangkan berkenaan kawalan bagi meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem serta melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya agar boleh diakses pada bila-bila masa.

Pengurusan operasi dan komunikasi juga mencakupi aspek perlindungan maklumat dalam rangkaian dan infrastruktur serta aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan. Memastikan keselamatan pertukaran maklumat dan perisian antara agensi dan agensi luar terjamin serta mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang selain memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

- **Bidang 07: Kawalan Capaian**

Bidang ini menerangkan kawalan capaian ke atas maklumat dan aset ICT bertujuan menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian, sistem pengurusan, dan maklumat dalam sistem

aplikasi serta memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

- **Bidang 08: Perolehan, Pembangunan dan Penyelenggaraan Sistem**

Bidang ini menerangkan kawalan bagi memastikan sistem yang dibangunkan sendiri atau oleh pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian seperti dapat melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi, memastikan fail sistem dikawal, dikendalikan dengan baik dan selamat. Juga kawalan bagaimana untuk menjaga dan menjamin keselamatan sistem maklumat dan aplikasi serta memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian.

- **Bidang 09: Pengurusan Pengendalian Insiden Keselamatan**

Bidang ini bertujuan untuk memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT. Selain itu, dapat memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

- **Bidang 10: Pengurusan Kesyinambungan Perkhidmatan**

Bidang ini menerangkan kawalan bagi menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

- **Bidang 11: Pematuhan**

Bidang ini menerangkan kawalan bagi meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKICT.

Panduan Untuk Membangunkan DASAR KESELAMATAN ICT JABATAN

Dokumen Dasar Keselamatan ICT (DKICT)

LANGKAH-LANGKAH UNTUK MEMBANGUNKAN DKICT

1. Kenal pasti aktiviti dan aset ICT;
2. Kenal pasti ancaman-ancaman bagi setiap aktiviti dan aset ICT;
3. Merangka dasar bagi meminimumkan kesan ancaman;
4. Menyenarai langkah-langkah keselamatan bagi menyokong dasar; dan
5. Menyediakan garis panduan dan prosedur pelaksanaan.

ANTARA ASET ICT YANG PERLU DILINDUNGI

1. Peralatan dan perisian komputer;
2. Peralatan komunikasi;
3. Premis peralatan komputer dan komunikasi termasuk makmal komputer;
4. Bekalan elektrik, air, kawalan persekitaran dan kemudahan yang berasakan ICT;
5. Media pembekalan dan penyimpanan data;
6. Dokumentasi dan program sistem/ aplikasi komputer; dan
7. Maklumat-maklumat sensitif.

RANGKA DASAR KESELAMATAN ICT KERAJAAN

Dirumus bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah menyeluruh untuk melindungi aset ICT kerajaan. Perlindungan keselamatan ini perlu bersesuaian dengan nilai atau sensitiviti aset yang dimaksudkan. Ia juga perlu seimbang dengan kesan yang mungkin timbul akibat kegagalan perlindungan yang sesuai.

Perkara-perkara umum yang perlu dinyatakan dalam dokumen dasar adalah seperti berikut:

1. Pernyataan dasar keselamatan ICT agensi;
2. Penjelasan kepentingan keselamatan ICT;
3. Definisi keselamatan ICT termasuk skop aset yang dilindungi;
4. Objektif memastikan perkhidmatan ICT organisasi berterusan dan mengurangkan kesan akibat sesuatu insiden;
5. Prinsip-prinsip keselamatan yang disandarkan;
6. Tugas dan tanggungjawab setiap individu;
7. Keperluan program kesedaran dan latihan keselamatan ICT; dan
8. Standard dan prosedur (SOP) keselamatan ICT.

PEGAWAI KESELAMATAN ICT (ICTSO)

Setiap agensi perlu melantik seorang pegawai sama ada pegawai sistem maklumat atau pegawai teknikal yang bertanggungjawab penuh bagi melaksanakan program-program keselamatan ICT termasuklah menentukan semua pegawai dan staf jabatan memahami dan mematuhi dasar keselamatan ICT kerajaan dan jabatan.

JAWATANKUASA

Satu jawatankuasa atau pasukan kerja perlulah ditubuhkan bagi membangunkan dasar keselamatan ICT jabatan yang akan dipengerusikan oleh CIO dan ahli terdiri dari pelbagai bahagian/unit/jabatan yang berkepentingan dalam ICT. Dokumen dasar keselamatan ICT jabatan yang disediakan mestilah diperakukan oleh CIO dan Ketua Jabatan.



DRAF DASAR

Mengandungi misi dan objektif dasar dan hendaklah selaras dengan misi dan objektif jabatan. Dokumen berkenaan mestilah jelas, ringkas dan mudah difahami. Rujukan lain seperti MyMIS, MS ISO/IEC 27001:2006, dan pengalaman ahli boleh dibuat dalam membantu memudahkan penyediaan dasar.

REVIU

Draf dokumen diedarkan kepada ahli jawatankuasa bagi mendapatkan maklum balas dan kemudiannya mencadangkan dan mengambil tindakan penambahbaikan. Ini diikuti dengan persetujuan daripada ahli sebelum draf dokumen berkenaan dibentangkan kepada CIO.

KELULUSAN CIO

Memberi taklimat dan membentangkan draf dasar keselamatan ICT jabatan kepada CIO dan Ketua Jabatan yang dihadiri oleh semua Ketua Jabatan bagi mendapatkan perakuan mesyuarat.

PELAKSANAAN

Dasar keselamatan ICT yang dipersetujui akan dimaklumkan kepada semua warga jabatan agar mematuhi penentuan dasar dapat dilaksanakan.

