SURAT PEKELILING ICT NO. 5/2012

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: PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

RUJ. KAMI: JKM/ICTU/100-15.02 KLT.1(24) **TARIKH:** 7 Disember 2012

---

1. TUJUAN

1.1 Surat Pekeliling ini bertujuan untuk memaklumkan bahawa Kerajaan Negeri mengambil maklum kepentingan penilaian tahap keselamatan rangkaian dan system ICT sektor awam. Oleh yang demikian, semua agensi Kerajaan Negeri digalakkan untuk melaksanakan penilaian ini berpandukan Pekeliling Persekutuan iaitu Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.

1.2 Ia bertujuan untuk menjelaskan pelaksanaan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT yang perlu diberikan perhatian dan diambil tindakan oleh agensi-agensi Kerajaan Negeri.

2. PELAKSANAAN

2.1 Kerajaan Negeri Sarawak telah melaksanakan satu infrastruktur rangkaian ICT berpusat dipanggil SarawakNet, maka penilaian keselamatan rangkaian dan sistem ICT bagi semua Kementerian, Jabatan, Pejabat Residen dan Daerah akan diurus dan diselenggara oleh Unit ICT, Jabatan Ketua Menteri.

2.2 Walaubagaipun, semua Pihak Berkuasa Tempatan dan Badan Berkanun Negeri adalah bertanggungjawab dan digalakkan untuk melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT bagi agensi masing-masing.

2.3 Sebarang kemusykilan berkaitan dengan pelaksanaan boleh berhubung terus dengan Unit ICT, Jabatan Ketua Menteri.

2.4 Surat Pekeliling Am Bilangan 3 Tahun 2009 adalah dilampirkan bersama untuk rujukan dan tindakan selanjutnya.

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

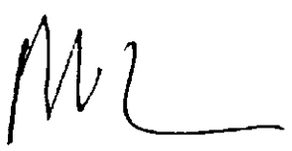
b) Mengesan kelemahan sistem ICT;

c) Melaksanakan tindakan pengukuhan; dan

d) Memantau keberkesanan kawalan pengukuhan.

8. Penilaian Tahap Keselamatan boleh dilaksanakan secara *in-house* atau mendapat perkhidmatan pihak ketiga yang bertauliah.

"BERKHIDMAT UNTUK NEGARA"

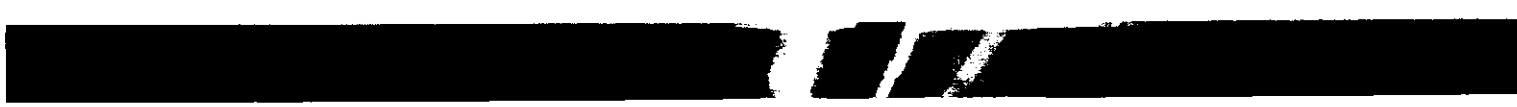


TAN SRI MOHD SIDEK HASSAN
Ketua Setiausaha Negara

Lampiran kepada Surat Pekeliling Am
Bilangan 3 Tahun 2009

GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

UNIT PEMODENAN 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 : 03-8872 3000 / 8872 5000
Telefaks : 03-8888 3721
Laman Web : www.mampu.gov.my
Versi : 1
Pada : 2009
Penulis : MAMPU

KANDUNGAN

KANDUNGAN

GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

LAMPIRAN

GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

TUJUAN

TUJUAN

Dokumen ini bertujuan untuk memberi panduan mengenai pelaksanaan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT (Penilaian Tahap Keselamatan ICT) Sektor Awam.

LANGKAH PENILAIAN

LANGKAH-LANGKAH PENILAIAN

Terdapat tujuh (7) langkah dalam Penilaian Tahap Keselamatan.

LANGKAH 1
Tubuh Pasukan Kerja Penilaian Tahap Keselamatan

LANGKAH 2
Semak Dasar Keselamatan ICT

LANGKAH 3
Nilai Amalan Keselamatan Fizikal

LANGKAH 4
Ujian Penembusan

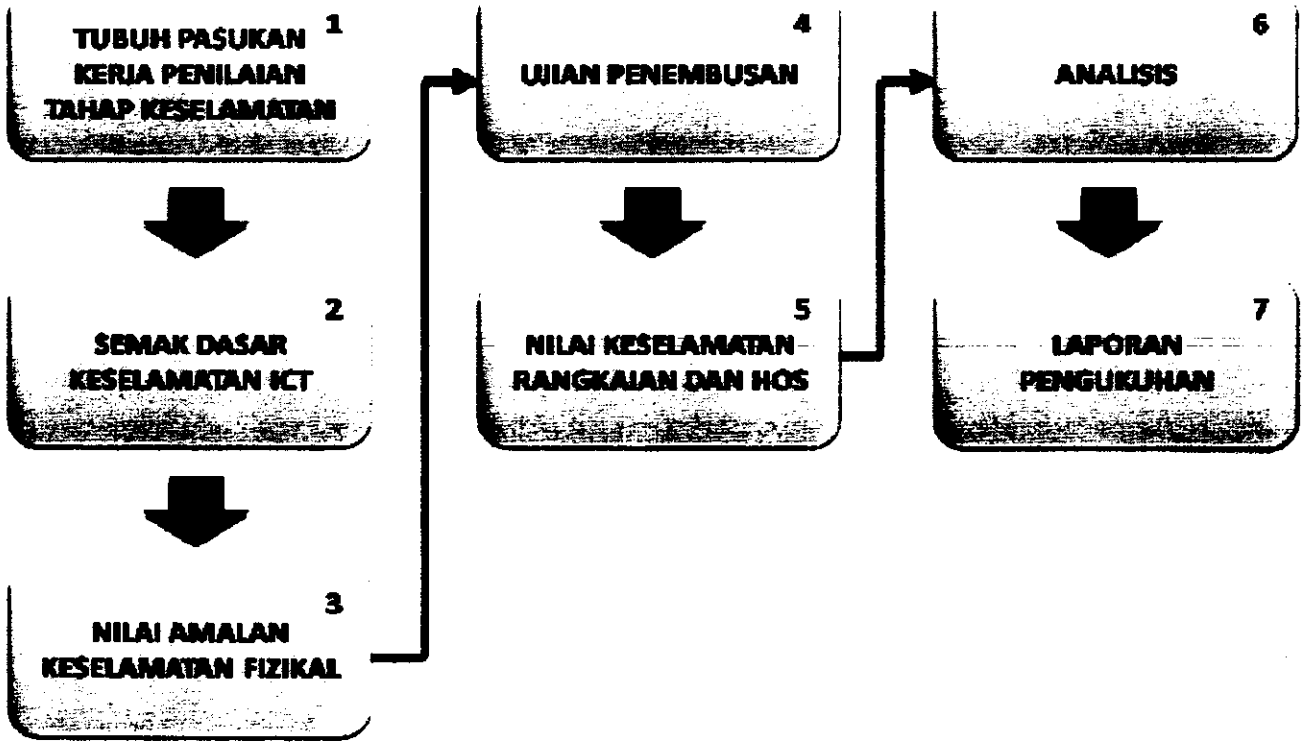
LANGKAH 5
Nilai Keselamatan Rangkaian dan Hos

LANGKAH 6
Analisis

LANGKAH 7
Laporan Pengukuhan

Berikut adalah penerangan langkah-langkah, butiran aktiviti yang perlu dilaksanakan dan hasil penemuan setiap langkah dalam Penilaian Tahap Keselamatan.

