KERAJAAN MALAYSIA

SURAT PEKELILING AM BILANGAN 4 TAHUN 2024

GARIS PANDUAN
PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

JABATAN PERDANA MENTERI

21 MAC 2024

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua YB Setiausaha Kerajaan Negeri
Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri
Semua Pihak Berkuasa Tempatan

JABATAN PERDANA MENTERI
PRIME MINISTER'S DEPARTMENT
Blok B8, Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 Putrajaya
MALAYSIA

Tel. : 03-8000 8000
Fax : 03-8888 3904
Web : http://www.jpm.gov.my
Emel : jpm@jpm.gov.my

Rujukan Kami: MKN.10.700-8/151 JLD 3 (6)

Tarikh: 21 Mac 2024

Semua Ketua Setiausaha Kementerian

Semua Ketua Jabatan Persekutuan

Semua YB Setiausaha Kerajaan Negeri

Semua Pihak Berkuasa Berkanun Persekutuan dan Negeri

Semua Pihak Berkuasa Tempatan

SURAT PEKELILING AM BILANGAN 4 TAHUN 2024

GARIS PANDUAN
PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

1. TUJUAN

Surat Pekeliling Am ini bertujuan untuk dijadikan rujukan pelaksanaan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT (PTK ICT) yang perlu diberikan perhatian serta tindakan yang sewajarnya oleh Agensi Sektor Awam.

2. LATAR BELAKANG

2.1 Kerajaan telah menerbitkan dokumen Strategi Keselamatan Siber Malaysia (Malaysia *Cyber Security Strategy*, MCSS) pada 12 Oktober 2020. Seiring dengan visi MCSS ini, agensi perlu mempertingkatkan sistem penyampaian perkhidmatan Kerajaan menerusi penggunaan teknologi baharu (*new technology*) dan teknologi sedang muncul (*emerging technology*) supaya boleh dicapai pada bila-bila masa disamping memastikan ruang siber negara selamat, dipercayai dan berdaya tahan untuk memacu perkembangan ekonomi serta menjamin kesejahteraan rakyat.

2.2 Semua maklumat atau data yang disimpan, diproses dan dihantar dalam bentuk digital di ruang siber hendaklah berada pada tahap ketersediaan yang tinggi, selamat dan dipercayai. Rangkaian, sistem dan aset ICT di agensi perlu dilindungi daripada ancaman keselamatan siber dengan tindakan mengesan dan menghalang pencerobohan perisian hasad, komuniti penggodam, pelanggaran data, mengelakkan kebocoran serta kecurian data yang melibatkan maklumat sensitif dan harta intelek.

2.3 Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam telah melangkaui tempoh lima tahun, perlu dikaji semula dan ditambah baik untuk memastikan keselamatan data adalah tersedia, selamat dan dipercayai seiring dengan perkembangan teknologi terkini.

3. PELAKSANAAN

Garis Panduan PTK ICT Sektor Awam dilampirkan bersama Surat Pekeliling Am ini untuk rujukan dan pelaksanaan semua Agensi Sektor Awam.

4. PROGRAM PEMANTAUAN KESELAMATAN RANGKAIAN DAN SISTEM ICT

4.1 Sebagai langkah mengurangkan risiko gangguan sistem penyampaian perkhidmatan digital Kerajaan, Ketua Jabatan perlu melaksanakan PTK ICT sebelum pelancaran sistem aplikasi dan rangkaian yang baharu, secara berkala (sekurang kurangnya sekali setiap tahun) dan apabila berlaku perubahan pada rangkaian dan sistem ICT.

4.2 Pelaksanaan PTK ICT merupakan satu kaedah untuk membolehkan agensi memantau dan mengesan kelemahan serta ancaman terhadap rangkaian dan sistem ICT supaya pengukuhan dan penambahbaikan keselamatan ICT dapat dirancang dan dilaksanakan.

5. PERANAN DAN TANGGUNGJAWAB KETUA JABATAN

5.1 Semua agensi hendaklah mematuhi Surat Pekeliling Am ini dan seterusnya melaksanakan tanggungjawab yang ditetapkan. Untuk maksud ini, semua Ketua Jabatan adalah diminta mengambil tindakan-tindakan berikut:

(i) Menjalankan penilaian tahap keselamatan tahap keselamatan rangkaian dan sistem ICT.

(ii) Mengesan kelemahan tahap keselamatan rangkaian dan sistem ICT.

(iii) Melaksanakan tindakan pengukuhan.

(iv) Memantau keberkesanan kawalan pengukuhan.

5.2 Pelaksanaan PTK ICT boleh dilaksanakan secara dalaman (*in-house)* atau melalui perkhidmatan pihak ketiga (*outsource)* yang telah memenuhi syarat-syarat yang ditetapkan oleh Kerajaan.

6. MAKLUMAT PERTANYAAN

Sebarang pertanyaan berkaitan dengan Surat Pekeliling Am ini hendaklah dirujuk kepada Agensi Keselamatan Siber Negara (NACSA) melalui maklumat perhubungan seperti di bawah:

Agensi Keselamatan Siber Negara (NACSA)
Majlis Keselamatan Negara
Aras LG & G, Blok Barat
Bangunan Perdana Putra
62502 PUTRAJAYA
Telefon : 03-8064 4888
Faks : 03-8064 4848
E-mel : admin@nacsa.gov.my

7. PEMAKAIAN

Surat Pekeliling Am ini terpakai kepada semua Agensi Sektor Awam bermula dari tarikh Surat Pekeliling Am ini ditandatangani. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Surat Pekeliling Am ini pada keseluruhannya dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Negeri dan Pihak Berkuasa Tempatan.

8. PEMBATALAN

Dengan berkuat kuasanya Surat Pekeliling Am ini, Surat Pekeliling Am Bil. 3 Tahun 2009 Garis Panduan Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam adalah dibatalkan.

9. TARIKH KUAT KUASA

Surat Pekeliling Am ini berkuat kuasa mulai dari tarikh ia dikeluarkan

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

(TAN SRI DATO' SERI MOHD ZUKI BIN ALI)
Ketua Setiausaha Negara

GARIS PANDUAN
PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM

AGENSI KESELAMATAN SIBER NEGARA (NACSA)
MAJLIS KESELAMATAN NEGARA
JABATAN PERDANA MENTERI

KANDUNGAN

PERKARA **MUKA SURAT**

GARIS PANDUAN
PENILAIAN TAHAP KESELAMATAN RANGKAIAN DAN SISTEM ICT SEKTOR AWAM (PTK ICT)

---

1. PENGENALAN

Peningkatan insiden keselamatan siber dan kemunculan pelbagai teknik serangan siber bersasar (*targeted cyber attacks*) menyebabkan wujudnya keperluan untuk menilai risiko ancaman keselamatan maklumat sebelum pelancaran rangkaian dan sistem ICT yang baharu secara berkala serta apabila berlakunya perubahan pada rangkaian dan sistem ICT agensi.

Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT (PTK ICT) perlu dilaksanakan untuk mengesan kelemahan dan kerentanan yang mungkin wujud pada rangkaian dan sistem ICT bagi membolehkan tindakan pengukuhan, pemantauan dan pengawalan risiko dengan lebih efektif dilaksanakan.

PTK ICT membantu agensi lebih bersedia dalam menangani insiden keselamatan siber dan secara tidak langsung akan meningkatkan tahap jaminan keselamatan dari aspek Kerahsiaan, Integriti dan Ketersediaan (*Confidentiality*, *Integrity and Availability* (CIA)) pada data di rangkaian dan sistem ICT agensi.

2. TUJUAN

Garis Panduan PTK ICT Sektor Awam ini bertujuan sebagai:

(i) Rujukan pelaksanaan PTK ICT di agensi.
(ii) Panduan perancangan, pelaksanaan dan pemantauan program PTK ICT yang berkesan.

3. TAFSIRAN

3.1 Bagi tujuan Surat Pekeliling Am ini yang hanya terpakai kepada sektor awam, terma di bawah ditafsirkan seperti yang berikut:

(i) **"Agensi"** ialah Agensi Sektor Awam yang merangkumi kementerian dan jabatan pada peringkat pentadbiran Kerajaan, Kerajaan Persekutuan, Badan Berkanun Persekutuan, Pejabat Setiausaha Kerajaan (SUK) Negeri, Badan Berkanun Negeri serta Pihak Berkuasa Tempatan (PBT).

(ii) **"Ancaman"** ialah penyebab bagi insiden-insiden tidak diingini yang boleh mengakibatkan kemudaratan kepada sistem dan organisasi serta berupaya mengancam keselamatan negara.

(iii) **"Ancaman Siber"** ialah ancaman yang berpunca daripada Internet atau rangkaian menggunakan laluan komunikasi data yang memberi kesan terhadap kerahsiaan, integriti dan ketersediaan sistem maklumat dari dalam agensi mahupun dari jarak jauh serta penyebaran maklumat melalui medium siber yang bertentangan dengan undang-undang negara serta berupaya menggugat keselamatan negara.

(iv) **"Aset ICT"** ialah peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

(v) **"*Attack Surface Analysis*"** ialah analisis keselamatan berkenaan pendedahan dan kelemahan rangkaian dan sistem ICT agensi yang menjadi punca pencerobohan data dan gangguan perkhidmatan. Aktiviti ini menilai pelbagai kelemahan yang ditemui, pengumpulan data risikan ancaman dan menilai risiko ancaman yang diketahui dan tidak diketahui terhadap kemungkinan serangan siber.

(vi) **"*Attack Surface*"** ialah set sempadan untuk sistem, elemen sistem atau persekitaran dimana penggodam cuba untuk menceroboh dan mengakibatkan perubahan ke atas data atau mengekstrak keluar data.