PEMBUDAYAAN

Merancang dan melaksanakan program-program pembudayaan keselamatan ICT khususnya latihan dalaman bagi meningkatkan pengetahuan personel berkaitan keselamatan ICT.

KUATKUASA

ICTSO menguatkuasakan pematuhan dasar keselamatan ICT jabatan dari semasa ke semasa.

KAJIAN SEMULA DOKUMEN DASAR

Kajian atau semakan semula dokumen dasar bagi memastikan dokumen dasar dikemas kini yang melibatkan perubahan teknologi, perundangan dan lain-lain perkara berkaitan.

iii. Menetapkan pendekatan untuk menilai risiko aset ICT

Agensi perlu mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan (*vulnerability*) yang semakin meningkat hari ini. Justeru itu, agensi perlu menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT agensi.

Semua agensi Kerajaan hendaklah melaksanakan penilaian risiko aset ICT berasaskan metodologi Penilaian Risiko Terperinci (*Malaysian Public Sector ICT Risk Assessment Methodology, MyRAM*) berpandukan kepada Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

Sepuluh (10) langkah utama dalam MyRAM adalah seperti berikut:

- 1 Menubuhkan Jawatankuasa Penilaian Risiko
- 2 Menetapkan sempadan
- 3 Mengenal pasti Aset
- 4 Menilai Aset
- 5 Menilai Ancaman
- 6 Menilai Kelemahan
- 7 Mengenal pasti Kawalan
- 8 Menganalisa Impak
- 9 Menganalisa Kebarangkalian
- 10 Mengukur Risiko

Agensi hendaklah melaksanakan penilaian risiko berasaskan 10 langkah utama seperti di atas. Setiap langkah MyRAM saling bergantung dengan menghasilkan satu atau lebih dokumen yang merupakan input kepada satu atau lebih langkah utama MyRAM.

Langkah-langkah ini berperanan membantu dalam menganalisis nilai aset dari aspek kritikaliti aset berkenaan dalam menyokong sistem penyampaian perkhidmatan. MyRAM memerlukan komitmen dan pemerhatian yang berterusan untuk memastikan output yang dihasilkan adalah tepat dan lengkap.

iv. **Mendapat persetujuan pengurusan untuk melaksana ISMS**

Pihak pengurusan agensi perlu memberi persetujuan berhubung semua tindakan yang dirancang untuk menjayakan pelaksanaan pengurusan sistem keselamatan maklumat sebagai tanda sokongan dan komitmen ke atas usaha ini sebelum melangkah ke fasa *Do*.

v. **Menyedia Penyataan Pemakaian (*Statement of Applicability, SoA*)**

Agensi yang berhasrat untuk mendapat pensijilan MS ISO/IEC 27001:2007 mesti menyediakan SoA yang menjelaskan justifikasi dan rujukan kawalan dalam melindungi keselamatan aset ICT.

Pilihan kawalan dalam SoA perlu dihubungkan dengan hasil penilaian risiko dan proses penguraian risiko (RTP) bagi menyokong alasan memilih kawalan-kawalan yang terdapat dalam *Annex A (normative)*, MS ISO/IEC 27001:2007.

Keperluan bagi mewujudkan ISMS merujuk kepada Seksyen 4.2.1 MS ISO/IEC 27001:2007 disenaraikan seperti dalam Rajah 10.

Rajah 10: Keperluan untuk mewujudkan ISMS merujuk kepada Seksyen 4.2.1

- ✓ Menetapkan skop ISMS
- ✓ Menetapkan dasar ISMS
- ✓ Menetapkan pendekatan untuk menilai risiko aset ICT
- ✓ Mengenal pasti risiko keselamatan aset ICT dalam skop ISMS
- ✓ Menganalisis dan menilai risiko keselamatan aset ICT

-
- ✓ Menentu dan menilai pilihan dan tindakan penguraian risiko (*Risk Treatment Plan, RTP*)
 - ✓ Memilih kawalan untuk menangani risiko aset ICT yang telah dikenal pasti
 - ✓ Mendapat persetujuan pengurusan berhubung dengan semua sisa risiko (*residual risk*)
 - ✓ Mendapat persetujuan pengurusan untuk melaksanakan ISMS
 - ✓ Menyediakan Penyataan Pemakaian (*Statement of Applicability, SoA*) yang mendaftar kawalan sebagaimana dinyatakan dalam *Annex A, MS ISO/IEC 27001:2007*
-

b) Melaksana ISMS (rujuk kepada Seksyen 4.2.2)

i. Membangunkan Pelan Penguraian Risiko

Output daripada proses penilaian risiko setiap aset ICT akan diguna pakai untuk membangunkan Pelan Penguraian Risiko bagi mengurus risiko aset ICT. Pelan ini bertujuan untuk menambah baik tahap keselamatan yang sedia ada dan mencadangkan strategi perlindungan yang perlu dilaksanakan bagi menangani tahap risiko keselamatan ICT. Tindakan mengurai risiko termasuk:

- Menerima risiko yang akan terjadi selagi ia memenuhi kriteria yang ditetapkan oleh pengurusan;
- Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
- Memindahkan risiko ke entiti lain seperti pembekal, pakar runding dan pihak lain yang berkepentingan; dan
- Mengelak atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat menghalang berlakunya risiko.