LANGKAH-LANGKAH PENILAIAN TAHAP KESELAMATAN



LANGKAH 1:
Tubuh Pasukan Kerja Penilaian Tahap Keselamatan

L
A
N
G
K
A
H

1

Pengurus ICT Jabatan hendaklah mendapat pertimbangan dan kelulusan Jawatankuasa Pemandu ICT (JPICT) Jabatan untuk melaksanakan Penilaian Tahap Keselamatan di peringkat agensi masing-masing.

Keahlian Pasukan Kerja Penilaian Tahap Keselamatan agensi adalah seperti berikut:

i. **Pengerusi** : Pengurus ICT Agensi atau yang setara.

ii. **Ahli-ahli** : Kumpulan Pelaksana hendaklah dianggotai oleh Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat dalam bidang-bidang berikut:
- Sistem Aplikasi;
- Sistem Pengoperasian;
- Rangkaian; dan
- Keselamatan.

iii. **Urus Setia** : Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat

LANGKAH 1:
Tubuh Pasukan Kerja Penilaian Tahap Keselamatan

Bidang tugas rujukan Pasukan Kerja Penilaian Tahap Keselamatan yang berikut hendaklah diambil perhatian dalam melaksanakan Penilaian Tahap Keselamatan di peringkat agensi masing-masing.

AHLI PASUKAN KERJA	PERANAN DAN TANGGUNG JAWAB
i. Pengerusi Pengurus ICT Agensi atau yang setara	- Menerajui arah tuju projek; - Menetapkan skop dan jadual pelaksanaan; - Menyediakan sumber; - Memantau kemajuan; - Mengurus projek; - Memastikan pelaksanaan projek mengikut jadual; - Menyelesaikan isu-isu projek; dan - Mentadbir projek: (a) Melantik ahli Pasukan Kerja Penilaian Tahap Keselamatan. Contoh urus tadbir Pasukan Kerja adalah di Rajah 1; (b) Merancang dan menetapkan jadual pelaksanaan penilaian tahap keselamatan; (c) Melaksana urusan pentadbiran yang berkaitan dengan aktiviti-aktiviti dalam proses penilaian; (d) Mengumpul maklumat yang diperlukan untuk menyokong skop dan jadual kerja penilaian tahap keselamatan; (e) Menetapkan bilangan pelayan; dan (f) Menentukan IP *public network* dan IP *internal network* untuk penilaian tahap keselamatan dari luaran dan dalaman rangkaian agensi melalui pengujian penembusan dan *ethical hacking*.
ii. Kumpulan Pelaksana - Sistem Aplikasi; - Sistem Pengoperasian; - Rangkaian; dan - Keselamatan.	- Melaksanakan penilaian tahap keselamatan; dan - Kemuka cadangan pembangunan/penambahbaikan.
iii. Urus Setia - Pegawai Teknologi Maklumat; atau - Penolong Pegawai Teknologi Maklumat	- Menjalankan tugas-tugas keurusetiaan penilaian tahap keselamatan agensi.

LANGKAH 1:
Tubuh Pasukan Kerja Penilaian Tahap Keselamatan

L
A
N
G
K
A
H

1

OUTPUT

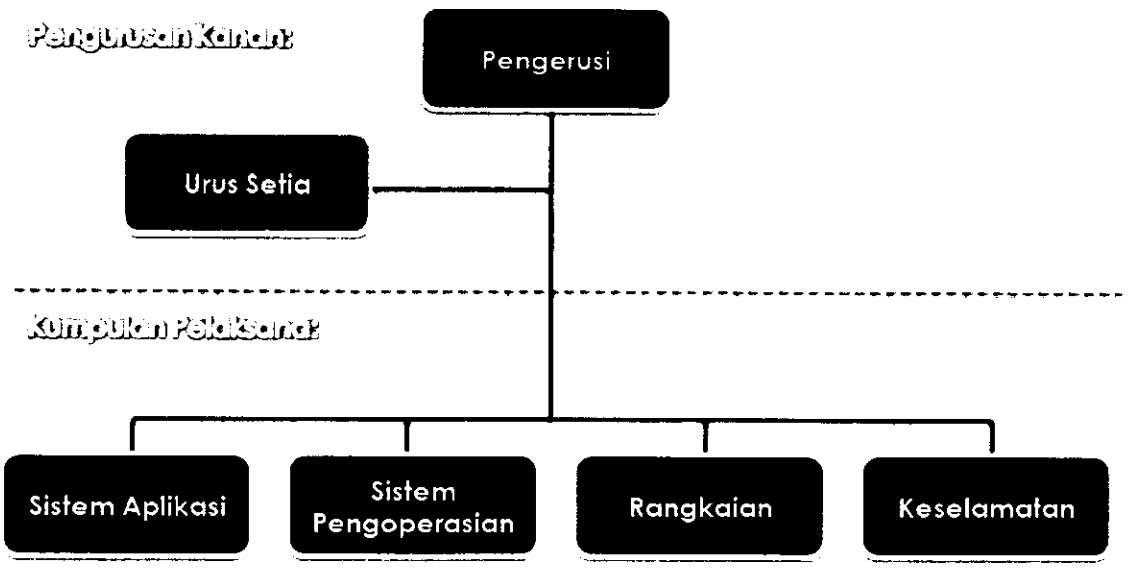
i. **Jadual Pelaksanaan Penilaian Tahap Keselamatan. Rujuk contoh di Lampiran A;**

ii. **Struktur Kumpulan Pelaksana;**

iii. **Skop Kerja Penilaian Tahap Keselamatan. Rujuk contoh di Lampiran B; dan**

iv. **Mesyuarat / perbincangan status kemajuan pelaksanaan penilaian keselamatan ICT.**

Agensi boleh melantik ahli-ahli Pasukan Kerja Penilaian Tahap Keselamatan berdasarkan kategori fungsi dan contoh urus tadbir berikut:



Rajah 1:
Urus Tadbir Pasukan Kerja Penilaian Tahap Keselamatan

LANGKAH 2:
Semak Dasar Keselamatan ICT

Kumpulan Pelaksana perlu semak Dasar Keselamatan ICT agensi yang telah dibangunkan.

AKTIVITI-AKTIVITI

i. Semak dasar keselamatan ICT Agensi dengan menemu bual kumpulan sasaran dan membuat pemerhatian. Contoh Borang Soal Selidik adalah seperti di Lampiran C; dan

ii. Menganalisis data penemuan soal selidik, temu bual dan pemerhatian.

OUTPUT

i. Hasil semakan Dasar Keselamatan ICT.