(vii) **"*Cloud Framework Agreement* (CFA)"** ialah kontrak yang ditandatangani antara Kerajaan Malaysia dengan setiap CSP dan MSP. Kontrak Panel Berpusat bagi perkhidmatan pengkomputeran awan yang dilaksanakan dikenali sebagai CFA dan MAMPU berperanan sebagai pentadbir kontrak CFA.

(viii) **"*Cloud Service Provider* (CSP)"** ialah pembekal atau penyedia perkhidmatan pengkomputeran awan, sama ada dalam negara mahupun luar negara. CSP bertanggungjawab menyediakan perkhidmatan pengkomputeran awan seperti storan, rangkaian, pelayan dan sebagainya.

(ix) **"Harta Intelek"** ialah apa-apa karya, ciptaan, rekaan, variasi baru tumbuhan, maklumat sulit termasuk rahsia perdagangan yang layak untuk mendapat perlindungan di bawah mana-mana undang-undang harta intelek, khususnya undang-undang hak cipta, paten, reka bentuk perindustrian, cap dagangan, petunjuk geografi, reka bentuk susun atur litar bersepadu, jenis baru tumbuhan dan undang-undang *'Common Law'*.

(x) **"Infrastruktur Sebagai Perkhidmatan (*Infrastructure as a Service* atau IaaS)"** ialah model perkhidmatan yang menyediakan infrastruktur asas bagi sumber pengkomputeran seperti *Central Processing Unit* (CPU), memori (RAM), storan, keselamatan dan rangkaian secara maya bagi menyokong operasi aplikasi atau perisian pengguna. Model ini membenarkan pengguna mengurus dan mengawal sistem pengoperasian (OS), storan, aplikasi dan komponen rangkaian.

(xi) ***"Intrusive"*** ialah ujian penembusan yang dilaksanakan untuk mengesan dan mengeksploitasi kelemahan rangkaian dan sistem ICT yang telah dijumpai.

(xii) **"Kebocoran Data"** ialah keadaan apabila data atau perisian sulit dicuri atau diketahui orang yang tidak berkenaan.

(xiii) **"Kerentanan"** ialah kelemahan, kekurangan, atau ralat yang terdapat dalam rangkaian dan sistem ICT yang berpotensi dieksploitasi oleh mana-mana agen ancaman yang boleh mengakibatkan gangguan atau kerosakan pada sistem ICT, kebocoran atau pelanggaran data agensi.

(xiv) **"Keselamatan Fizikal"** ialah aspek keselamatan fizikal berdasarkan peraturan dan sistem yang dibentuk dan dilaksanakan dengan tujuan untuk menghalang akses yang tidak dibenarkan.

(xv) **"Keselamatan Perimeter"** ialah perlindungan keselamatan sempadan rangkaian agensi daripada penggodam, penceroboh dan dari individu yang tidak diingini. Ini memerlukan aktiviti pengesanan, pengawasan, analisis corak (*pattern analysis*), pengecaman ancaman dan tindak balas yang berkesan.

(xvi) **"Ketua Jabatan"** ialah pegawai yang mengetuai sesebuah agensi awam di peringkat ibu pejabat, iaitu termasuk Ketua Setiausaha, Ketua Pengarah dan Ketua Perkhidmatan.

(xvii) **"*Managed Service Provider* (MSP)"** ialah syarikat tempatan yang dilantik oleh CSP yang bertanggungjawab untuk melaksanakan pengurusan dan khidmat sokongan teknikal perkhidmatan pengkomputeran awan selain daripada perkhidmatan yang diberikan oleh CSP.

(xviii) ***"Non-intrusive"*** ialah ujian penembusan yang dilaksanakan secara pasif untuk mengenal pasti dan mengesan kelemahan rangkaian dan sistem ICT tanpa tindakan eksploitasi.

(xix) **"Pengumpulan Maklumat Risikan (*Intelligence gathering*)"** ialah pengumpulan dan analisis data yang ditemui daripada pelbagai sumber yang boleh dipercayai bagi mengenal pasti bentuk ancaman siber semasa dan berpotensi berlaku kepada rangkaian dan sistem ICT. Maklumat yang diperoleh dapat digunakan oleh penilai dalam menentukan keperluan dan teknik untuk melaksanakan PTK ICT.

(xx) **"Perisian Sebagai Perkhidmatan (*Software as a Service* atau SaaS)"** ialah model perkhidmatan yang menyediakan perisian aplikasi melalui Internet, mengikut keperluan dan berasaskan kepada langganan. CSP bertanggungjawab menguruskan semua keperluan infrastruktur ICT, penyelenggaraan dan keselamatan (*security patches*). Pengguna hanya memerlukan sambungan ke Internet melalui pelayar web peranti tetap atau mudah alih bagi mengkonfigurasi aplikasi mengikut keperluan.

(xxi) **"Platfom Sebagai Perkhidmatan (*Platform as a Service* atau PaaS)"** ialah model perkhidmatan yang menyediakan platfom bagi membangunkan perisian aplikasi melalui Internet, mengikut keperluan dan berasaskan kepada langganan. CSP menyediakan platfom yang diperlukan dalam kitaran pembangunan sistem seperti *operating systems, development tools, database, programming languages* dan *libraries* menerusi perkhidmatan yang disediakan.

(xxii) **"Pelanggaran Data"** ialah perbuatan yang tidak mematuhi terma dan undang-undang yang menyebabkan data dicerobohi dan dicuri tanpa pengetahuan atau kebenaran pemilik sistem.

(xxiii) **"Risiko"** ialah pendedahan kepada ancaman siber dan eksploitasi kelemahan yang mengakibatkan serangan siber dan pelanggaran data.

(xxiv) **"Sistem ICT"** ialah satu persekitaran / tetapan yang terdiri daripada perisian meliputi sistem / program yang digunakan dan individu yang menggunakannya.

(xxv) “**Ujian Kotak Hitam (*Black-Box Testing*)”** ialah pengujian menggunakan metodologi penilaian keselamatan yang dilaksanakan secara luaran dan dalaman. Penilai **tidak disediakan sebarang maklumat** berkenaan rangkaian dan sistem ICT yang akan dinilai. Penilai perlu menentukan teknik yang diperlukan untuk mengesan kelemahan dan eksploitasi yang boleh digunakan bagi cubaan menceroboh dari luar. Aktiviti ini dapat menunjukkan kemungkinan penggunaan teknik penggodaman terkini yang akan digunakan oleh penggodam sebenar (*real threat actor*) terhadap rangkaian dan sistem ICT.

Ujian ini dijalankan berdasarkan kriteria / skop ujian tertentu bersama dengan keperluan teknologi, perisian dan teknik yang akan ditentukan dan difikirkan sesuai oleh penilai. Aktiviti ini adalah rumit dan mengambil tempoh masa yang lebih lama untuk menghasilkan keputusan ujian yang menyeluruh.

(xxvi) **“Ujian Kotak Kelabu (*Grey-Box Testing)*”** ialah pengujian yang dilaksanakan berdasarkan **maklumat terhad** disediakan kepada penilai sebelum penilaian tahap keselamatan dilaksanakan meliputi maklumat reka bentuk rangkaian dan sistem ICT serta akaun pengguna. Maklumat tersebut digunakan oleh penilai untuk memahami tahap akses yang boleh digunakan oleh pengguna sistem yang sah dan kemungkinan berlakunya kerosakan disebabkan penyalahgunaan capaian kepada rangkaian dan sistem ICT.

(xxvii) **“Ujian Kotak Putih (*White-Box Testing)*”** ialah pengujian dilaksanakan berdasarkan **maklumat terperinci** yang disediakan kepada penilai sebelum penilaian tahap keselamatan dilaksanakan seperti kod sumber sistem aplikasi, reka bentuk rangkaian dan akses kepada sistem aplikasi. Maklumat ini digunakan bagi melaksanakan ujian bersasar kepada skop penilaian bagi mengenal pasti kerentanan dan kepelbagaian jenis serangan yang berpotensi boleh berlaku.

(xxviii) **"Ujian Penembusan *(Penetration Testing)*"** ialah kaedah menguji kekukuhan mekanisme keselamatan sistem komputer dengan membuat pencerobohan yang terancang. Pengujian ini dilaksanakan untuk mencari kelemahan dan kerentanan yang tidak dijangka pada rangkaian dan sistem ICT.

(xxix) **"Ujian Penembusan Persekitaran Luaran (*External Penetration Testing*)"** ialah ujian yang dilaksanakan secara luaran kepada infrastruktur rangkaian untuk mengenal pasti kelemahan dan kerentanan konfigurasi keselamatan yang mungkin terdedah kepada penggodam dan ancaman dari luar.

(xxx) **"Ujian Penembusan Persekitaran Dalaman (*Internal Penetration Testing*)"** ialah ujian yang dilaksanakan secara dalaman kepada infrastruktur rangkaian untuk mengenal pasti kelemahan dan kerentanan konfigurasi keselamatan yang mungkin terdedah kepada penggodam dan ancaman dari dalam.

(xxxi) ***"Zero-Day Attacks"*** ialah serangan yang mengeksploitasi kerentanan perkakasan, perisian tegar (*firmware*) atau perisian yang tidak diketahui sebelum ini.

4. LANGKAH-LANGKAH PTK ICT

4.1 Langkah-langkah pelaksanaan PTK ICT ini adalah seperti berikut:

(i) Mewujudkan / menubuhkan tadbir urus dan pasukan kerja PTK ICT.

(ii) Menyediakan Pelan Pelaksanaan PTK ICT agensi.

(iii) Menyemak pematuhan rangkaian, sistem ICT dan keselamatan fizikal terhadap Dasar Keselamatan ICT / Polisi Keselamatan Siber.