Jika risiko diterima, maka tidak ada tindakan yang perlu dilakukan untuk melindungi aset tersebut. Sementara risiko yang perlu dikurangkan ke tahap yang boleh diterima, hendaklah melalui penggunaan kawalan yang sesuai untuk memastikan perkhidmatan tidak terganggu. Semua kawalan yang sesuai ditakrifkan di Annex A (*normative*) dalam MS ISO/IEC 27001:2007 yang meringkaskan kawalan yang sesuai untuk menangani risiko. Manakala penerangan perincian kawalan tersebut dinyatakan dalam MS ISO/IEC 17799:2006 atau ISO/IEC 27002:2005.

ii. **Melaksanakan Pelan Penguraian Risiko**

Pelan Penguraian Risiko menetapkan strategi untuk menangani risiko keselamatan ICT perlu mendapat persetujuan pengurusan sebelum dilaksanakan. Antara program yang boleh dilaksanakan adalah seperti berikut:

- Kesedaran dan latihan keperluan Pengurusan Sistem Keselamatan Maklumat;
- Melaksanakan strategi perlindungan keselamatan;
- Memantau semua aktiviti pengurusan keselamatan; dan
- Memantau pematuhan dasar dan peraturan keselamatan ICT.

iii. **Melaksanakan kawalan keselamatan ICT**

Agensi hendaklah melaksanakan kawalan yang telah dipilih bagi mencapai objektif kawalan keselamatan ICT. Agensi harus mempunyai prosedur untuk melaksanakan kawalan yang dipilih serta menggariskan tindakan, peranan dan tanggungjawab selaras dengan ketetapan dalam Pelan Penguraian Risiko.

iv. **Mengukur keberkesanan kawalan keselamatan ICT**

Agensi perlu menentukan kaedah untuk mengukur dan menilai keberkesanan kawalan. Pelaksanaan kawalan hendaklah dapat melindungi keselamatan aset maklumat

tersebut. Maka agensi perlu menetapkan bagaimana untuk mengukur keberkesanan kawalan yang telah dilaksanakan bagi memastikan kawalan tersebut mencapai objektif perlindungan maklumat.

Bagi tujuan pensijilan, kaedah yang telah dikenal pasti untuk mengukur keberkesanan kawalan perlu didokumentasikan sebagai keterangan tentang bagaimana agensi menilai keberkesanan kawalan keselamatan ICT.

v. **Melaksana program pendidikan keselamatan ICT**

Agensi harus melaksanakan program kesedaran dan latihan yang bertujuan bagi memastikan semua personel dalam skop Pengurusan Sistem Keselamatan Maklumat mempunyai kemahiran dan kepakaran untuk menjayakan peranan dan tanggungjawab masing-masing.

Program pendidikan keselamatan ICT yang dikendalikan seharusnya dapat meningkatkan kompetensi yang diperlukan, memberikan latihan untuk memenuhi keperluan Pengurusan Sistem Keselamatan Maklumat, menilai keberkesanan latihan serta mendokumentasikan kemahiran dan kelayakan yang dicapai. Ini bertujuan untuk merancang program pendidikan keselamatan yang dapat memenuhi keperluan dan menjayakan Pengurusan Sistem Keselamatan Maklumat dalam agensi.

vi. **Menguruskan operasi ISMS**

Agensi harus mengendalikan ISMS sesuai dengan kawalan, dasar dan prosedur yang telah dikenal pasti. Operasi harian ISMS akan memberikan maklumat yang diperlukan untuk fasa *Check* bagi menilai sama ada tatacara keselamatan maklumat yang dilaksanakan dapat mencapai fungsi yang dimaksudkan. Bagi menjayakan aktiviti penilaian ini, semua dokumen dan rekod yang diperlukan mesti dikumpulkan selama operasi harian ISMS.

vii. **Mengurus semua sumber ISMS**

Agensi perlu mengenal pasti dan menyediakan sumber yang diperlukan untuk mewujudkan, melaksana, memantau, menyemak, menyelenggara dan menambah baik suatu pengurusan sistem keselamatan maklumat.

Pengurusan bertanggungjawab untuk menyediakan keperluan sumber kewangan, kawalan perlindungan dan personel yang mencukupi bagi menjayakan ISMS.

viii. **Melaksana Prosedur dan Kawalan ISMS bagi Menangani Insiden Keselamatan Maklumat**

Agensi Kerajaan perlu menyediakan prosedur untuk mengurus insiden keselamatan maklumat. Antara perkara yang perlu diambil kira adalah:

- Mengenal pasti insiden keselamatan maklumat;
- Melaporkan sebarang insiden keselamatan maklumat;
- Menilai kejadian insiden keselamatan maklumat;
- Mengambil tindakan terhadap insiden dengan cara yang berkesan; dan
- Menyekat kerosakan akibat insiden keselamatan maklumat.

Agensi perlu merekodkan kejadian insiden keselamatan maklumat. Ini penting untuk menilai sama ada hasil penemuan penilaian risiko dan Pelan Penguraian Risiko dapat mencapai matlamat strategik perlindungan dan menjayakan operasi harian ISMS.

Keperluan bagi melaksanakan ISMS adalah merujuk kepada Seksyen 4.2.2 MS ISO/IEC 27001:2007 sebagaimana disenaraikan dalam Rajah 11.

Rajah 11: Keperluan untuk melaksana ISMS merujuk kepada Seksyen 4.2.2

- ✓ Membangunkan Pelan Penguraian Risiko
- ✓ Melaksana Pelan Penguraian Risiko
- ✓ Melaksanakan kawalan keselamatan ICT
- ✓ Mengukur keberkesanan kawalan keselamatan ICT
- ✓ Melaksana program pendidikan keselamatan ICT
- ✓ Menguruskan operasi ISMS
- ✓ Mengurus semua sumber ISMS
- ✓ Melaksanakan prosedur dan kawalan ISMS bagi menangani insiden keselamatan maklumat

c) Memantau dan Menilai ISMS (rujuk kepada Seksyen 4.2.3)

Perkataan *Shall* dalam seksyen 4.2.3 untuk fasa *Check* adalah untuk memastikan agensi mempunyai proses untuk mengawas dan memeriksa ISMS setelah melaksanakan fasa *Do*. Secara terperinci, fasa ini merangkumi aktiviti seperti dalam Rajah 12 berikut:

Rajah 12: Senarai Aktiviti Dalam Fasa *Check*

- ✓ Guna prosedur dan kawalan untuk memantau ISMS
- ✓ Sahkan keselamatan dipatuhi
- ✓ Ukur keberkesanan kawalan ISMS
- ✓ Semak semula penilaian risiko secara berkala
- ✓ Laksana Audit Dalam ISMS secara berkala
- ✓ Laksana semakan semula ISMS
- ✓ Kemas kini pelan keselamatan ICT, jika perlu
- ✓ Selenggara rekod-rekod peristiwa dan tindakan ISMS

i. **Melakukan Pemantauan dan Semak Semula Prosedur**

Pemantauan prosedur membolehkan pengurusan ISMS menyemak sama ada kawalan yang dilaksanakan adalah berkesan dan tanggungjawab yang diberikan kepada pegawai adalah betul sepertimana yang dimaksudkan dalam Pelan Penguraian Risiko.

Untuk keperluan pensijilan, agensi perlu mendokumentasikan setiap kegiatan pemantauan ini dan tindakan yang perlu diambil sebagai bukti dokumen terhadap keputusan kegiatan pemantauan. Agensi boleh memantau pematuan ke atas prosedur-prosedur ISMS melalui Jawatankuasa ISMS agensi atau yang setara.

ii. **Menilai Semula Keberkesanan ISMS**

Agensi perlu menilai sejauh mana keberkesanan pengurusan sistem keselamatan maklumat. Ini boleh diketahui menerusi pematuan kepada dasar keselamatan ICT dan keberkesanan suatu kawalan ISMS (lihat perkara iii). Penilaian keberkesanan ISMS harus mengambil kira penilaian keselamatan, penemuan audit (lihat perkara v) dan cadangan penambahbaikan dari pihak pengurusan (lihat perkara vi). Sebarang kekurangan dalam keberkesanan ISMS hendaklah diambil tindakan pembetulan supaya pengurusan sistem keselamatan maklumat dapat dikekalkan dan ditambah baik.

iii. **Mengukur Keberkesanan Kawalan**

Agensi perlu menentukan kaedah yang sesuai untuk membuat pemantauan ke atas proses dan kawalan ISMS. Agensi harus mengukur keberkesanan proses dan kawalan di mana sesuai, bagi memastikan kawalan dapat memenuhi keperluan sepertimana yang dikenal pasti. Kemantapan sesuatu proses dan kawalan ISMS dapat dinilai dari segi keupayaannya menghasilkan output. Agensi hendaklah merujuk kepada International Standard (ISO/IEC 27004: 2009 *Information Technology-Security Techniques - Information Security Management Measurement*).

iv. **Menilai Semula Penilaian Risiko Secara Berkala**

Bagi memastikan ISMS masih kekal efisien adalah penting untuk memantau dan mengesan sebarang perubahan yang boleh menjejaskan pelaksanaan ISMS. Penilaian semula risiko ini akan mengenal pasti sebarang ancaman, kelemahan (*vulnerability*) dan impak yang diakibatkan oleh perkara seperti berikut:

- Perubahan dasar yang boleh memberi kesan kepada keputusan penguraian risiko atau penilaian aset;
- Perubahan kepada teknologi dan proses-proses perkhidmatan;
- Pemasangan dan naik taraf sistem/aplikasi baru; dan
- Perubahan struktur organisasi (visi/misi/objektif);
- Pelaksanaan kawalan baru selaras dengan strategi perlindungan dalam Pelan Penguraian Risiko; dan
- Peristiwa seperti insiden keselamatan ICT.

v. **Melaksanakan Audit Dalam ISMS**

Agensi hendaklah melaksanakan Audit Dalam ISMS bagi memastikan dasar, prosedur dan kawalan menepati keperluan yang telah dikenal pasti (rujuk seksyen 6: Audit Dalam ISMS). Audit hendaklah dilaksanakan secara berkala sebagaimana yang dirancang.

vi. **Melaksanakan Semakan Semula ISMS**

Di dalam fasa *Check*, pengurusan agensi hendaklah menyemak semula dan menilai keberkesanan ISMS. Antara perkara yang perlu dinilai dan disemak adalah seperti berikut:

- Adakah skop ISMS masih relevan?
- Adakah kawalan masih relevan dan efektif?

- Adakah prosedur masih relevan dan diguna pakai dengan betul?
- Adakah peranan dan tanggungjawab semua personel dalam skop ISMS masih relevan?
- Adakah aktiviti-aktiviti keselamatan dilaksanakan seperti dirancang?
- Adakah proses pengendalian insiden keselamatan ICT masih relevan?
- Adakah pelan kesinambungan perkhidmatan masih relevan?

Proses ini akan mengenal pasti sebarang penambahbaikan yang perlu dilaksanakan dalam fasa *Act*.

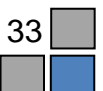
vii. **Mengemas kini Pelan Keselamatan ICT**

Agensi perlu menyediakan prosedur untuk mengambil kira penemuan aktiviti-aktiviti pemantauan dan penyemakan sebagai asas untuk mengemas kini pelan keselamatan ICT, jika ada. Ini supaya tindakan sewajarnya dapat dirancang dan dilaksanakan bagi memastikan keberkesanan pelan tersebut.

viii. **Merekodkan Peristiwa dan Tindakan**

Agensi hendaklah merekodkan semua peristiwa dan tindakan seperti di bawah bagi memastikan sebarang penambahbaikan dapat dikenal pasti:

- Keputusan semakan semula ISMS;
- Audit keselamatan dan Audit Dalam ISMS;
- Pengujian sistem;
- Laporan insiden keselamatan;
- Penemuan pemantauan aktiviti-aktiviti keselamatan; dan
- Maklum balas dan sebarang cadangan daripada pemilik sistem maklumat, pengurusan dan pengguna.