LANGKAH 3:
Nilai Amalan Keselamatan Fizikal

LANGKAH 3

Kumpulan Pelaksana perlu menilai kekuatan dan kelemahan kawalan keselamatan fizikal melalui pemerhatian persekitaran fizikal dan juga langkah-langkah keselamatan yang sedia ada di agensi.

AKTIVITI-AKTIVITI

i. Memastikan wujudnya sistem kawalan keselamatan fizikal di lokasi penempatan aset ICT agensi. Pemeriksaan keselamatan fizikal adalah seperti pengkabelan, punca kuasa elektrik, kawalan akses, alat pemadam kebakaran dan peralatan pemantauan keselamatan;

ii. Menilai ancaman keselamatan yang merangkumi perkara berikut:
   (a) Memeriksa pelan tindakan jika berlaku bencana seperti kebakaran dan banjir;
   (b) Persekitaran bagi mengelakkan kecurian atau pencerobohan; dan
   (c) Semua peralatan disimpan dalam bilik yang berkunci.

iii. Menemu bual pegawai keselamatan ICT untuk memahami amalan dan prosedur keselamatan ICT sedia ada;

iv. Memeriksa Buku Daftar Masuk/Keluar ke Bilik Server; dan

v. Memerhati amalan sebenar keselamatan di laluan keluar masuk ke premis agensi.

OUTPUT

i. Hasil penemuan keselamatan fizikal.

LANGKAH 4:
Ujian Penembusan

Kumpulan Pelaksana perlu menilai kekuatan dan kelemahan kawalan keselamatan fizikal melalui pemerhatian persekitaran fizikal dan juga langkah-langkah keselamatan yang sedia ada di agensi.

AKTIVITI-AKTIVITI

i. Menjalankan penembusan untuk mendapatkan akses secara remote kepada sistem, fail-fail dan maklumat agensi. Pengujian penembusan dijalankan melalui alamat IP dalaman (*internal* IP) dan alamat IP luaran (*external* IP) seperti Rajah 2;

ii. Menjalankan *network sniffing* untuk mendapatkan maklumat yang disalurkan ke rangkaian;

iii. Mengenal pasti sebarang kelemahan aplikasi atau konfigurasi yang boleh menjejaskan keselamatan ICT;

iv. Menamatkan sebarang aktiviti penembusan setelah berjaya memasuki sistem ICT bagi mengelakkan sebarang perubahan ke atas maklumat atau data sedia ada; dan

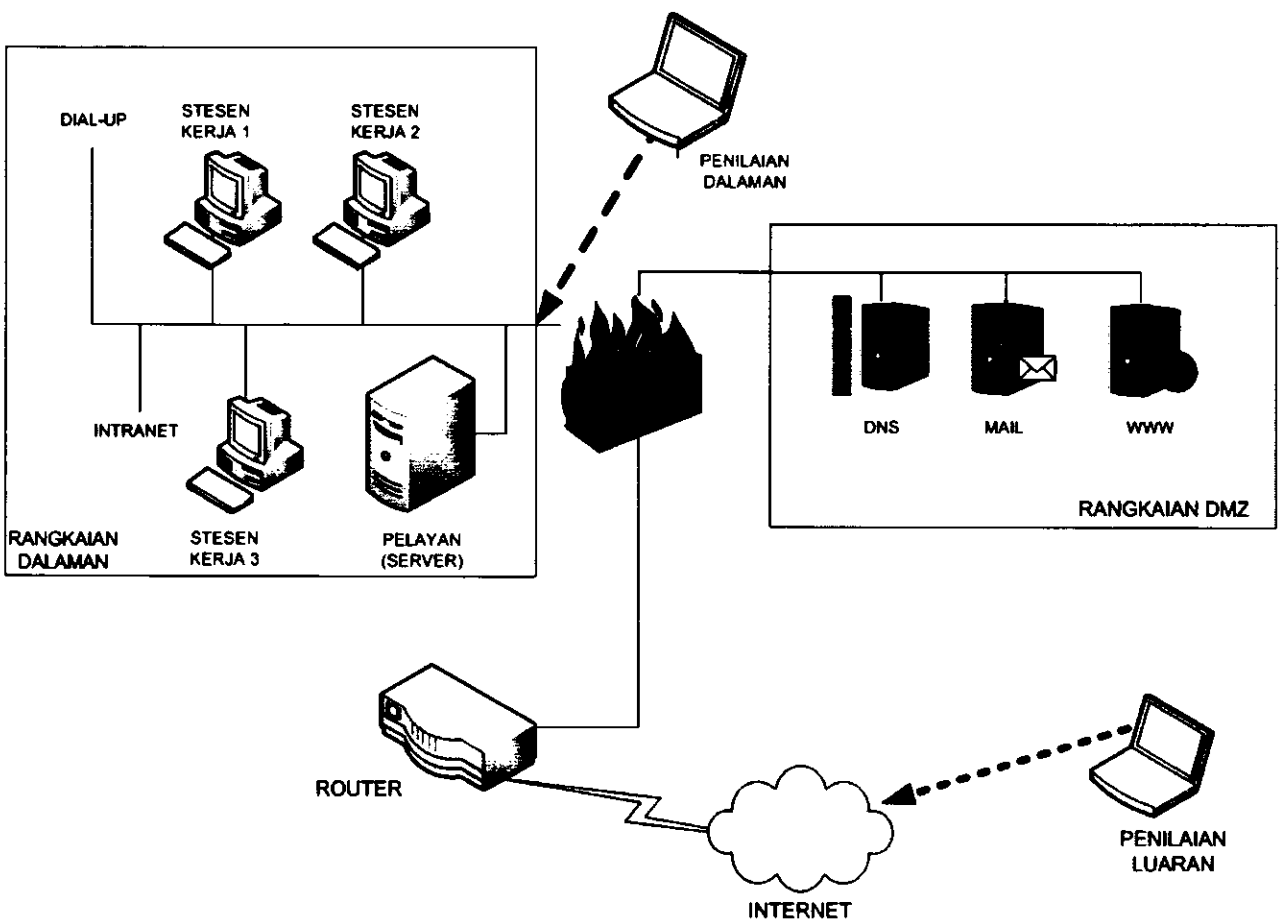
v. Menjalankan pengujian *denial of services* (DOS) untuk menguji keteguhan rangkaian semasa agensi. Pengujian DOS hendaklah mendapat kebenaran terlebih dahulu kerana pengujian akan mengganggu perkhidmatan agensi.

OUTPUT

i. Hasil penemuan penembusan dalaman dan luaran.

LANGKAH 4:
Ujian Penembusan

LANGKAH 4



Rajah 2:
Ujian penembusan melalui alamat IP dalaman dan alamat IP luaran

LANGKAH 5:
Nilai Keselamatan Rangkaian dan Hos

Kumpulan Pelaksana perlu menilai reka bentuk dan keselamatan rangkaian ICT dan sistem-sistem aplikasi sama ada ciri-ciri keselamatan telah diambil kira.

AKTIVITI-AKTIVITI

i. Menilai reka bentuk rangkaian ICT;

ii. Menyemak perimeter dan peranti-peranti;

iii. Menyemak keselamatan sistem pengoperasian dan configuration setup; dan

iv. Menyemak keselamatan sistem aplikasi.