(iv) Mengenalpasti kerentanan rangkaian dan sistem ICT melalui pelaksanaan:

a. Ujian penembusan dan penilaian kerentanan keselamatan rangkaian dan sistem ICT.
b. Penilaian asas keselamatan (*Security Baseline Assessment*).
c. Ujian penembusan dan penilaian kerentanan perkhidmatan pengkomputeran awan.
d. *Compromise Assessment* (CA) untuk mengenal pasti punca dan sebarang aktiviti pencerobohan.

(v) Melaksanakan analisis hasil penemuan, menyediakan cadangan pengukuhan dan merumuskan semua aktiviti PTK ICT.

(vi) Menyediakan laporan yang komprehensif dan lengkap.

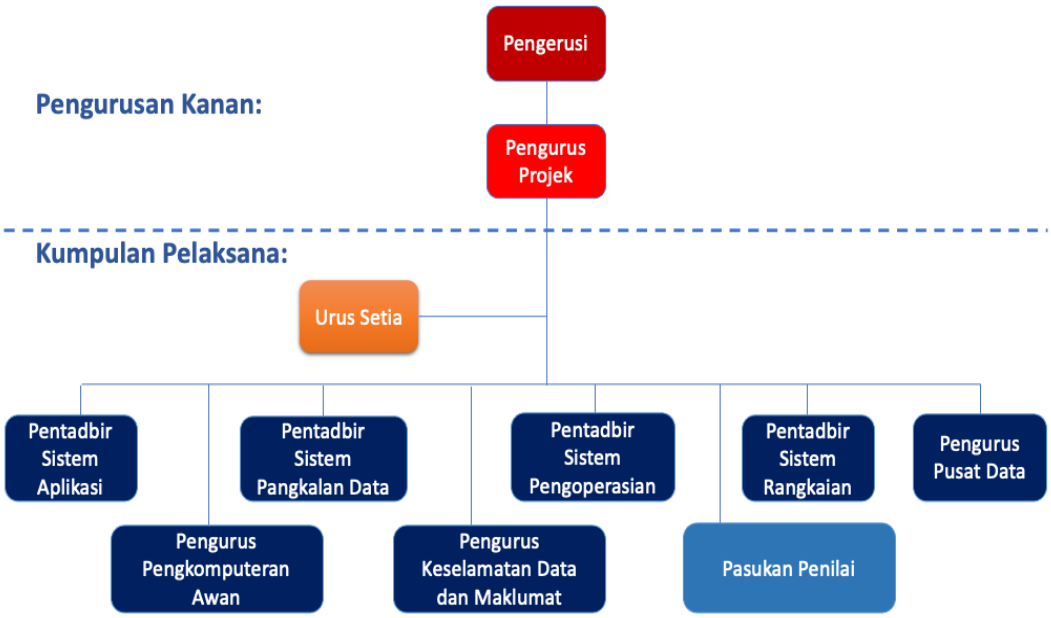
(vii) Melaksanakan tindakan pengukuhan dan penambahbaikan terhadap sebarang kelemahan yang ditemui mengikut tempoh masa yang dipersetujui dan tahap keparahan (*severity*) kerentanan.

(viii) Melaksanakan ujian pasca penilaian untuk mengesahkan dan memastikan kelemahan telah berjaya dipulihkan.

5. MENUBUHKAN PASUKAN KERJA PTK ICT

5.1 Agensi hendaklah mendapatkan pertimbangan dan kelulusan Jawatankuasa Pemandu ICT (JPICT) atau mana-mana jawatankuasa yang setara untuk menubuhkan Pasukan Kerja PTK ICT untuk melaksanakan Penilaian Tahap Keselamatan ICT di peringkat agensi masing-masing.

5.2 Cadangan keahlian Pasukan Kerja PTK ICT adalah seperti berikut:



Rajah 1: Cadangan Struktur Tadbir Urus Pasukan Kerja PTK ICT

5.3 Peranan keahlian Pasukan Kerja PTK ICT agensi adalah seperti berikut:

PERANAN	JAWATAN
Pengurusan Kanan	
i. Pengerusi	*Chief Digital Officer* (CDO) atau Pegawai Keselamatan ICT (ICTSO)
ii. Pengurus Projek	Pengurus ICT / Keselamatan atau yang setara
Kumpulan Pelaksana	
iii. Ahli-ahli	Dilantik dalam kalangan Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat yang terlibat mengurus dan mentadbir bidang tugas seperti di bawah: ▪ Sistem Aplikasi. ▪ Sistem Pangkalan Data. ▪ Sistem Pengoperasian.

PERANAN	JAWATAN
	▪ Sistem Rangkaian. ▪ Pengurusan Pusat Data. ▪ Pengurusan Pengkomputeran Awan. ▪ Keselamatan Data dan Maklumat.
iv. Pasukan Penilai	Pasukan Penilai boleh dilantik secara dalaman atau menggunakan pihak ketiga seperti di bawah: a. Secara dalaman - terdiri daripada Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat yang mempunyai pengetahuan dan kepakaran untuk melaksanakan PTK ICT. b. Pihak ketiga (*outsource*) - melalui perkhidmatan pihak ketiga yang telah memenuhi syarat-syarat ditetapkan oleh Kerajaan seperti di **Para 18.**
v. Urus Setia	Terdiri daripada Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat yang akan menguruskan pelaksanaan PTK ICT.

Jadual 1: Keahlian Pasukan Kerja PTK ICT

5.4 Peranan dan tanggungjawab Pasukan Kerja PTK ICT yang dilantik adalah seperti berikut:

AHLI PASUKAN KERJA	PERANAN DAN TANGGUNGJAWAB
i. Pengerusi	a. Meneraju dan menetapkan arah tuju pelaksanaan PTK ICT. b. Memastikan sumber yang diperlukan disediakan. c. Membuat keputusan berhubung isu-isu berkaitan dengan pelaksanaan PTK ICT. d. Melantik ahli Pasukan Kerja PTK ICT. Contoh tadbir urus Pasukan Kerja seperti di Rajah 1.
ii. Pengurus Projek	a. Menetapkan skop dan merancang jadual pelaksanaan. b. Melaksanakan urusan pentadbiran dan menyelaras sumber. c. Memantau kemajuan pelaksanaan PTK ICT. d. Memastikan pelaksanaan PTK ICT mengikut jadual. e. Menyelesaikan isu-isu pelaksanaan PTK ICT. f. Mentadbir pelaksanaan PTK ICT
iii. Ahli-ahli	a. Melaksanakan dan membantu aktiviti PTK ICT. b. Menyediakan *IP public network* dan *IP internal network* untuk penilaian tahap keselamatan ICT dari luaran dan dalaman rangkaian agensi melalui pengujian penembusan mengikut keperluan. c. Menetapkan bilangan sistem aplikasi, peralatan infrastruktur dan pelayan / *server* yang akan dilaksanakan PTK ICT berdasarkan skop.

AHLI PASUKAN KERJA	PERANAN DAN TANGGUNG JAWAB
	d. Mengesahkan laporan yang telah disediakan oleh Pasukan Penilai (secara dalaman / pihak ketiga (*outsource*)). e. Melaksanakan tindakan pengukuhan.
iv. Pasukan Penilai	Melaksanakan penilaian PTK ICT berdasarkan skop perkhidmatan yang telah ditetapkan seperti **Para 4 (iii) hingga (viii).**
v. Urus Setia	a. Menjalankan tugas-tugas keurusetiaan PTK ICT agensi. b. Memastikan jadual pelaksanaan PTK ICT dipatuhi. c. Melaksana urusan pentadbiran yang berkaitan dengan aktiviti-aktiviti dalam proses penilaian PTK ICT. d. Mengumpul maklumat yang diperlukan untuk menyokong skop dan jadual kerja PTK ICT. e. Memastikan semua dokumentasi berhubung PTK ICT disediakan dan dikemaskini dengan sewajarnya. f. Menyediakan minit mesyuarat / nota perbincangan status kemajuan pelaksanaan PTK ICT. g. Menyediakan repositori berpusat di peringkat agensi (PTJ) bagi menyimpan semua dokumentasi PTK ICT dengan selamat dan dengan akses yang ditetapkan.

Jadual 2: Peranan dan tanggungjawab Pasukan Kerja PTK ICT

6. PENYEDIAAN PELAN PELAKSANAAN PTK ICT

6.1 Penyediaan pelan pelaksanaan PTK ICT dilaksanakan secara dalaman atau bersama pihak ketiga merangkumi dan tidak terhad pada perkara berikut:

i. Menyatakan skop penilaian yang dilaksanakan.

ii. Menyenaraikan sistem dan aset ICT yang terlibat.

iii. Menyenaraikan jenis-jenis ujian penembusan.

iv. Menyediakan Jadual Pelaksanaan PTK ICT yang mengandungi senarai aktiviti seperti tarikh, aktiviti utama, perincian aktiviti (yang menerangkan secara terperinci daripada aktiviti utama), tempoh jangkaan siap setiap aktiviti dan pegawai yang bertanggungjawab.

v. Menyenaraikan perisian, peralatan dan metodologi untuk ujian penembusan.

vi. Senarai dasar / pekeliling / polisi / piawai yang dirujuk.

vii. Bilangan mesyuarat kemajuan pelaksanaan PTK ICT.

viii. Jadual bayaran kepada pihak ketiga sekiranya berkaitan.

ix. Menyenaraikan kakitangan yang terlibat dalam pelaksanaan PTK ICT.

x. Serahan laporan yang perlu disediakan.

6.2 Serahan laporan yang perlu disediakan dalam pelaksanaan PTK ICT antaranya dan tidak terhad pada perkara berikut:

i. Laporan kemajuan pelaksanaan PTK ICT.

ii. Laporan hasil penemuan PTK ICT.

iii. Laporan cadangan tindakan pengukuhan.

iv. Laporan penilaian ujian semula.