Perekodan Ini dapat membantu dalam mengesan aktiviti-aktiviti ISMS yang tidak berjalan lancar supaya aktiviti tersebut dapat diselenggara bagi memastikan kejayaan ISMS.

d) Selenggara dan Tambah Baik ISMS (rujuk Kepada Seksyen 4.2.4)

Perkataan *Shall* yang dinyatakan dalam MS ISO/IEC 27001:2007, seksyen 4.2.4 adalah merujuk kepada fasa *Act*. Rajah 13 menunjukkan langkah-langkah penyelenggaraan dan penambahbaikan ISMS.

Rajah 13: Keperluan untuk menyelenggara dan menambah baik ISMS

- ✓ Laksana penambahbaikan ISMS
- ✓ Ambil tindakan pembetulan dan/atau pencegahan yang sewajarnya
- ✓ Terapkan sebarang kejadian sebagai pembelajaran keselamatan
- ✓ Maklum perubahan ISMS kepada semua pihak yang berkenaan
- ✓ Pastikan perubahan ISMS mencapai objektif

i. Melaksanakan Tindakan Penambahbaikan Yang Telah Dikenal Pasti.

Proses pemantauan dan penyemakan semula ISMS dalam fasa *Check* mungkin telah mengenal pasti perubahan yang memerlukan penambahbaikan kepada ISMS bagi memastikan keselamatan maklumat diurus dengan sebaiknya. Agensi hendaklah melaksanakan tindakan penambahbaikan dengan mengambil sebarang tindakan yang difikirkan perlu bagi memastikan penambahbaikan berjalan lancar serta mengambil kira maklum balas yang diterima dari fasa *Check*.

Melaksana tindakan penambahbaikan yang telah dikenal pasti mempunyai persamaan dengan melaksanakan prosedur dan kawalan ISMS sedia ada pada peringkat awal. Adalah penting memastikan sebarang tindakan penambahbaikan boleh berjalan lancar dengan kawalan ISMS yang sedia ada.

ii. **Mengambil Tindakan Pembetulan Dan/Atau Pencegahan**

Agensi perlu mewujudkan proses supaya keberkesanan ISMS dapat ditambah baik secara berterusan (lihat Seksyen 8: Penambahbaikan Berterusan). Ini melibatkan perkara seperti penemuan audit dan semak semula ISMS, analisis pemantauan aktiviti pengurusan sistem keselamatan maklumat dan insiden keselamatan ICT. Maka tindakan pembetulan dan pencegahan perlu dilaksanakan bagi menangani sebarang ketidakakuran dalam operasi ISMS dan memastikan perkara tersebut tidak berulang.

Sebarang kejadian hendaklah diambil pengajaran, serta pengalaman jabatan lain yang telah melaksanakan ISMS hendaklah diambil kira dalam memastikan kelancaran pengurusan sistem keselamatan maklumat.

iii. **Maklum Tindakan dan Penambahbaikan Kepada Pihak Berkenaan**

Tindakan pembetulan dan pencegahan hendaklah direkodkan. Hasil penambahbaikan hendaklah dimaklumkan kepada pihak yang berkenaan seperti pengurusan kanan, Jawatankuasa Keselamatan ICT atau yang setara. Sebarang penambahbaikan yang melibatkan perubahan kepada pengurusan sistem keselamatan maklumat hendaklah dimaklumkan kepada semua pengguna supaya sebarang ketidakpatuhan kepada dasar, prosedur dan kawalan baru dapat dielakkan.

iv. **Memastikan Penambahbaikan Mencapai Objektif**

Agensi hendaklah memastikan tindakan penambahbaikan dapat memenuhi keperluan dan mencapai objektif yang dimaksudkan. Ini termasuklah menyemak semula tindakan pembetulan dan pencegahan yang telah dilaksanakan. Kaedah pengukuran dan kawalan yang ditetapkan untuk mengukur keberkesanan proses ISMS boleh membantu dalam mengenal pasti kejayaan tindakan penambahbaikan tersebut. Penemuan pengukuran proses ISMS dan kawalan ini perlu didokumentasikan dan boleh membantu agensi dalam pengurusan risiko.

5.2.3 Keperluan Dokumentasi

a) Keperluan

Dokumentasi Pengurusan Sistem Keselamatan Maklumat hendaklah merangkumi keperluan yang dinyatakan dalam Seksyen 4.3, MS ISO/IEC 27001:2007 seperti di Rajah 14.

Rajah 14: Keperluan Dokumentasi ISMS

Kandungan dokumentasi ISMS amat bergantung kepada kesesuaian agensi: <ul style="list-style-type: none">✓ saiz dan aktiviti organisasi✓ keperluan dokumentasi agensi✓ skop ISMS✓ pemakaian kawalan keselamatan✓ kerumitan sistem maklumat
DOKUMENTASI ISMS:
Pernyataan dasar dan objektif ISMS
Skop ISMS
Prosedur dan kawalan yang menyokong pelaksanaan ISMS
Penerangan mengenai metodologi penilaian risiko yang diamalkan oleh agensi
Laporan penilaian risiko
Pelan penguraian risiko
Prosedur kaedah pengukuran proses dan kawalan ISMS
Rekod menunjukkan bukti pematuhan kepada keperluan dan keberkesanan operasi ISMS
Pernyataan Pemakaian (SoA)

b) Bukti Dokumen

Dokumen ISMS hendaklah mengandungi maklumat yang tepat berhubung dengan pengurusan sistem keselamatan maklumat yang diamalkan oleh agensi. Di samping keperluan dokumen ISMS yang dinyatakan di atas, bukti dokumen ISMS termasuklah semua Minit Mesyuarat yang membincangkan isu-isu berbangkit berhubung pelaksanaan ISMS, sebarang nota status kemajuan yang diangkat ke pihak pengurusan untuk pertimbangan dan tindakan yang telah diambil untuk menangani sebarang isu ISMS yang dibangkitkan.