OUTPUT

i. Hasil penemuan keselamatan rangkaian dan hos seperti router, firewall dan sebarang peranti-peranti komunikasi data;

ii. Hasil penemuan reka bentuk rangkaian ICT agensi; dan

iii. Hasil penemuan keselamatan sistem operasi dan sistem aplikasi.

LANGKAH 6:
Analisis

L
A
N
G
K
A
H

6

Kumpulan Pelaksana perlu menganalisis data penemuan serta merumuskan jenis serangan yang berjaya digunakan untuk membuat penembusan.

AKTIVITI-AKTIVITI

i. **Menganalisis data yang dikumpulkan dan membuat perbandingan dengan amalan-amalan terbaik. Agensi boleh merujuk kepada amalan terbaik seperti dalam ISO/IEC 27002:2005 – Information Technology–Security Techniques–Code of Practice for Information Security Management;**

ii. **Mengklasifikasikan kelemahan pengoperasian sistem sedia ada;**

iii. **Merumuskan jenis serangan penembusan; dan**

iv. **Mengenal pasti kelemahan sebenar supaya langkah-langkah pengukuhan dapat dilaksanakan.**

OUTPUT

i. **Hasil penemuan kelemahan rangkaian dan sistem ICT.**

LANGKAH 7:
Laporan Pengukuhan

Kumpulan Pelaksana hendaklah menyediakan laporan yang komprehensif merangkumi hasil penemuan penilaian dan cadangan langkah-langkah pengukuhan keselamatan ICT berdasarkan amalan-amalan terbaik untuk meminimumkan tahap risiko, jika ada, ke tahap yang boleh diterima oleh agensi.

Laporan hendaklah dibentangkan kepada Jawatankuasa Pemandu ICT untuk pertimbangan dan kelulusan supaya langkah-langkah pengukuhan keselamatan ICT agensi dapat dirancang.

AKTIVITI-AKTIVITI

i. Mencadangkan langkah-langkah penyelesaian jangka panjang dan pendek bagi menangani ancaman dan kelemahan aset ICT dalam Laporan Penilaian Tahap Keselamatan. Panduan penyediaan laporan adalah seperti di Lampiran D.

OUTPUT

i. Perakukan cadangan penyelesaian jangka pendek dan panjang; dan

ii. Laporan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT yang merangkumi:
   (a) Cadangan penambahbaikan Dasar Keselamatan ICT Agensi;
   (b) Cadangan penambahbaikan amalan keselamatan fizikal;
   (c) Cadangan langkah-langkah pengukuhan sistem pengoperasian dan sistem aplikasi;
   (d) Cadangan penambahbaikan reka bentuk rangkaian ICT, jika perlu; dan
   (e) Cadangan pengukuhan keselamatan sistem pengoperasian, sistem aplikasi dan konfigurasi peralatan rangkaian ICT.

PENDEKATAN PENILAIAN

TAHAP KESELAMATAN

PENDEKATAN PENILAIAN TAHAP KESELAMATAN

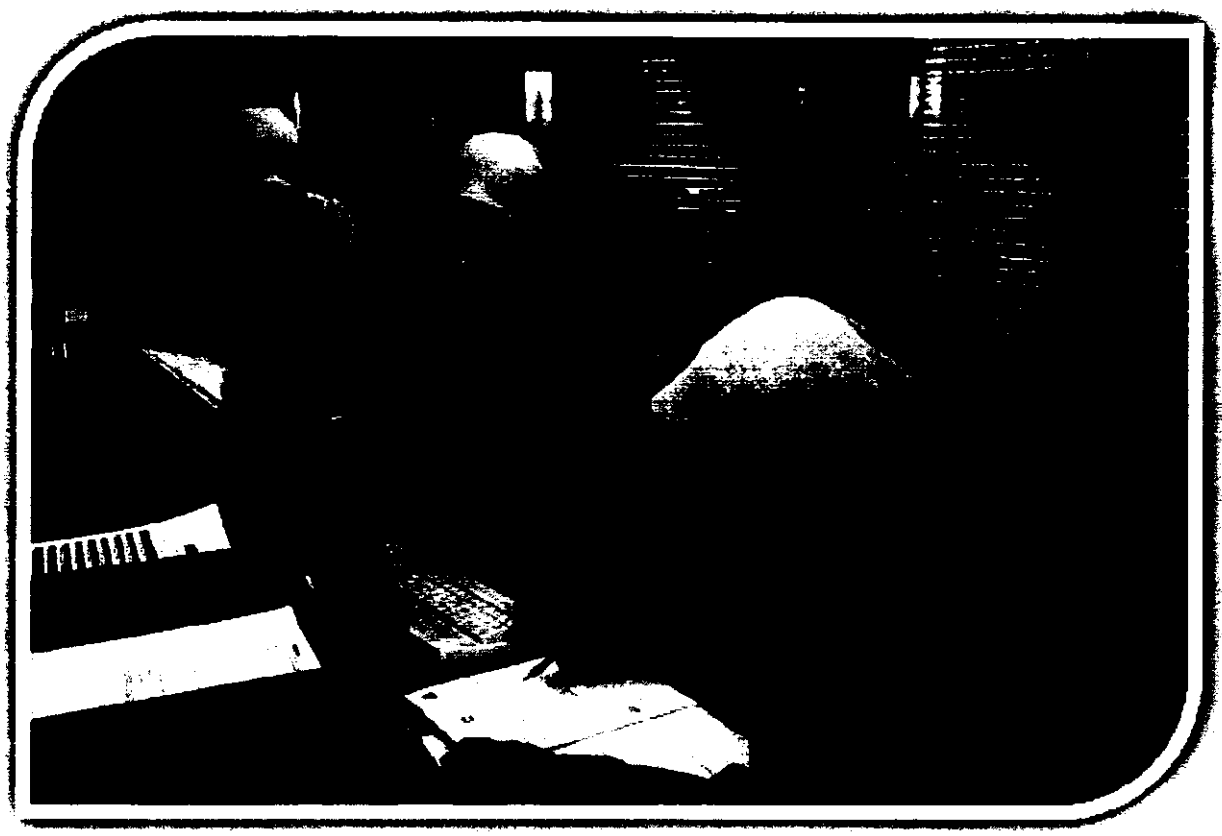
Agensi Sektor Awam hendaklah mengamalkan pendekatan yang sistematik dalam mengurus dan memantau aspek keselamatan sistem ICT pada setiap masa. Ini adalah kerana serangan terhadap rangkaian dan sistem ICT akan mengganggu sistem penyampaian perkhidmatan Kerajaan.