6.3 Laporan hendaklah dibentangkan kepada JPICT atau mana-mana jawatankuasa yang setara untuk pertimbangan dan kelulusan supaya langkah-langkah pengukuhan keselamatan ICT agensi dapat dirancang.

7. SEMAKAN PEMATUHAN DASAR KESELAMATAN ICT / POLISI KESELAMATAN SIBER AGENSI

7.1 Pasukan penilai perlu menyemak pematuhan Dasar Keselamatan ICT (DKICT) / Polisi Keselamatan Siber (PKS) agensi yang berkuatkuasa. Semakan boleh dilaksanakan melalui sesi soal selidik dan temu bual dengan kumpulan sasaran atau membuat pemerhatian pematuhan DKICT / PKS yang berkuat kuasa di agensi.

7.2 Pasukan penilai juga boleh menggunakan contoh borang soal selidik seperti di **Lampiran A** selaras dengan DKICT / PKS agensi yang berkuat kuasa.

7.3 Aktiviti penilaian pematuhan keselamatan fizikal dilaksanakan melalui penilaian dan pemerhatian kepada persekitaran fizikal serta langkah-langkah keselamatan yang berkuat kuasa di agensi. Aktiviti penilaian yang perlu dilaksanakan dan tidak terhad pada perkara berikut:

i. Menyemak wujudnya prosedur / polisi / tatacara sistem kawalan keselamatan fizikal di lokasi penempatan aset ICT agensi seperti Pusat Data, Bilik Pelayan (*server*), ruang kerja dan lain-lain berkaitan. Pemeriksaan keselamatan fizikal adalah mengikut skop yang telah ditetapkan di dalam Arahan Keselamatan (Semakan dan

Pindaan 2017) dan arahan-arahan lain yang berkuatkuasa.

ii. Menemu bual ICTSO untuk memahami amalan dan prosedur keselamatan ICT sedia ada.

iii. Memeriksa Buku Daftar Masuk / Keluar ke Pusat Data / Bilik Pelayan.

iv. Memerhati amalan dan prosedur sebenar keselamatan di laluan keluar masuk ke premis agensi supaya mematuhi peraturan kawalan akses.

v. Melaksanakan ujian penilaian kerentanan ke atas sistem kawalan pemantauan, sistem sokongan dan sistem kawalan akses yang digunakan.

7.4 Menyediakan laporan analisis data ke atas hasil penemuan daripada sesi soal selidik, temu bual dan pemerhatian yang dilaksanakan.

8. UJIAN PENEMBUSAN DAN PENILAIAN KERENTANAN KESELAMATAN RANGKAIAN DAN SISTEM ICT (VAPT)

8.1 Ujian Penembusan dan Penilaian Kerentanan Keselamatan Rangkaian dan Sistem ICT atau *Vulnerability Assessment and Penetration Test* (VAPT) dilaksanakan bagi membantu agensi mengenal pasti kelemahan dan kerentanan yang berpotensi wujud terhadap rangkaian dan sistem ICT yang digunakan oleh agensi. Pelaksanaan VAPT disyorkan pada persekitaran pementasan (*staging environment*) dan bukan di dalam persekitaran produksi (*production environment*).

8.2 Melalui aktiviti ujian VAPT agensi dapat memperkukuhkan keselamatan rangkaian dan sistem ICT dan seterusnya mengelakkan kebocoran data yang boleh menyebabkan kerugian kewangan, menjejaskan reputasi dan keupayaan

agensi untuk berfungsi akibat ancaman siber. VAPT boleh dilaksanakan melalui dua kaedah iaitu ujian penembusan infrastruktur rangkaian dan ujian penembusan aplikasi.

8.3 Pelaksanaan VAPT perlu mengambil kira perkara seperti berikut:

i. Memastikan setiap data untuk digunakan ketika ujian penembusan adalah terjamin keselamatannya dan sesuai digunakan dalam persekitaran ujian.

ii. Menentukan pendekatan dan metodologi untuk ujian penembusan sama ada ujian kotak putih, ujian kotak hitam atau ujian kotak kelabu.

iii. Menyatakan dengan jelas tempoh masa dan gangguan yang mungkin berlaku kepada perkhidmatan sebagai sebahagian daripada keperluan ujian.

8.4 VAPT Infrastruktur Rangkaian

8.4.1 VAPT Infrastruktur Rangkaian hendaklah dilaksanakan dari persekitaran luaran dan persekitaran dalaman. Ini adalah untuk memastikan semua konfigurasi dan kawalan keselamatan infrastruktur rangkaian diuji secara menyeluruh dan berada pada tahap optimum seperti yang telah ditetapkan oleh agensi.

8.4.2 Penilaian kerentanan (*vulnerability assessment*) dilaksanakan kepada infrastruktur rangkaian berdasarkan teknik eksploitasi secara *intrusive* dan *non-instrusive* untuk mengenal pasti kerentanan dan kelemahan konfigurasi infrastruktur rangkaian.

8.4.3 Pengumpulan maklumat dan *Attack Surface Analysis.*

i. Melaksanakan pengumpulan maklumat infrastruktur rangkaian melalui aktiviti tinjauan rangkaian dan teknik pengumpulan maklumat yang bersesuaian bagi pelaksanaan ujian secara luaran.

ii. Pelaksanaan ujian secara dalaman dilaksanakan melalui pengumpulan profil infrastruktur rangkaian dan maklumat peralatan yang boleh diperoleh dan tidak terhad pada kaedah berikut:

- Semakan reka bentuk rangkaian.
- Imbasan rangkaian.
- *Network packets capturing* untuk mengesan protokol dan perkhidmatan yang diaktifkan.

iii. Mengenal pasti *Attack Surface* yang wujud dalam rangkaian ICT agensi.

8.4.4 Aktiviti ujian VAPT infrastruktur rangkaian adalah seperti berikut:

i. Menyediakan perancangan dan melaksanakan program eksploitasi kerentanan dan mengesahkan hasil penemuan dengan pembuktian.

ii. Melaksanakan pengimbasan kepada rangkaian menggunakan beberapa perisian penilaian kerentanan (perisian percuma dan berbayar) bagi mengesan perkhidmatan, perisian dan peralatan rangkaian yang terdedah kepada risiko ancaman siber.

iii. Melaksanakan aktiviti mengesan protokol dan perkhidmatan rangkaian yang mungkin terdedah kepada serangan siber seperti *man-in-the-middle,*

brute force, credentials stuffing attacks dan lain-lain.

iv. Menganalisis risiko yang terdedah (*exposure risk*) kepada infrastruktur rangkaian dan maklumat peralatan yang digunakan oleh agensi berdasarkan data dari aktiviti pengumpulan maklumat yang diperolehi dari sumber luaran dan dalaman.

8.4.5 Melaksanakan analisis ke atas hasil penemuan yang ditemui dan berpotensi dieksploit, tidak terhad pada kategori berikut:

i. Penafian Perkhidmatan (*Denial of Service*).
ii. Kata Laluan Lemah.
iii. *Privileged User Access*.
iv. Pendedahan Maklumat Pangkalan Data (*Database Information Disclosure*).
v. *Man-In-The-Middle attack*.
vi. Terdedah kepada *Brute Force*.
vii. Kelemahan konfigurasi perisian / sistem pada peralatan rangkaian.

8.4.6 Menyediakan laporan penilaian secara terperinci dengan mencadangkan penambahbaikan mengikut amalan terbaik industri keselamatan untuk penilaian dan tindakan selanjutnya agensi merangkumi maklumat seperti berikut:

i. Peralatan rangkaian yang berisiko.
ii. Perkhidmatan rangkaian yang berisiko.
iii. Keterangan kerentanan dan tahap keparahan seperti *Common Vulnerabilities and Exposures Identification* (CVE ID) atau *Common Vulnerability Scoring System* (CVSS).
iv. Impak kelemahan dan kerentanan.

v. Teknik dan pengetahuan umum untuk pemetaan analisis ancaman seperti MITRE ATT&CK.
vi. Bukti eksploitasi termasuk tarikh dan masa ujian.
vii. Cadangan tindakan pengukuhan dan rumusan ke atas kelemahan dan kerentanan yang ditemui.

8.5 VAPT Aplikasi

8.5.1 VAPT aplikasi dilaksanakan bagi mengenal pasti, menilai dan memperbaiki kelemahan yang mungkin wujud disebabkan oleh reka bentuk sistem aplikasi dan teknik pengaturcaraan ketika agensi membangunkan sistem aplikasi. Melalui ujian ini agensi dapat mempertingkatkan dan memperkukuhkan kawalan keselamatan kepada sistem aplikasi melibatkan perkhidmatan web, modul aplikasi web, Antaramuka Pengaturcaraan Aplikasi (*Aplication Programming Interface*, API), aplikasi mudah alih dan lain-lain sistem yang terlibat.

8.5.2 VAPT dapat membantu agensi dalam memastikan ciri-ciri keselamatan maklumat dipatuhi supaya capaian dan pengubahsuaian data secara tidak sah, kebocoran data, kerugian kewangan serta reputasi agensi yang terjejas akibat ancaman siber dapat dielakkan.

8.5.3 Terdapat dua kaedah ujian yang perlu dilakukan iaitu Ujian Keselamatan Aplikasi Dinamik (*Dynamic Application Security Test*) dilaksanakan secara ujian kotak hitam dan ujian kotak kelabu manakala Ujian Keselamatan Aplikasi Statik (*Static Application Security Test*) dilaksanakan secara ujian kotak putih.