Dokumen ISMS hendaklah dapat menunjukkan bahawa pelaksanaan kawalan ISMS adalah berasaskan penemuan penilaian risiko, Pelan Penguraian Risiko dan Dasar Keselamatan ICT. Perkara ini sering dibangkitkan dalam audit pengurusan sistem keselamatan maklumat.

c) Selenggara dan Tambah Baik ISMS (rujuk kepada Seksyen 4.2.4)

MS ISO/IEC 27001:2007, Seksyen 4.3.2 dan 4.3.3 menetapkan keperluan untuk mengawal dan melindungi semua dokumen dan rekod ISMS. Prosedur kawalan dokumen dan rekod perlu dibangunkan untuk menangani keperluan ini. Rajah 15 menyenaraikan perkara-perkara yang perlu dinyatakan dalam prosedur kawalan dokumen ISMS.

Rajah 15: Keperluan Kawalan Prosedur Dokumentasi ISMS

Antara Perkara Yang Perlu Dinyatakan Dalam Prosedur

- ✓ Peringkat dokumen ISMS
- ✓ Keselamatan dokumen dan rekod ISMS;
- ✓ Format rujukan dokumen dan rekod ISMS;
- ✓ Versi dokumen
- ✓ Capaian dokumen

Tanggungjawab dan tindakan dalam:

- kawalan dokumen baru dan pindaan dokumen
- mewujudkan, mengumpul maklumat dan data;
- ✓ - menerima dan mengurus rekod
- menyelenggara dan menyimpan rekod
- mengawal pergerakan rekod
- melupuskan rekod ISMS
- menyimpan rekod elektronik ISMS

- ✓ Borang cadangan pindaan dokumen ISMS

5.3 PENJELASAN STANDARD DI BAWAH SEKSYEN 5: TANGGUNGJAWAB PENGURUSAN

Seksyen 5 dalam MS ISO/IEC 27001:2007 menjelaskan keperluan komitmen pengurusan dengan mewujudkan, melaksana, operasi, memantau dan menyemak, menyelenggara dan menambah baik ISMS.

5.3.1 Komitmen Pengurusan

Pengurusan perlu memberikan komitmen serta memainkan peranan dan tanggungjawab dalam pelaksanaan ISMS. Rajah 16 menunjukkan peranan dan tanggungjawab yang seharusnya diambil oleh pihak pengurusan dalam menggalakkan pelaksanaan ISMS di agensi masing-masing.

Rajah 16: Komitmen Pengurusan

Peranan Dan Tanggungjawab Pengurusan

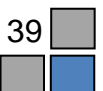
- ✓ Memperakui Jawatankuasa Kerja ISMS atau setara di peringkat agensi
- ✓ Memperakui Dasar Keselamatan ICT

- ✓ Memperakui keperluan kursus kesedaran untuk melaksanakan pensijilan MS ISO/IEC 27001:2007 ISMS
- ✓ Memperakui skop pensijilan MS ISO/IEC 27001:2007 ISMS dan jadual pelaksanaan
- ✓ Memperakui struktur organisasi ISMS
- ✓ Memantau pelaksanaan pensijilan ISMS ke atas skop yang telah ditetapkan
- ✓ Memperakui kriteria penerimaan risiko, tahap risiko, penemuan penilaian risiko dan pelan penguraian risiko
- ✓ Mengkaji semula pengurusan sistem keselamatan maklumat
- ✓ Memantau keputusan mesyuarat berhubung ISMS
- ✓ Menyediakan sumber-sumber untuk melaksanakan ISMS
- ✓ Melantik Pasukan Audit Dalam
- ✓ Melantik badan pensijilan tempatan ISMS untuk melaksanakan pengauditan ke atas skop ISMS
- ✓ Memperakui Laporan Audit Dalam ISMS
- ✓ Memperakui Laporan Audit Pensijilan
- ✓ Memantau pelaksanaan tindakan pembetulan dan pencegahan ke atas ketakakuran yang ditemui oleh Pasukan Audit Dalam/Audit Pensijilan
- ✓ Memantau tindakan penambahbaikan yang disarankan oleh pengurusan atau pengguna
- ✓ Memantau keberkesanan tindakan penambahbaikan, pembetulan dan pencegahan

5.3.2 Pengurusan Sumber

a) Bekalan Sumber

Agensi hendaklah memastikan semua sumber adalah mencukupi untuk mewujudkan, melaksana, memantau, menyemak, menyelenggara dan menambah baik ISMS. Ini merangkumi semua keperluan yang dinyatakan dalam Seksyen 4 sehingga Seksyen 8.



Bekalan sumber adalah sangat penting supaya aktiviti-aktiviti seperti menjalankan penilaian risiko, melaksanakan kawalan keselamatan ICT sedia ada dan operasi harian ISMS berjalan lancar.

b) **Pembangunan Kompetensi**

Agensi hendaklah mengenal pasti keperluan program latihan keselamatan ICT untuk semua personel di bawah skop ISMS supaya masing-masing mempunyai kemahiran dan kepakaran yang sewajarnya bagi melaksanakan peranan dan tanggungjawab yang diperuntukkan dalam urus tadbir ISMS.

Agensi hendaklah memberi kesedaran berhubung dengan peranan dan tanggungjawab semua pengguna seperti mana yang ditetapkan dalam Dasar Keselamatan ICT peringkat agensi. Rekod latihan semua pengguna hendaklah diselenggara dengan baik. Penilaian latihan perlu dilaksanakan untuk menentukan objektif tercapai.