Agensi boleh melaksanakan Penilaian Tahap Keselamatan dengan menggunakan salah satu dari pendekatan berikut iaitu sama ada:

(a) Agensi Melaksanakan Sendiri	(b) Melantik Pihak Ketiga yang Bertauliah
Agensi boleh melaksanakan sendiri Penilaian Tahap Keselamatan dengan melantik pegawai-pegawai yang memenuhi syarat-syarat berikut:	**Agensi boleh mendapat perkhidmatan pihak ketiga yang bertauliah dan memenuhi syarat-syarat berikut:**
i. Memastikan Pegawai Teknologi Maklumat yang bertanggung jawab melaksanakan Penilaian Tahap Keselamatan mempunyai pengetahuan dan kemahiran dalam pengoperasian dan komunikasi ICT;	**i. Syarikat yang telah berdaftar dengan Kementerian Kewangan di bawah pecahan kepala berikut:** **- 210104: Software Products and Services** **- 210105: Other Computer Related Services** **- 210106: Networking Product and Services** **- 242600: Pengurusan Keselamatan**
ii. Memastikan pegawai berkenaan mempunyai mempunyai kemahiran dalam aspek-aspek melaksanakan ujian penembusan ke atas rangkaian dan sistem ICT; dan	**ii. Syarikat yang dipersijilkan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2005 atau MS ISO/IEC 27001:2006; dan**
iii. Memastikan pegawai berkenaan menjalani latihan ujian penembusan rangkaian ICT yang ditawarkan oleh pusat latihan yang bertauliah dalam bidang keselamatan ICT.	**iii. Syarikat yang tiada kaitan dengan vendor yang membekalkan sistem-sistem ICT agensi. Agensi boleh menggunakan panduan seperti di Lampiran E untuk menyenarai pendek pihak ketiga yang berkelayakan.**

Kedua-dua pendekatan di atas perlu mematuhi Langkah 1 hingga Langkah 7 untuk melaksanakan penilaian tahap keselamatan yang telah ditetapkan di dalam garis panduan ini.

KHIDMAT NASIHAT



KHIDMAT NASIHAT

Sebarang kemusykilan yang timbul berkaitan dengan garis panduan ini dan hasil pelaksanaan Penilaian Tahap Keselamatan ICT hendaklah dikemukakan kepada MAMPU seperti di bawah:

Bahagian Pematuhan ICT
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 : 03-8872 3000 / 8872 5000
Faks : 03-8888 3721

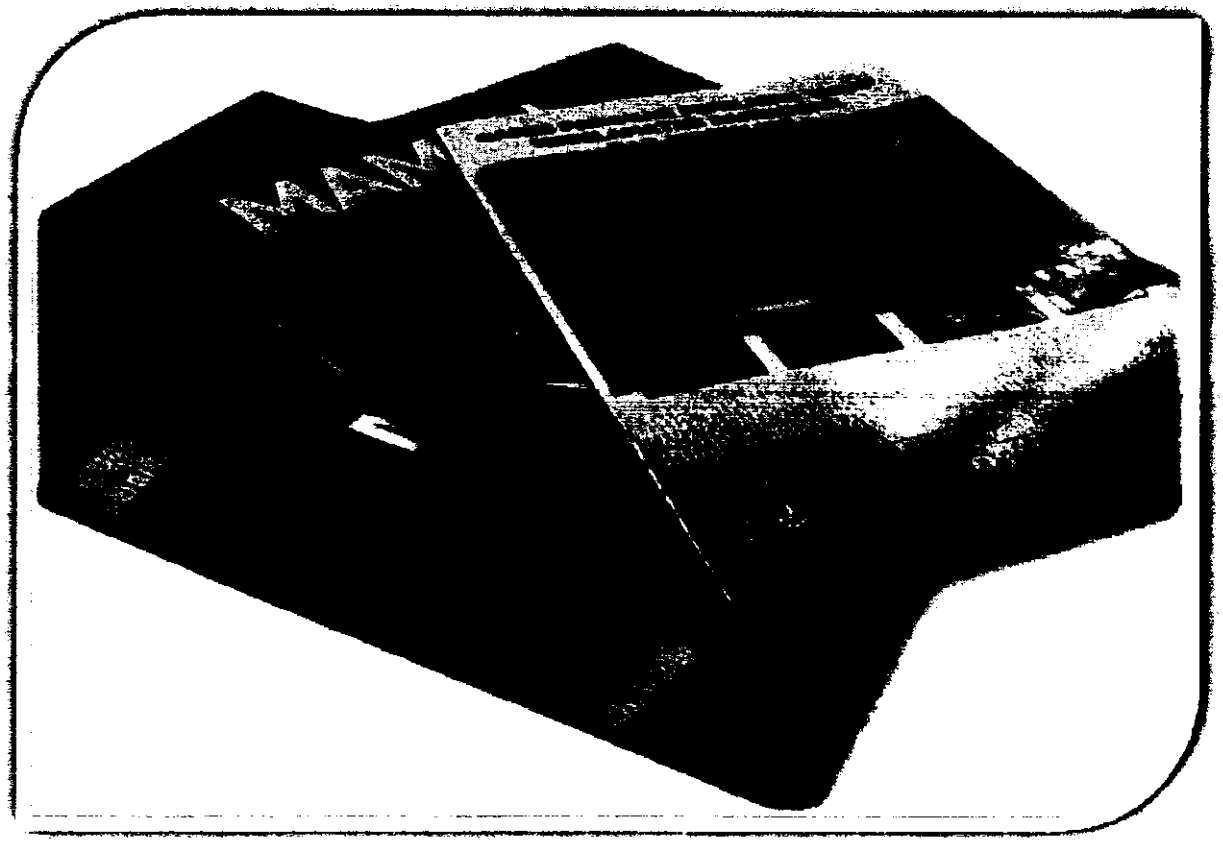
PENUTUP

PENUTUP

Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam ini menjelaskan langkah-langkah penilaian serta memperincikan aktiviti-aktiviti yang perlu dilaksanakan dalam menilai tahap keselamatan bagi membantu agensi merancang pengukuhan yang bersesuaian.

Agensi-agensi hendaklah mematuhi garis panduan ini di dalam menilai tahap keselamatan rangkaian dan sistem ICT masing-masing.

LAMPIRAN



Contoh Jadual Pelaksanaan Penilaian Tahap Keselamatan *

BIL	TARIKH	AKTIVITI	PERINCIAN AKTIVITI	PEGAWAI BERTANGGUNG JAWAB
1.0	Pengurusan Projek			
1.1	hari/ bulan/ tahun	Mesyuarat Kick-Off	i. Menyatakan secara formal dan bersetuju dengan: - Struktur Kumpulan Pelaksana - Skop dan jadual kerja - Proses pentadbiran dan pemantauan (*monitoring process*) - Proses memeriksa dan pertimbangan semula; dan ii. Mengumpul maklumat yang diperlukan untuk menyokong skop dan jadual kerja penilaian tahap keselamatan.	
2.0	Ujian Penembusan Secara Luaran (18 hari)			
2.1	hari/ bulan/ tahun	Eksploitasi Kelemahan (vulnerabilities)	i. Mengenal pasti kelemahan komponen rangkaian dan mengeksploitasi kelemahan untuk mendapat akses ke dalam komponen rangkaian; dan ii. Mengenal pasti sebarang kelemahan aplikasi atau konfigurasi yang tidak tepat dan mengeksploitasi kelemahan untuk mendapat akses ke dalam aplikasi-aplikasi dalam pelayan (*server*).	
2.2	hari/ bulan/ tahun	Ujian Penembusan	i. Laksana penembusan sistem untuk mendapat fail-fail sistem (Contoh: fail kata laluan).	
3.0	Nilai Reka Bentuk Rangkaian dan Keselamatan (2 hari)			
3.1	hari/ bulan/ tahun	Nilai Semula Rangkaian	i. Pertimbangan semula reka bentuk rangkaian.	
3.2	hari/ bulan/ tahun	Nilai Peranti dalam Perimeter	i. Pertimbangan semula perimeter, peranti-peranti (*devices*) dan *configuration setup*.	