8.5.4 Ujian Keselamatan Aplikasi Dinamik adalah satu metodologi bagi menganalisis aplikasi dalam keadaan dinamik, *running state* semasa fasa pengujian atau fasa pengoperasian. Simulasi serangan ke atas aplikasi dilaksanakan bagi menilai tindak balas aplikasi dan

menentukan ia mempunyai kelemahan atau tidak. Senarai kelemahan umum sistem aplikasi boleh merujuk kepada senarai kerentanan semasa seperti *Open Web Application Security Project* (OWASP) *Top 10 Vulnerabilities*, OWASP *API Security Top 10* dan OWASP *Mobile Top 10*.

8.5.5 Ujian Keselamatan Aplikasi Statik ialah pendekatan ujian yang dilaksanakan secara ujian kotak putih untuk mengenal pasti kelemahan keselamatan di dalam kod sumber, *bytecode* atau *binary code.*

8.5.6 Pengumpulan maklumat bagi aktiviti ujian keselamatan aplikasi dinamik boleh dilaksanakan melalui semakan dokumentasi sistem, carta alir sistem dan capaian yang digunakan untuk mengakses sistem bagi mengenal pasti komponen dan modul yang digunakan manakala untuk aktiviti ujian keselamatan aplikasi statik kod sumber perlu disediakan oleh pemilik sistem bagi melaksanakan ujian analisis kod sumber.

8.5.7 Mencadangkan teknik serangan yang akan digunakan terhadap sistem aplikasi dalaman, web dan mudah alih mengikut kategori risiko dan kelemahan aplikasi seperti OWASP *Top 10 Vulnerabilities*, OWASP *API Security Top 10* dan OWASP *Mobile Top 10*.

8.5.8 Aktiviti VAPT aplikasi adalah seperti berikut:

i. Melaksanakan pengimbasan aplikasi dinamik dengan menggunakan beberapa perisian pengimbas keselamatan aplikasi dinamik (perisian terbuka dan berbayar) untuk mengenal pasti komponen dan perkhidmatan sistem aplikasi yang terdedah kepada serangan dan lapuk (*outdated*).

ii. Pelaksanaan pengimbasan aplikasi statik pula, dijalankan dengan menganalisis kod sumber menggunakan perisian pengimbasan kod secara automatik. Manakala untuk semakan kod sumber secara manual pasukan penilai boleh merujuk kepada garis panduan yang dibangunkan oleh *OWASP Code Review Guide*. Ini adalah untuk mengesahkan sama ada amalan pengaturcaraan yang selamat digunakan di dalam sistem aplikasi agensi.

8.5.9 Melaksanakan analisis lengkap kepada ujian VAPT aplikasi yang telah dijalankan. Analisis ini perlu menerangkan ujian kerentanan, kategori risiko yang dijumpai dan risiko keselamatan berdasarkan rujukan pemodelan ancaman sistem aplikasi seperti *OWASP Top 10 Vulnerabilities* dan *OWASP API Security Top 10* yang terkini.

8.5.10 Menyenaraikan hasil penemuan menggunakan format *Risk Severity Matrix* berdasarkan standard amalan terbaik industri keselamatan.

8.5.11 Menyediakan laporan penilaian penuh yang merangkumi maklumat untuk penilaian dan tindakan agensi terhadap peningkatan keselamatan, ancaman pertahanan dan tindak balas seperti berikut:

i. Maklumat sistem aplikasi yang terjejas.
ii. *Port* dan perkhidmatan sistem aplikasi yang terjejas.
iii. Sistem aplikasi yang berisiko.
iv. *Common Vulnerabilities and Exposures Identification* (CVE ID).
v. *Common Vulnerability Scoring System* (CVSS).
vi. Keterangan kerentanan dan tahap keparahan.
vii. Teknik dan pengetahuan umum (MITRE ATT&CK) untuk pemetaan analisis ancaman.

viii. Bukti eksploitasi termasuk tarikh dan masa pelaksanaan.
ix. Cadangan untuk pemulihan kerentanan dan kelemahan yang ditemui.

9. PENILAIAN KESELAMATAN DAN KERENTANAN SISTEM PENGOPERASIAN HOS

9.1 Penilaian hos adalah satu aktiviti mencari kelemahan konfigurasi dan kerentanan keselamatan di sistem pengoperasian (*operating system*) yang dipasang pada pelayan dan komputer peribadi seperti konfigurasi kebenaran fail tidak selamat (*insecure file permissions*), pepijat (*bugs)*, pintu belakang (*backdoor*) dan lain-lain perisian yang sepatutnya tidak dipasang.

9.2 Penilaian ini dapat mengenal pasti kelemahan konfigurasi dan kerentanan sistem pengoperasian hos yang digunakan di agensi dan seterusnya melaksanakan tindakan penambahbaikan dan pengukuhan keselamatan kepada hos yang terlibat.

9.3 Menyenaraikan bilangan hos dan maklumat tambahan seperti nama hos, maklumat alamat IP, salinan maklumat konfigurasi hos yang sedang digunakan untuk aktiviti penilaian.

9.4 Semakan konfigurasi sistem pengoperasian hos dan penilaian kerentanan hendaklah meliputi tetapi tidak terhad pada perkara berikut:

i. Analisis jurang (*gap analysis*) kepada amalan terbaik industri keselamatan hos.
ii. Kemas kini sistem pengoperasian dan kemas kini perisian.
iii. Konfigurasi sistem fail.
iv. *Secure boot setting*.
v. Penetapan proses sistem (*system process setting*).

vi. Tetapan perkhidmatan sistem pengoperasian hos (*operating system services setting*).
vii. Konfigurasi tembok api (*firewall)*.
viii. Log dan pengauditan.
ix. Akses sistem, pengesahan dan kebenaran.
x. Tetapan pengguna dan kumpulan (*user and group settings*).
xi. Kebenaran fail sistem (*system file permission*).
xii. Penilaian kelemahan sistem pengoperasian hos untuk kerentanan yang telah diketahui dan sistem yang sudah lapuk.

9.5 Menyediakan laporan analisis ke atas hasil penemuan daripada aktiviti penilaian keselamatan dan kerentanan sistem pengoperasian hos yang dilaksanakan.

9.6 Mencadangan tindakan pengukuhan yang boleh dilaksanakan berdasarkan kelemahan dan kerentanan yang ditemui.

10. PENILAIAN KONFIGURASI DAN KERENTANAN PERALATAN KESELAMATAN

10.1 Penilaian konfigurasi dan kerentanan peralatan keselamatan adalah aktiviti yang dilakukan untuk menyemak dan menentukan peralatan rangkaian yang digunakan oleh agensi berdasarkan konfigurasi amalan terbaik industri keselamatan dan tidak mengandungi sebarang kelemahan dan kerentanan yang boleh dieksploitasi oleh penggodam.

10.2 Penilaian ini dapat mengenal pasti kelemahan konfigurasi dan kerentanan peralatan keselamatan yang digunakan di agensi dan seterusnya mengenalpasti tindakan penambahbaikan serta pengukuhan kepada keselamatan peralatan yang digunakan.

10.3 Menentukan dan menyenaraikan bilangan peralatan keselamatan seperti nama peralatan, jenis peralatan, maklumat alamat IP dan maklumat konfigurasi peralatan keselamatan yang sedang digunakan untuk aktiviti penilaian.

10.4 Melaksanakan aktiviti semakan (*cross check*) konfigurasi peralatan keselamatan yang digunakan oleh agensi berdasarkan amalan terbaik industri secara automatik menggunakan *tools* / aplikasi yang bersesuaian atau secara manual.

10.5 Aktiviti penilaian konfigurasi peralatan keselamatan dan kerentanan hendaklah meliputi tetapi tidak terhad pada perkara berikut:

i. Keselamatan operasi (*operation security*).
ii. Kawalan capaian (*access control*).
iii. Memastikan peralatan mengaktifkan fungsi log dan *audit trail.*
iv. Salinan pendua (*backup).*
v. Semakan penggunaan *firmware* untuk mengesan kerentanan yang diketahui dan tidak diketahui serta sistem yang sudah lapuk.
vi. Memastikan polisi yang digunakan adalah mengikut amalan terbaik industri keselamatan dan mematuhi polisi dasar keselamatan agensi.
vii. Mempunyai dan menyimpan rekod polisi dan konfigurasi.

10.6 Menyediakan laporan analisis ke atas hasil penemuan daripada aktiviti penilaian konfigurasi dan kerentanan peralatan keselamatan yang dilaksanakan.

10.7 Mencadangkan tindakan pengukuhan yang boleh dilaksanakan berdasarkan kerentanan dan kelemahan yang ditemui.

11. PENILAIAN KESELAMATAN PANGKALAN DATA (*DATABASE SECURITY ASSESSMENT*)

11.1 Penilaian keselamatan pangkalan data adalah aktiviti penilaian bagi mengenalpasti kelemahan dan kerentanan yang mungkin wujud pada perisian serta konfigurasi di pangkalan data yang membolehkan percubaan yang tidak dibenarkan melalui pengubahsuaian fungsi dan logik pengaturcaraan.

11.2 Matlamat ujian ini adalah untuk mendapatkan maklumat teknikal terperinci mengenai konfigurasi sistem pangkalan data yang telah digunakan berbanding penanda aras dan piawaian standard industri yang berkaitan bagi mengesan kelemahan yang wujud.

11.3 Penilai perlu melaksanakan penilaian teknikal secara menyeluruh melibatkan konfigurasi sistem pangkalan data mengikut dasar keselamatan agensi.

11.4 Menentukan dan menyenaraikan bilangan, perisian, maklumat alamat IP dan maklumat konfigurasi pangkalan data yang sedang digunakan di agensi.