5.4 PENJELASAN STANDARD DI BAWAH SEKSYEN 6: AUDIT DALAM ISMS

Audit Dalam ISMS adalah audit yang dilaksanakan oleh agensi dan bukan audit oleh pihak ketiga. Aktiviti audit ini merupakan keperluan utama dalam Seksyen 6, MS ISO/IEC 27001:2007.

Audit ini bertujuan menentukan sama ada proses, prosedur dan kawalan dalam ISMS dapat memenuhi keperluan keselamatan yang telah dikenal pasti. Di samping itu, untuk mengenal pasti pematuhan kepada arahan dan peraturan keselamatan yang diterbitkan dari semasa ke semasa.

Juru audit ISMS hendaklah memastikan semua pemakaian kawalan ISMS dilaksanakan dan kawalan tersebut mencapai objektif keselamatan yang ditetapkan. Agensi perlu mempunyai perancangan audit ISMS dan menyediakan dokumentasi berhubung peranan dan tanggungjawab audit.

Semua penemuan audit hendaklah direkodkan dan diambil tindakan untuk penambahbaikan, jika perlu. Sebarang ketakakuran perlu diambil tindakan dengan segera. Punca ketakakuran hendaklah dikenal pasti segera dan ditangani bagi mengelak kejadian berulang. Agensi hendaklah menyediakan prosedur untuk mengesahkan bahawa tindakan penambahbaikan telah dilaksanakan.

Semua agensi Kerajaan hendaklah merujuk kepada Panduan Audit Dalam ISMS Sektor Awam sebagai panduan melaksanakan Audit Dalam ISMS.

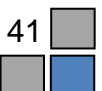
5.5 PENJELASAN STANDARD DI BAWAH SEKSYEN 7: KAJIAN SEMULA ISMS

Pengurusan hendaklah menyemak semula urus tadbir dan semua program ISMS supaya selaras dengan perancangan ISMS. Keperluan ini merujuk kepada Seksyen 7, MS ISO/IEC 27001:2007 bagi memastikan keberkesanan dan kemampuan ISMS yang telah dilaksanakan.

Semakan semula ini membolehkan pengurusan menilai dan membuat keputusan keperluan penambahbaikan dan perubahan yang diperlukan untuk mengurus sistem keselamatan maklumat.

Fasa *Check* mengutamakan pemantauan dan penyemakan semula terhadap sebarang perubahan dalam operasi dan perkhidmatan di persekitaran ISMS. Perubahan ini akan membawa kepada ancaman baru dan penilaian pihak pengurusan sangat penting bagi memastikan ISMS sedia ada, masih relevan dan dapat mengekalkan sistem keselamatan maklumat.

Setelah menilai keadaan ini, pengurusan mungkin membuat keputusan supaya dasar dan prosedur ISMS sedia ada perlu ditambah, dipinda atau ditambah baik. Ini juga mungkin membawa kepada keperluan untuk melihat semula kawalan pengukuhan keselamatan maklumat sedia ada, atau sama ada terdapat keperluan untuk menambah, menukar atau menambah baik kawalan ISMS tersebut.



MS ISO/IEC 27001:2005, Seksyen 7.2 dan Seksyen 7.3 telah menetapkan keperluan untuk *input* dan *output* bagi menjayakan keperluan penyemakan semula ISMS oleh pihak pengurusan.

Agensi hendaklah memastikan input yang disediakan adalah mencukupi dan tepat supaya pihak pengurusan boleh membuat pertimbangan dan keputusan yang tepat. Pengurusan bertanggungjawab untuk memastikan tindakan diambil ke atas semua keputusan mesyuarat.

5.6 PENJELASAN STANDARD DI BAWAH SEKSYEN 8: PENAMBAHBAIKAN BERTERUSAN

Ancaman sistem keselamatan maklumat sentiasa berubah yang dipengaruhi oleh faktor-faktor dalaman dan luaran agensi. Maka, adalah penting untuk mengurus risiko secara proaktif dengan melaksanakan penyemakan semula seperti yang disarankan dalam fasa *Check*. Selain itu, ia bertujuan untuk menangani sebarang perubahan yang boleh mengganggu kelancaran ISMS.

Bagi tujuan ini agensi perlu mempunyai proses untuk melaksanakan penambahbaikan yang telah dikenal pasti dan mengambil tindakan pembetulan serta pencegahan (rujuk Seksyen 8.2 dan Seksyen 8.3 dalam MS ISO/IEC 27001:2007).

Agensi hendaklah mengenal pasti sebarang ketakakuran dalam operasi ISMS. Punca ketakakuran perlu dikenal pasti dan menentukan tindakan yang perlu diambil supaya punca ketakakuran boleh ditangani dengan segera. Tindakan pembetulan hendaklah dilaksanakan segera bagi mengelak kejadian berulang yang boleh menjejaskan sistem keselamatan maklumat.

Output kepada tindakan penambahbaikan perlu direkodkan dan disemak bagi memastikan tindakan tersebut mencapai objektif yang disasarkan. Agensi perlu menentukan sebarang tindakan yang difikirkan sesuai bagi mengenal pasti potensi dan punca ketakakuran.

Sijil akan dikeluarkan oleh badan pensijilan setelah semua penemuan audit diambil tindakan dan dipersetujui. Badan pensijilan akan mengeluarkan sijil yang sah laku untuk tempoh tiga (3) tahun. Dalam tempoh tersebut, agensi perlu melalui beberapa Audit Pemantauan (*surveillance*) yang melibatkan badan pensijilan bagi memantau pelaksanaan terhadap ISMS dan memastikan agensi sentiasa patuh kepada keselamatan maklumat secara efektif dari semasa ke semasa.