LAMPIRAN A

BIL	TARIKH	AKTIVITI	PERINCIAN AKTIVITI	PEGAWAI BERTANGGUNG JAWAB
4.0	Ujian Penembusan Secara Dalaman (10 hari)			
4.1	hari/ bulan/ tahun	Eksploitasi kelemahan	i. Mengenal pasti kelemahan komponen rangkaian dan mengeksploitasi kelemahan untuk mendapat akses ke dalam komponen rangkaian; dan ii. Mengenal pasti sebarang kelemahan aplikasi atau konfigurasi yang tidak tepat dan mengeksploitasi kelemahan untuk mendapat akses ke dalam aplikasi-aplikasi dalam pelayan (*server*).	
4.2	hari/ bulan/ tahun	Ujian Penembusan	i. Laksana penembusan sistem untuk mendapat fail-fail sistem (Contoh: fail kata laluan).	
5.0	Semak Dasar Keselamatan ICT (2 hari)			
5.1	hari/ bulan/ tahun	Semak dasar	i. Semak maklumat yang berkaitan dalam Dasar Keselamatan ICT.	
5.2	hari/ bulan/ tahun	Temu duga	i. Temu duga pegawai-pegawai yang berkenaan.	
6.0	Nilai Amalan Keselamatan Fizikal (2 hari)			
6.1	hari/ bulan/ tahun	Semak Maklumat Yang Berkaitan	i. Semak keselamatan fizikal seperti pengkabelan, punca kuasa elektrik, Buku Rekod Pelawat, alat pemadam kebakaran dan mekanisme pemantauan keselamatan; dan ii. Semak amalan kawalan akses seperti buku rekod pelawat.	
6.2	hari/ bulan/ tahun	Temu duga	i. Temu duga pegawai-pegawai yang berkenaan untuk mengetahui keselamatan fizikal yang diamalkan. - Pilih dan perhatikan amalan sebenar di laluan keluar masuk premis	

BIL	TARIKH	AKTIVITI	PERINCIAN AKTIVITI	PEGAWAI BERTANGGUNG JAWAB
7.0	Mesyuarat Kemajuan (1 hari)			
7.1	hari/ bulan/ tahun	Mesyuarat Kemajuan	i. Objektif mesyuarat: - Lapor kemajuan projek Penilaian Tahap Keselamatan; - Lapor sebarang kelemahan kritikal yang ditemui dan cadang langkah pengukuhan untuk menangani dengan segera; dan - Pastikan maklumat keselamatan adalah benar atau tepat sebelum menyediakan laporan.	
8.0	Nilai Keselamatan Hos (1 hari)			
8.1	hari/ bulan/ tahun	Nilai Hos	i. Periksa pelayan untuk mengetahui kelemahan; dan ii. Periksa konfigurasi pelayan berbanding amalan terbaik untuk konfigurasi sesebuah pelayan.	
9.0	Analisis Data dan Penyediaan Laporan Akhir (23 hari)			
9.1	hari/ bulan/ tahun	Analisis Data dan Penyediaan Laporan	i. Analisis data penemuan penilaian, rangkaian, hos dan ujian penembusan. Banding penemuan dengan amalan terbaik terkini untuk menangani risiko yang tidak boleh diterima; ii. Kategorikan kelemahan mengikut tajuk-tajuk utama seperti fizikal, prosedur, teknikal, perisian, aplikasi dan sebagainya; iii. Analisis data untuk mengenal pasti persamaan atau percanggahan maklumat; dan iv. Kenalpasti ancaman, risiko dan kelemahan: - Kumpul cadangan langkah-langkah pengukuhan - Sedia laporan akhir.	

LAMPIRAN A

LAMPIRAN A

BIL	TARIKH	AKTIVITI	PERINCIAN AKTIVITI	PEGAWAI BERTANGGUNG JAWAB
9.2	hari/ bulan/ tahun	Verifikasi Laporan	i. Pengesahan penemuan-penemuan dan langkah-langkah pengukuhan yang dicadangkan dalam laporan akhir.	
9.3	hari/ bulan/ tahun	Pembentangan Laporan Akhir	i. Bentang penemuan dan pengukuhan Penilaian Tahap Keselamatan dalam Mesyuarat Jawatankuasa Pemandu ICT untuk mendapat pertimbangan dan kelulusan.	
10.0	Pengukuhan Sistem dan Konfigurasi Semula			
10.1	hari/ bulan/ tahun	Tentu Sah Langkah Pengukuhan	i. Laksanakan langkah-langkah pengukuhan yang telah diluluskan oleh Mesyuarat Jawatankuasa Pemandu ICT.	

Contoh Format Skop Perkhidmatan

PENILAIAN TAHAP KESELAMATAN

Skop Perkhidmatan

(NAMA JABATAN)

(bulan/tahun)

(alamat penuh jabatan)

Perhatian kerahsiaan:

Maklumat yang terdapat dalam dokumen ini hanya diperuntukkan kepada senarai edaran yang ditetapkan sahaja. Ini adalah kerana dokumen mungkin mengandungi maklumat rahsia dari segi undang-undang.

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

LAMPIRAN B

Tajuk	Penilaian Tahap Keselamatan
Disediakan Oleh	(*nama Ketua Pelaksana*)
Tarikh	*hh/bb/tttt*
Versi	

SENARAI EDARAN:

1. **Ketua Pegawai Maklumat (*Chief Information Officer*)**
2. **Pengurus ICT**
3. **Pegawai Keselamatan ICT (ICTSO)**

SKOP PERKHIDMATAN

Berikut adalah senarai aktiviti dalam skop kerja untuk melaksanakan Penilaian Tahap Keselamatan di (nama Jabatan).