11.5 Aktiviti utama penilaian keselamatan pangkalan data hendaklah meliputi tetapi tidak terhad pada perkara berikut:

i. Analisis jurang (*gap analysis*) kepada amalan terbaik industri keselamatan pangkalan data.
ii. Konfigurasi umum pangkalan data seperti *database version* dan tahap kemaskini / tampalan keselamatan (*security patch level*).
iii. Konfigurasi fail sistem pangkalan data.
iv. Kebenaran capaian pangkalan data secara umum dan maklumat sensitif.
v. Pengauditan dan log.

vi. Pengesahan dan kebenaran capaian pengguna dan pentadbir (*access right*).
vii. *Database communication services (listener / SQL Agent / UDP).*
viii. Replikasi pangkalan data (*data replication*).
ix. Penilaian kerentanan perisian pangkalan data untuk kerentanan yang diketahui dan tidak diketahui serta sistem yang sudah lapuk.

11.6 Menyediakan laporan analisis ke atas hasil penemuan daripada aktiviti penilaian keselamatan pangkalan yang dilaksanakan.

11.7 Mencadangkan tindakan pengukuhan yang boleh dilaksanakan berdasarkan kerentanan dan kelemahan yang ditemui.

12. PENILAIAN KESELAMATAN PENGKOMPUTERAN AWAN

12.1 Ujian penembusan dan penilaian kerentanan perkhidmatan pengkomputeran awan merupakan aktiviti yang dilaksanakan untuk mengesan dan mengenal pasti sebarang kelemahan dan kerentanan yang mungkin wujud pada sistem aplikasi dalam persekitaran pengkomputeran awan. Tindakan pengukuhan seterusnya dapat dilaksanakan terhadap hasil penemuan kelemahan dan kerentanan yang ditemui supaya risiko pelanggaran dan kebocoran data dapat dikurangkan.

12.2 **Perbezaan ujian penembusan di premis dan pengkomputeran awan.**

Perbezaan yang di antara dua ujian ini adalah seperti berikut:

Bil.	Ujian Penembusan di Premis	Ujian Penembusan di Pengkomputeran Awan
1.	Boleh dilaksanakan kepada semua jenis infrastruktur rangkaian dan sistem	Pelaksanaan terhad kepada jenis model perkhidmatan dan model

Bil.	Ujian Penembusan di Premis	Ujian Penembusan di Pengkomputeran Awan
	aplikasi ICT tanpa sebarang sekatan.	pelaksanaan yang dilanggan melalui CSP.
2.	Mengenal pasti kelemahan dan kerentanan secara menyeluruh kepada infrastruktur rangkaian dan sistem aplikasi ICT yang terdapat di premis agensi.	Memfokuskan kepada mengenal pasti kelemahan dan kerentanan yang boleh dieksploitasi oleh penggodam.
3.	Agensi menentukan sendiri polisi dan skop bagi pelaksanaan ujian penembusan.	CSP mempunyai polisi dalam melaksanakan ujian penembusan tersendiri yang perlu dipatuhi oleh agensi sebelum melaksanakan sebarang aktiviti ujian penembusan dan kerentanan.

12.3 **Keperluan Pelaksanaan Ujian Penembusan dan Penilaian Kerentanan.**

Ujian penembusan dan penilaian kerentanan dilaksanakan untuk mengenal pasti kekuatan dan kelemahan sistem aplikasi dan data yang ditempatkan di pengkomputeran awan. Ujian ini akan dapat membantu agensi untuk:

- Mengenal pasti risiko dan kelemahan pada sistem.
- Mengesan kerentanan yang wujud dan boleh dieksploitasi oleh penggodam.
- Membuktikan potensi kerentanan yang telah ditemui jika ia dieksploitasi.
- Menyediakan laporan lengkap hasil penemuan.
- Menyediakan laporan lengkap cadangan tindakan pengukuhan.

- Melaksanakan tindakan pengukuhan kepada kelemahan dan kerentanan yang ditemui.

12.4 Polisi Keselamatan Perkhidmatan Pengkomputeran Awan oleh CSP

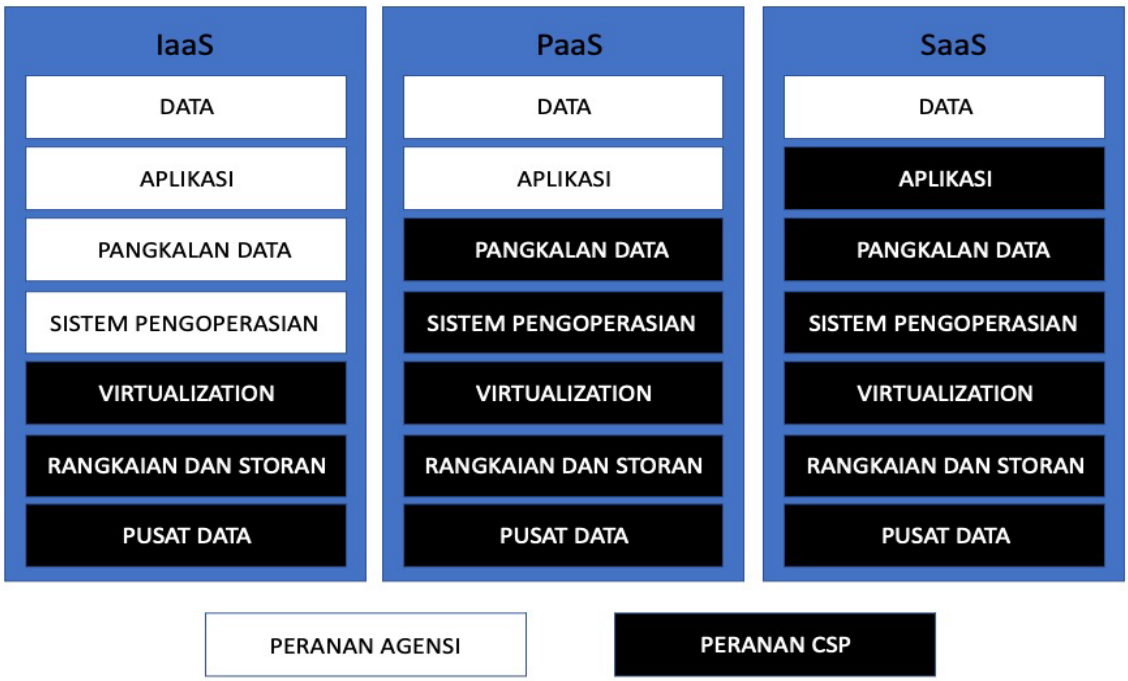
CSP bertanggungjawab memastikan aspek keselamatan dipatuhi di dalam menyediakan perkhidmatan pengkomputeran awan kepada agensi Sektor Awam mengikut piawaian MSO ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 serta peraturan yang sedang berkuat kuasa dari semasa ke semasa seperti dalam perjanjian CFA.

Agensi perlu mengadakan perbincangan bersama pihak MSP dan CSP yang telah dilantik bagi mengenal pasti skop dan aktiviti ujian penembusan dan penilaian kerentanan yang boleh dilaksanakan terhadap perkhidmatan yang telah dilanggan oleh agensi. Ini adalah bagi memastikan tiada sebarang pertindihan aktiviti ujian yang telah dirancang oleh agensi dan tidak melanggar polisi keselamatan yang telah ditetapkan oleh MSP dan CSP.

12.5 Perkongsian Tanggungjawab Keselamatan Pengkomputeran Awan

Agensi dan CSP mempunyai kawalan dan tanggungjawab yang berlainan di perkhidmatan pengkomputeran awan berdasarkan model perkhidmatan pengkomputeran awan yang ditawarkan iaitu Infrastruktur sebagai perkhidmatan, Platform sebagai perkhidmatan dan Perisian sebagai perkhidmatan.

Agihan kawalan dan tanggungjawab CSP dan agensi adalah seperti rajah di bawah berdasarkan perkhidmatan awan yang dilanggan. Agensi bertanggungjawab sepenuhnya kepada data manakala CSP bertanggungjawab kepada infrastruktur perkhidmatan pengkomputeran awan yang disediakan.



Rajah 2: Agihan Kawalan dan Tanggungjawab antara CSP dan Agensi Sektor Awam

Ujian penembusan yang dilaksanakan oleh agensi perlu melihat kepada perkhidmatan yang telah dilanggan dan merangka pelan ujian penembusan dan penilaian kerentanan yang bersesuaian.

12.6 Aktiviti Ujian Penembusan Keselamatan Perkhidmatan Pengkomputeran Awan

i. Agensi boleh melaksanakan aktiviti ujian penembusan dan penilaian kerentanan keselamatan perkhidmatan pengkomputeran awan berdasarkan aktiviti yang disenaraikan tetapi tidak terhad pada perkara berikut:

- **Sistem / Aplikasi:** mengenal pasti sistem / aplikasi, antara muka pengguna dan API yang terlibat untuk pengujian.
- **Capaian data:** mengenal pasti kaedah bagaimana pengujian data akan dilaksanakan melalui sistem / aplikasi atau terus ke pangkalan data atau kedua-duanya.