6.1 PERSEDIAAN PENSIJILAN

Sebelum agensi menjalani aktiviti pensijilan, perlulah dipastikan bahawa segala keperluan telah dilaksana dan rekod telah dikemas kini bagi memastikan kelancaran aktiviti pensijilan. Persediaan menghadapi pensijilan merangkumi empat (4) perkara yang perlu diberikan perhatian oleh agensi iaitu penilaian pematuhan, bukti auditan, pengecualian dan penerimaan risiko serta dokumentasi pengurusan sistem.

6.1.1 Penilaian Pematuhan

Agensi perlu melaksanakan semua aktiviti dalam Fasa *Plan* sebelum menilai pematuhan kepada standard MS ISO/IEC 27001:2007. Penilaian pematuhan dilaksanakan untuk melihat tahap pematuhan agensi terhadap keperluan standard. Setelah menilai pematuhan aktiviti tersebut, agensi perlu mendokumentasikan output daripada semua aktiviti tersebut bagi tujuan rekod dan bukti semasa audit dilaksanakan kelak. Seterusnya agensi perlu merangka pelan bagi menambah baik tahap pematuhan keperluan standard.

Sebagai contoh, antara aktiviti yang perlu dilaksanakan oleh agensi dalam Fasa *Plan* adalah melaksanakan penilaian risiko dan menyediakan laporan penilaian risiko. Seterusnya merangka satu Pelan Penguraian Risiko.

6.1.2 Bukti Auditan

Agensi perlu mengemukakan bukti kewujudan dan pelaksanaan ISMS. Bukti perlulah dapat menjelaskan berkenaan kitaran proses pelaksanaan ISMS, bermula dari penetapan skop, pewujudan dan pelaksanaan prosedur, dasar-dasar, kawalan-kawalan, senarai aset ICT terlibat serta lain-lain aspek berkenaan keselamatan maklumat di agensi.

Bukti auditan juga perlu dikemas kini dan memenuhi keperluan Standard MS ISO/IEC 27001:2007. Semua dasar, prosedur, standard pengoperasian dan dokumen sokongan hendaklah diedar, difahami dan dipatuhi oleh personel yang terlibat dalam skop ISMS.

6.1.3 Pengecualian dan Penerimaan Risiko

Sebarang pengecualian terhadap kawalan dalam Annex A (*normative*), MS ISO/IEC 27001:2007 yang tidak terlibat dalam skop ISMS perlu diberikan justifikasi dan disertakan dengan bukti penerimaan risiko sesuatu aset ICT.

Pengurusan atasan perlu mengakui bahawa sebarang pengecualian kawalan atau penerimaan risiko tidak memberi impak yang boleh menjejaskan perkhidmatan mahupun operasi agensi.

6.1.4 Dokumentasi Pengurusan Sistem

Semua aktiviti yang telah dilaksanakan dan hasil setiap proses perlulah disokong dengan dokumentasi, rekod-rekod atau lain-lain bentuk bukti yang dapat menjelaskan pematuhan terhadap standard MS ISO/IEC 27001:2007. Sebagai contoh sebarang keputusan yang telah dibuat oleh pengurusan atasan dan tindakan yang telah diambil hendaklah disokong dengan Minit Mesyuarat berkenaan hal yang dibincangkan.

6.2 METODOLOGI AUDIT

Terdapat metodologi audit yang perlu dijalani oleh agensi dalam mendapatkan pensijilan ISMS iaitu Audit Peringkat I, Audit Peringkat II, Audit Pemantauan (*surveillance*) dan Audit Penilaian Semula.

6.2.1 Audit Peringkat I

Agensi perlu melantik badan pensijilan tempatan yang terdiri daripada rakyat Malaysia untuk menjalankan audit ke atas pengurusan sistem keselamatan maklumat. Juru audit pensijilan yang dilantik akan menyemak sama ada dokumentasi yang disediakan memenuhi keperluan standard seperti skop ISMS, Dasar Keselamatan ICT, Laporan Penilaian Risiko, Pelan Penguraian Risiko, Pernyataan Pemakaian dan Laporan Audit Dalam ISMS . Keperluan dokumentasi ISMS adalah merujuk kepada Seksyen 4.3.1 dalam MS ISO/IEC 27001:2007.

6.2.2 Audit Peringkat II

Agensi perlu menjalankan Audit Peringkat II dengan menerima Pasukan Audit daripada badan pensijilan yang telah menjalankan Audit Peringkat I. Tempoh masa audit peringkat II adalah tertakluk kepada tindakan yang telah diambil ke atas semua penemuan audit peringkat I. Tumpuan audit peringkat II ini adalah pematuhan kepada MS ISO/IEC 27001:2007 dan keberkesanan pelaksanaannya.

6.2.3 Audit Pemantauan

Agensi perlu menjalani Audit Pemantauan Tahun 1 dan Tahun 2 dengan menerima Pasukan Audit daripada badan pensijilan yang telah menjalankan Audit Peringkat I dan Audit Peringkat II setelah mendapat pensijilan bagi menilai dan memastikan pematuhan terhadap standard dilaksanakan secara berterusan.

6.2.4 Audit Penilaian Semula

Sebelum tamat tempoh sah laku pensijilan, agensi perlu menerima Pasukan Audit daripada badan pensijilan tempatan untuk menjalankan audit pensijilan bagi tujuan penyambungan sijil MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat.



**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

www.mampu.gov.my

HAK CIPTA 2010 @ MAMPU

Hak cipta terpelihara. Tiada mana-mana bahagian di dalam buku ini boleh diterbitkan semula, dicetak, disalin dan disiarkan bagi tujuan komersial dalam apa-apa bentuk sekalipun tanpa mendapat kebenaran secara bertulis daripada pemegang hak cipta.