Skop kerja merangkumi perkara-perkara:

i. **Pengurusan Projek** dengan perincian aktiviti seperti berikut:
   - Mengurus projek;
   - Memastikan pelaksanaan projek mengikut jadual;
   - Menyelesaikan isu-isu projek; dan
   - Mentadbir projek:
     (a) Melantik ahli kumpulan pelaksana;
     (b) Merancang dan menetapkan jadual pelaksanaan penilaian tahap keselamatan;
     (c) Melaksana urusan pentadbiran yang berkaitan dengan aktiviti-aktiviti dalam proses penilaian;
     (d) Mengumpul maklumat yang diperlukan untuk menyokong skop dan jadual kerja penilaian tahap keselamatan;
     (e) Menetapkan bilangan pelayan; dan
     (f) Menentukan IP *public network* dan IP *internal network* untuk penilaian tahap keselamatan dari luaran dan dalaman rangkaian agensi melalui pengujian penembusan atau *ethical hacking*.

ii. **Kumpulan Pelaksana** merangkumi fungsi seperti Sistem Aplikasi, Sistem Pengoperasian, Rangkaian dan Keselamatan akan:
   - Melaksanakan penilaian tahap keselamatan; dan
   - Kemukakan cadangan pembangunan/penambahbaikan.

iii. **Semak Dasar Keselamatan ICT** dengan perincian aktiviti seperti berikut:
   - Semak maklumat yang berkaitan dalam Dasar Keselamatan ICT; dan
   - Temu duga pegawai-pegawai yang berkenaan.

iv. **Nilai Amalan Keselamatan Fizikal** dengan perincian aktiviti seperti:
   - Semak keselamatan fizikal seperti pengkabelan, punca kuasa elektrik, Buku Rekod Pelawat, alat pemadam kebakaran dan mekanisme pemantauan keselamatan.

v. **Ujian Penembusan Secara Luaran** (eksploitasi kelemahan dan ujian penembusan) dengan perincian aktiviti seperti:
- Mengenal pasti k elemahan komponen rangkaian dan mengeksploitasi kelemahan untuk mendapat akses ke dalam komponen rangkaian;
- Mengenal pasti sebarang kelemahan aplikasi atau konfigurasi dan mengeksploitasi kelemahan untuk mendapat akses ke dalam aplikasi-aplikasi dalam pelayan (server); dan
- Berdasarkan alamat IP luaran berikut:
  (nyatakan IP luaran).

vi. **Ujian Penembusan Secara Dalaman** (eksploitasi kelemahan dan ujian penembusan) dengan perincian aktiviti seperti:
- Uji tahap keselamatan rangkaian dalaman;
- Simulasi serangan: capaian remote, DOS, *network sniffing* dan *spoofing*;
- Berikut adalah julat alamat IP yang diuji:
  (nyatakan julat alamat IP); dan
- Penilaian Kelemahan (*vulnerability*) ke atas pelayan berikut:
  (senaraikan IP pelayan yang hendak dinilai).

vii. **Penilaian Hos** ke atas pelayan berikut sahaja:
- (senaraikan pelayan terlibat)
- Butiran penilaian adalah seperti berikut:
  (a) *System Configuration*;
  (b) *File Permission*;
  (c) *Authentication*;
  (d) *Auditing and system logs*; dan
  (e) *System services and application*.

viii. **Analisis Data** dengan perincian aktiviti seperti:
- Analisis data penemuan penilaian, rangkaian, hos dan ujian penembusan. Banding penemuan dengan amalan baik terkini untuk menangani risiko yang tidak boleh diterima;
- Kategorikan kelemahan mengikut tajuk-tajuk utama seperti fizikal, prosedur, teknikal, perisian, aplikasi dan sebagainya;
- Analisis data untuk mengenal pasti persamaan atau percanggahan maklumat; dan

- Kenal pasti ancaman, risiko dan kelemahan:
  (a) Kumpul cadangan langkah-langkah pengukuhan
  (b) Sediakan laporan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT.

ix. **Penemuan dan Cadangan Pengukuhan** dengan perincian aktiviti seperti:
- Bentang penemuan Penilaian Tahap Keselamatan dan cadangan langkah-langkah pengukuhan melalui pendekatan jangka pendek dan/atau panjang untuk pertimbangan dan kelulusan Mesyuarat Jawatankuasa Pemandu ICT Agensi.

LAMPIRAN C

Borang Soal Selidik Untuk Semak Dasar Keselamatan ICT

BIL	NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
	BIDANG 1: DASAR KESELAMATAN		
1.	**Adakah wujud dokumen Dasar Keselamatan ICT?**		
2.	Adakah dasar tersebut mengandungi objektif dan skop keselamatan maklumat?		
3.	**Adakah dasar keselamatan ICT mendapat kelulusan di peringkat atasan?**		
4.	Adakah dasar tersebut diedarkan kepada semua warga agensi?		
	BIDANG 2: PENGURUSAN KESELAMATAN ICT		
5.	**Adakah wujud jawatankuasa pengurusan keselamatan ICT terdiri dari pengurusan atasan atau yang setara, untuk memberi arah tuju dan sokongan?**		
6.	Adakah peranan dan tanggung jawab keselamatan maklumat dilaksanakan ke seluruh agensi?		
7.	**Adakah perlindungan ke atas aset ICT menjadi tanggung jawab agensi?**		
8.	Adakah wujud proses perolehan dan pemasangan aset ICT?		
	BIDANG 3: PENGURUSAN ASET		
9.	**Adakah agensi mempunyai inventori untuk aset-aset ICT?**		
10.	Adakah sistem inventori dikemas kini setiap kali berlaku perubahan dalam maklumat aset?		
11.	**Adakah aset maklumat diberi klasifikasi keselamatan? (Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar)**		
12.	Adakah terdapat prosedur untuk pelabelan maklumat terperingkat?		
13.	**Adakah terdapat prosedur untuk pengendalian maklumat terperingkat?**		

BIL	NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
	BIDANG 4: KESELAMATAN SUMBER MANUSIA		
14.	**Adakah keselamatan ICT dinyatakan dalam senarai tugas?**		
15.	Adakah pihak pembekal atau pihak ketiga perlu menanda-tangani perjanjian NDA (*Non Disclosure Agreement*)?		
16.	**Adakah kontraktor atau pekerja sementara diawasi jika kerja itu melibatkan akses pada kemudahan pemprosesan data?**		
17.	Adakah dasar tersebut diedarkan kepada semua warga agensi?		
	BIDANG 5: KESELAMATAN FIZIKAL DAN PERSEKITARAN		
18.	**Adakah kemudahan ICT dilindungi secara fizikal?**		
19.	Adakah peralatan komunikasi dan kabel dilindungi?		
20.	**Bolehkan data agensi dihapuskan tanpa kebenaran rasmi?**		
21.	Adakah aset ICT agensi dilupuskan mengikut prosedur rasmi?		
22.	**Adakah pelayan (*server*) dilindungi dari kegagalan sumber kuasa?**		
	BIDANG 6: PENGURUSAN OPERASI DAN KOMUNIKASI		
23.	**Adakah prosedur operasi didokumenkan dan dikawal?**		
24.	Adakah pengujian dan pembangunan sistem diasingkan dari pengoperasian?		
25.	**Adakah perisian anti-virus beroperasi di dalam semua pelayan, komputer peribadi dan komputer mudah alih?**		
26.	Adakah wujud dasar untuk pematuhan bagi perisian berlesen?		