- **Akses rangkaian:** memeriksa bagaimana reka bentuk rangkaian yang digunakan dapat melindungi data di sistem / aplikasi dan pangkalan data.
- ***Virtualization*:** mengenal pasti bagaimana konfigurasi *virtualization* yang digunakan dapat memisahkan / mengasingkan beban kerja proses dari sistem / aplikasi.
- **Pematuhan:** mengenalpasti semua pematuhan kepada undang-undang dan standard yang perlu oleh CSP dan agensi dalam memastikan perlindungan keselamatan data adalah terjamin.
- **Automasi:** mengenal pasti *tools* (berasaskan awan atau tidak) yang akan digunakan untuk ujian penembusan.
- **Pendekatan:** menentukan sama ada pentadbir aplikasi dan pentadbir perkhidmatan awan perlu terlibat dalam ujian penembusan.

ii. Surat Pekeliling Am Bilangan 2 Tahun 2021 Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) dalam Perkhidmatan Awam telah menetapkan bahawa ujian penembusan ini perlu dilaksanakan ke atas semua elemen pengkomputeran awan berdasarkan kepada konsep perlindungan secara mendalam (*security-in-depth*) meliputi komponen seperti berikut:

- *Web Interface.*
- *Authentication / Authorisation.*
- *Network Services.*
- *Transport Encryption.*
- *Crypto System.*
- *Cloud Interface.*
- *Mobile Interface.*
- *Security Configurability.*
- *Sotfware / Firmware.*
- *Physical Security*.

12.7 **Laporan**

Penilai hendaklah menyediakan laporan penilaian penuh dan tindakan pengukuhan yang perlu dilaksanakan oleh agensi seperti berikut:

i. Maklumat sistem / aplikasi dan data yang terjejas.
ii. Kelemahan konfigurasi pada *virtualization*.
iii. Pematuhan kepada undang-undang dan peraturan yang ditetapkan.
iv. *Common Vulnerabilities and Exposures Identification* (CVE ID).
v. *Common Vulnerability Scoring System* (CVSS).
vi. Keterangan kerentanan dan tahap keparahan.
vii. Teknik dan pengetahuan umum (MITRE ATT&CK) untuk pemetaan analisis ancaman.
viii. Bukti eksploitasi termasuk tarikh dan masa pelaksanaan.
ix. Cadangan tindakan pengukuhan terhadap kelemahan dan kerentanan yang ditemui.

13. *COMPROMISE ASSESSMENT* (CA)

13.1 CA merupakan tindakan pengesanan yang dilaksanakan secara proaktif bagi menilai dan mengukur tahap keselamatan ICT agensi melibatkan ancaman yang diketahui, tidak diketahui dan *zero-day attacks*. Tindakan ini secara tidak langsung mengesahkan bahawa infrastruktur semasa agensi adalah bebas daripada pencerobohan elemen luar yang mungkin berlaku tanpa disedari oleh pentadbir rangkaian dan sistem ICT di agensi.

13.2 CA dapat mengenal pasti sebarang aktiviti pencerobohan yang berlaku di persekitaran semasa atau yang telah berlaku dan masih aktif di agensi merangkumi perkara seperti di bawah:

i. Mengesan aktiviti pengguna yang mencurigakan.
ii. Menganalisis log-log keselamatan.
iii. Mengesan *Indicators of Compromise*.

13.3 Berikut adalah pendekatan dalam melaksanakan CA:

i. Mengenal pasti peralatan infrastruktur rangkaian dan sistem ICT.
   - menyenaraikan senarai peralatan infrastruktur dan sistem ICT yang sensitif dan berisiko tinggi yang mungkin menjadi sasaran serangan.

ii. Pengumpulan Artifak
   - mengumpul artifak daripada infrastruktur rangkaian dan sistem ICT yang telah dikenal pasti. Pengumpulan artifak yang melibatkan log daripada peralatan rangkaian, peralatan keselamatan rangkaian, pangkalan data dan sistem aplikasi yang terlibat.

   - Aktiviti pengumpulan artifak boleh dilaksanakan berdasarkan metodologi kitar hayat serangan seperti di **Lampiran B**.

iii. Menganalisis Artifak

   - Analisis secara mendalam kepada artifak yang telah dikumpul bagi mengenal pasti aktiviti penggodaman, menganalisis jenis serangan, pendekatan serangan yang diguna pakai oleh penggodam dan kelemahan yang boleh menyebabkan berlakunya penggodaman.

   - Pasukan penilai perlu melihat setiap butiran artifak secara terperinci yang menunjukkan sebarang kemungkinan cubaan pencerobohan dan aktiviti penggodaman yang telah berlaku dan mungkin masih aktif.

   - Sekiranya penggodaman berjaya dikesan pasukan penilai perlu melihat setakat mana penggodaman telah berlaku dan kesan kepada agensi.

13.4 Menyediakan laporan analisis data yang melibatkan hasil penemuan dari semakan artifak infrastruktur rangkaian, sistem ICT dan *end-point.*

13.5 Mencadangkan tindak balas dan pengukuhan yang perlu dilaksanakan terhadap sebarang hasil penemuan aktiviti penggodaman, menghentikan akses tanpa kebenaran yang ditemui dan menghapuskan semua *back-door* yang telah dikenal pasti.

14. ANALISIS HASIL PENEMUAN AKTIVITI PTK ICT

14.1 Pasukan penilai perlu menyediakan analisis ke atas hasil penemuan dan merumuskan semua aktiviti PTK ICT yang telah dilaksanakan berdasarkan aktiviti yang dinyatakan dalam garis panduan ini seperti berikut:

i. Mengklasifikasikan dan mengkategorikan kelemahan dan kerentanan mengikut aktiviti penilaian berdasarkan **Para 7 hingga Para 13**.
ii. Mengenal pasti persamaan atau percanggahan maklumat yang ditemui.
iii. Mengesahkan hasil penemuan kelemahan dan kerentanan supaya langkah pengukuhan yang tepat dapat dilaksanakan.
iv. Membuat perbandingan dengan amalan terbaik industri.

15. LAPORAN

15.1 Penyediaan laporan yang komprehensif perlu disediakan selepas selesai melaksanakan ujian penembusan. Jadual di bawah merupakan contoh format rujukan sebagai panduan penyediaan laporan PTK ICT. Sebarang maklumat tambahan boleh dimasukkan ke dalam laporan ini berdasarkan keperluan agensi dan pihak syarikat yang dilantik sekiranya ada.

Perkara	Keperluan Minimum
Ringkasan Eksekutif	Ringkasan keseluruhan (*high level*), skop, aktiviti dan hasil penemuan utama daripada aktiviti PTK ICT.
Skop kerja	Menyatakan dengan lengkap skop dan aktiviti yang telah dipersetujui dan dilaksanakan melibatkan aktiviti penilaian berdasarkan **Para 7 hingga Para 14**.
Metodologi yang digunakan	Perincian dan keterangan mengenai metodologi yang digunakan bagi pelaksanaan PTK ICT.
Had (*limitations*)	Menyatakan sebarang sekatan / had yang dikenakan ke atas ujian seperti waktu ujian yang ditetapkan, sekatan capaian, keperluan ujian khas untuk sistem warisan (*legacy system*) dan sebagainya.
Penemuan	i. Bagaimana capaian kepada infrastruktur rangkaian dan sistem ICT, hos, perisian dan sebagainya dapat dimanfaatkan menggunakan setiap kerentanan yang ditemui. ii. *Proof of Concept* dan bukti eksploitasi. iii. Menjelaskan kedudukan risiko / tahap keparahan setiap kerentanan. iv. Membuktikan sasaran yang terjejas. v. *Common Vulnerabilities and Exposures* (CVE), *Common Weakness Enumeration* (CWE), *Open Source Vulnerability Database* (OSVDB) dan lain-lain rujukan kelemahan yang digunakan oleh pasukan penilai. vi. Penerangan lengkap mengenai hasil penemuan dari aktiviti ujian penembusan yang ditemui. vii. Status pengukuhan yang boleh dilaksanakan. viii. Lain-lain perkara yang perlu dilaporkan.

Perkara	Keperluan Minimum
Alat (*tools*) / perisian yang digunakan	Alat, perisian dan teknik yang digunakan.
Appendix / Lampiran	Semua teknik pengumpulan perisikan dan pemodelan ancaman yang digunakan serta bahan rujukan yang digunakan untuk penulisan laporan.

Jadual 3: Cadangan templat penyediaan laporan

16. TINDAKAN PENGUKUHAN

16.1 Penilai hendaklah menyerah dan membentangkan laporan cadangan tindakan pengukuhan yang perlu dilaksanakan berdasarkan kelemahan dan kerentanan yang dikenal pasti.

16.2 Pemilik rangkaian dan sistem ICT hendaklah melaksanakan penambahbaikan atau pengukuhan terhadap sebarang kelemahan berisiko kritikal, tinggi dan sederhana yang dilaporkan oleh pasukan penilai dalam tempoh masa yang ditetapkan sebelum fasa pasca penilaian.

16.3 Tindakan pengukuhan boleh dilaksanakan berdasarkan cadangan yang disediakan oleh pasukan penilai seperti di bawah:

i. Cadangan penambahbaikan bagi mematuhi DKICT / PKS agensi.
ii. Cadangan langkah pengukuhan kerentanan keselamatan rangkaian dan sistem ICT.
iii. Cadangan penambahbaikan reka bentuk infrastruktur rangkaian ICT, jika perlu.
iv. Cadangan langkah pengukuhan keselamatan dan kerentanan bagi sistem pengoperasian hos.

v. Cadangan pengukuhan konfigurasi dan kerentanan peralatan keselamatan.
vi. Cadangan pengukuhan keselamatan pangkalan data.
vii. Cadangan pengukuhan keselamatan perkhidmatan pengkomputeran awan.
viii. Cadangan pengukuhan hasil penemuan CA.
ix. Laporan PTK ICT yang menyatakan dan menerangkan secara terperinci kelemahan, risiko dan impak keselamatan maklumat serta cadangan penyelesaian yang boleh dilaksanakan.
x. Cadangan untuk penambahbaikan keselamatan jangka pendek dan jangka panjang.

16.4 Menyediakan maklumat untuk input dalam membantu membuat keputusan tentang tahap kerumitan melibatkan teknikal, kos dan tempoh pemulihan serta sumber yang diperlukan kepada pihak pengurusan.