LAMPIRAN C

BIL	NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
	BIDANG 7: KAWALAN AKSES		
27.	Adakah agensi mempunyai dasar kawalan akses yang didokumenkan? (Contohnya menyenaraikan siapa yang boleh mengakses maklumat)		
28.	**Adakah terdapat proses pendaftaran rasmi sebelum akses kepada perkhidmatan ICT dibenarkan?**		
29.	Adakah hak akses ditarik balik sebaik sahaja pengguna bertukar keluar/bersara/berhenti/tamat perkhidmatan?		
30.	**Adakah *user root* atau *administrator* dikawal dan dihadkan?**		
31.	Adakah agensi mengeluarkan panduan ke atas kerahsiaan kata laluan?		
	BIDANG 8: PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM MAKLUMAT		
32.	**Adakah ciri-ciri keselamatan diambil kira dalam pembangunan sistem-sistem aplikasi?**		
33.	Adakah penilaian risiko dan pengurusan risiko di guna pakai untuk menganalisis kawalan? (Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam)		
34.	**Adakah terdapat proses pengurusan perubahan (*change request*) rasmi?**		
35.	Adakah dasar bagi penggunaan kriptografi untuk melindungi maklumat?		
	BIDANG 9: PELAN KESINAMBUNGAN PERKHIDMATAN		
36.	Adakah terdapat proses pengurusan kesinambungan perkhidmatan?		
37.	**Adakah pelan kesinambungan perkhidmatan disemak secara berkala?**		

BIL	NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
38.	Adakah program kesedaran pelan kesinambungan perkhidmatan diadakan?		
39.	**Adakah pelan kesinambungan perkhidmatan di uji?**		
40.	Adakah wujud perjanjian jika pelan kesinambungan perkhidmatan gagal?		
	BIDANG 10: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN		
41.	**Adakah agensi mempunyai prosedur pengurusan insiden?**		
42.	Adakah pengguna dimaklumkan mengenai proses pelaporan insiden keselamatan?		
	BIDANG 11: PEMATUHAN		
43.	**Adakah agensi menggalakkan hak harta intelek?**		
44.	Adakah peruntukan keselamatan ICT dinyatakan di dalam kontrak ICT?		
45.	**Adakah audit ICT dirancang dan dilaksanakan secara berkala?**		

Panduan Penyediaan Laporan Penilaian Tahap Keselamatan

PANDUAN LAPORAN PENILAIAN TAHAP KESELAMATAN	
Bahagian I: Pengenalan	**Menerangkan latar belakang program Penilaian Tahap Keselamatan seperti rumusan aktiviti-aktiviti yang dilaksanakan serta penemuan utama setiap aktiviti. Selain itu, skop kerja yang telah dipersetujui perlu dinyatakan di dalam bahagian ini.**
Bahagian II: Pengurusan Keselamatan Maklumat	Menerangkan mengenai pengurusan keselamatan maklumat. Perkara-perkara yang terlibat dalam bahagian ini ialah semakan ke atas dasar keselamatan ICT sedia ada, penilaian amalan, langkah-langkah keselamatan fizikal dan konfigurasi keselamatan rangkaian. Setiap penemuan penilaian dimaklumkan dengan disertakan syor cadangan penambahbaikan yang paling sesuai berasaskan amalan baik pengurusan keselamatan ICT.
Bahagian III: Ujian Penembusan	**Menghuraikan ulasan teknikal yang merangkumi maklumat/bukti mengenai penemuan ujian penembusan dalaman dan luaran. Ini termasuk penerangan mengenai setiap langkah penembusan yang dilaksanakan dan bukti yang telah diperolehi merangkumi *screen-captures* setiap aktiviti tersebut. Setiap kelemahan yang ditemui hendaklah disertakan bersama dengan cadangan tindakan pengukuhan.**
Bahagian IV: Penilaian Keselamatan Pelayan	Menjelaskan mengenai penilaian keselamatan yang telah dilaksanakan ke atas pelayan (*server*) yang menggunakan sistem pengoperasian sedia ada. Terangkan penilaian yang telah dilaksanakan terhadap setiap konfigurasi dan dilampirkan penemuannya. Sebarang penemuan kelemahan perlu disertakan dengan cadangan pengukuhan.
Bahagian V: Rumusan dan Cadangan	**Merumuskan semua penemuan penilaian keselamatan dan mencadangkan penambahbaikan amalan baik untuk setiap langkah dalam Penilaian Tahap Keselamatan, jika perlu.**

Panduan Borang Soal Selidik Menyenarai Pendek Pihak Ketiga Yang Bertauliah

BIL	PERKARA	YA	TIDAK	HURAIAN
1.	**Adakah penilaian keselamatan ICT menjadi urusan teras syarikat pembekal?**			
2.	Berapa lama syarikat pembekal telah memberikan perkhidmatan penilaian tahap keselamatan? (Sila isi butiran dalam ruang Huraian)			
3.	**Adakah pembekal menawarkan perkhidmatan yang boleh diubahsuai mengikut keperluan spesifik agensi?**			
4.	Adakah pembekal tiada kaitan dengan *vendor* yang membekalkan sistem-sistem ICT agensi?			
5.	**Adakah pembekal bergantung pada maklumat keselamatan ICT yang dihebahkan menerusi pelbagai media?**			
6.	Adakah pembekal menjalankan penyelidikan sendiri?			
7.	**Apakah kelayakan pakar perunding syarikat? (Sila isi butiran dalam ruang Huraian)**			
8.	Apakah tahap pengalaman pasukan ujian yang dicadangkan? (Berapa lama telah membuat pengujian dan apakah latar belakang mereka?) (Sila isi butiran dalam ruangan Huraian)			
9.	**Adakah personel pembekal ditauliahkan CISSP, CISA atau yang setaraf?**			
10.	Adakah personel pembekal menyumbang kepada industri keselamatan ICT? (Contoh: kertas kerja, penasihat, penceramah umum, dan sebagainya)			

BIL	PERKARA	YA	TIDAK	HURAIAN
11.	**Adakah kurikulum vitae ahli pasukan yang akan menyertai projek agensi ada disediakan?**			
12.	Apakah pendekatan pembekal dalam projek ini?			
13.	**Adakah pembekal mempunyai metodologi yang standard seperti OSSTM dan OWASP?**			
14.	Adakah pembekal pernah melaksanakan Penilaian Tahap Keselamatan di agensi Sektor Awam?			
15.	**Bolehkah agensi mendapat contoh laporan Penilaian Tahap Keselamatan untuk menilai output pembekal?**			
16.	Adakah isu-isu hasil penemuan dikemukakan dalam bentuk yang mudah difahami (*non-technical*)?			
17.	**Adakah pembekal *outsource* atau menggunakan kontraktor?**			
18.	Adakah terdapat rujukan dari pelanggan-pelanggan yang berpuas hati dengan perkhidmatan pembekal dalam sektor keselamatan ICT?			
19.	**Adakah pembekal mempunyai pengetahuan mengenai beberapa standard serta garis panduan amalan terbaik berkaitan dengan keselamatan ICT pada amnya, serta khusus untuk ujian penembusan? (seperti *Open Source Security Testing Methodology Manual* (OSSTMM), *The Open Web Application Security Project* (OWASP) dan sebagainya).**			

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