16.5 Sokongan dan komitmen penuh daripada pasukan projek PTK ICT, pengurus dan pentadbir sistem di agensi untuk melaksanakan aktiviti pengukuhan bagi kelemahan dan kerentanan yang telah dikenal pasti dalam masa yang ditetapkan. Pengurus dan pentadbir sistem hendaklah merancang dan melaksanakan pengukuhan kerentanan dengan teliti berdasarkan tahap risiko, kerumitan melibatkan teknikal, tempoh dan sumber sedia ada.

17. FASA PASCA PENILAIAN (*POST ASSESSMENT*)

17.1 Setelah aktiviti pemulihan selesai dilaksanakan, pasukan penilai hendaklah menjalankan ujian pasca penilaian untuk mengesahkan dan memastikan kelemahan dan kerentanan yang dilaporkan telah berjaya dipulihkan.

17.2 Menyediakan laporan ujian pasca penilaian yang merangkumi maklumat seperti berikut:

i. Laporan ujian pasca penilaian yang menyatakan dengan jelas perkara seperti berikut:

- Status kerentanan terkini.
- Aktiviti pemulihan oleh pemilik sistem.
- Bukti ujian dan eksploitasi, termasuk tarikh dan masa pelaksanaan.
- Cadangan tambahan untuk pemulihan kerentanan, jika diperlukan.

18. KAEDAH PELAKSANAAN / PENDEKATAN PTK ICT

18.1 Agensi 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.

18.2 Agensi boleh melaksanakan PTK ICT dengan menggunakan salah satu dari pendekatan berikut iaitu sama ada:

a. Kepakaran Sendiri (*In-House*)

Agensi boleh melaksanakan sendiri PTK ICT dengan melantik pegawai yang memenuhi syarat-syarat berikut:

i. Memastikan Pegawai Teknologi Maklumat yang bertanggungjawab melaksanakan PTK ICT mempunyai pengetahuan dan kemahiran dalam pengoperasian dan komunikasi ICT.

ii. Memastikan pegawai berkenaan mempunyai kemahiran dalam aspek-aspek melaksanakan ujian penembusan ke atas rangkaian dan sistem ICT.

iii. Memastikan pegawai berkenaan menjalani latihan ujian penembusan PTK ICT yang ditawarkan oleh

pusat latihan yang bertauliah dalam bidang keselamatan siber.

b. Melantik Pihak Ketiga (*Outsource*)

Agensi boleh mendapat perkhidmatan pihak ketiga yang bertauliah dan memenuhi syarat-syarat yang ditetapkan oleh Kerajaan seperti berikut:

i. Berdaftar dengan Kementerian Kewangan di bawah pecahan kepala berikut:

- 210107: ICT Security and Firewall, Encryption, PKI, Anti-Virus
- 242600: Pengurusan Keselamatan

ii. Dipersijilkan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001.

iii. Pasukan pelaksana PTK ICT hendaklah mempunyai pensijilan yang diiktiraf peringkat antarabangsa dalam bidang pengujian keselamatan ICT merangkumi rangkaian, sistem ICT atau setara.

iv. Tidak mempunyai apa-apa hubungan dan perkaitan dengan syarikat pembekal yang membangunkan, menyelenggara dan membekalkan infrastruktur rangkaian dan sistem ICT di agensi. Agensi boleh menggunakan panduan seperti di **Lampiran C** untuk membuat pemilihan pembekal pihak ketiga yang berkelayakan.

v. Hendaklah memastikan semua arahan, dasar dan pekeliling berkaitan yang berkuat kuasa dipatuhi.

vi. Menandatangani Borang Perakuan Akta Rahsia Rasmi 1972 [Akta 88] seperti di Lampiran “E” dan Lampiran “F” di dalam Arahan Keselamatan (Semakan dan Pindaan 2017).

vii. Lulus tapisan keselamatan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).

19. JAMINAN KERAHSIAAN, INTEGRITI DAN KETERSEDIAAN (*CONFIDENTIALITY, INTEGRITY AND AVAILABILITY*)

19.1 Agensi hendaklah memastikan perkara yang berkaitan CIA dipatuhi sebelum, semasa dan selepas program PTK ICT dilaksanakan. Ini adalah bagi memastikan semua maklumat sensitif dan rahsia rasmi sentiasa terperingkat terpelihara, dilindungi dan dikendalikan mengikut arahan dan pekeliling yang berkuat kuasa.

i. **Kerahsiaan** ialah semua maklumat sensitif yang dikongsi hendaklah diuruskan dengan betul oleh pasukan penilai / pihak ketiga yang dilantik.

ii. **Integriti** ialah pasukan penilai hendaklah memastikan maklumat sensitif dilindungi daripada pengubahsuaian yang tidak dibenarkan.

iii. **Ketersediaan** ialah pasukan penilai hendaklah menguruskan ujian PTK ICT dalam persekitaran terkawal untuk memastikan tiada gangguan kepada operasi di agensi dan operasi sistem.

20. PENUTUP

20.1 Garis Panduan PTK ICT Sektor Awam ini menjelaskan langkah-langkah penilaian serta memperincikan aktiviti-aktiviti yang perlu dilaksanakan dalam menilai tahap keselamatan ICT bagi membantu agensi merancang pengukuhan yang bersesuaian.

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

SENARAI LAMPIRAN

Lampiran A : Templat Borang Soal Selidik Bagi Tujuan Semakan Dasar Keselamatan ICT / Polisi Keselamatan Siber

Lampiran B : Panduan Pengumpulan Artifak Berdasarkan Metodologi Kitar Hayat Serangan

Lampiran C : Panduan Borang Soal Selidik Menyenarai Pendek Pihak Ketiga yang Bertauliah

LAMPIRAN A

Templat Borang Soal Selidik Bagi Tujuan Semakan Dasar Keselamatan ICT / Polisi Keselamatan Siber

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
BIDANG 1: DASAR / POLISI KESELAMATAN			
1.	Adakah wujud dokumen Dasar Keselamatan ICT / Polisi Keselamatan Siber?		
2.	Bilakah kali terakhir dasar / polisi keselamatan tersebut dikemaskini?		
3.	Adakah dasar / polisi tersebut mengandungi objektif serta skop keselamatan data dan maklumat?		
4.	Adakah Dasar Keselamatan ICT / Polisi Keselamatan Siber mendapat kelulusan di peringkat atasan?		
5.	Adakah dasar / polisi tersebut digunapakai dan disebar kepada semua warga agensi, pembekal, pakar runding, pihak ketiga dan pihak-pihak yang berurusan dengan agensi?		
BIDANG 2: ORGANISASI PENGURUSAN KESELAMATAN ICT			
6.	Adakah wujud Jawatankuasa Pengurusan Keselamatan ICT atau yang setara untuk memberi arah tuju dan sokongan?		
7.	Adakah agensi melantik CDO dan ICTSO untuk merancang, mengurus dan melaksana program keselamatan ICT?		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
8.	Adakah peranan dan tanggungjawab keselamatan maklumat dilaksanakan ke seluruh agensi?		
BIDANG 3: KESELAMATAN SUMBER MANUSIA			
9.	Adakah agensi melaksanakan program kesedaran dan latihan mengenai keselamatan siber kepada warga agensi dari semasa ke semasa atau sekurang-kurangnya sekali setahun?		
10.	Adakah DKICT / PKS agensi diedarkan kepada semua warga agensi untuk dibaca, difahami dan dipatuhi?		
11.	Adakah aset ICT dikembalikan kepada jabatan mengikut peraturan dan membatalkan semua kebenaran capaian kepada warga jabatan yang bertukar dan menamatkan perkhidmatan?		
12.	Adakah pihak pembekal atau pihak ketiga telah menandatangani Borang Perakuan Akta Rahsia Rasmi 1972 [Akta 88] seperti di Lampiran “E” dan Lampiran “F” di dalam Arahan Keselamatan (Semakan dan Pindaan 2017)?		
13.	Adakah pihak pembekal atau pekerja sementara diawasi jika kerja itu melibatkan akses pada kemudahan pemprosesan data?		

NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
BIDANG 4: PENGURUSAN ASET ICT		
14. Adakah pengurusan aset ICT Kerajaan dijalankan selaras dengan peraturan yang ditetapkan?		
15. Adakah wujud proses perolehan dan pemasangan aset ICT?		
16. Adakah agensi menggunakan Sistem Inventori atau Sistem Pengurusan Aset untuk merekod aset-aset ICT Kerajaan?		
17. Adakah maklumat aset ICT dikemaskini ke dalam sistem setiap kali berlaku perubahan?		
18. Adakah aset ICT kerajaan dilupuskan mengikut peraturan, prosedur dan tatacara semasa?		
19. Adakah tindakan keselamatan yang bersesuaian diambil kira untuk melindungi risiko penggunaan peralatan mudah alih dan kerja jarak jauh?		
20. Adakah peralatan ICT yang dipinjam untuk kegunaan rasmi luar pejabat mendapat kelulusan pegawai aset dan direkodkan peminjaman dan pemulangannya?		
21. Adakah aset ICT yang menyimpan maklumat yang mempunyai pengelasan keselamatan telah dilabelkan atau apa-apa kaedah penandaan sebagai “Rahsia Besar”, “Rahsia”, “Sulit” atau “Terhad”?		

NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
22. Adakah terdapat prosedur untuk pengendalian dan pelabelan maklumat terperingkat?		
23. Adakah terdapat prosedur untuk pengurusan media seperti penyimpanan, pemindahan, pertukaran maklumat dan pelupusan media?		
BIDANG 5: KAWALAN CAPAIAN		
24. Adakah agensi mempunyai dasar kawalan akses yang didokumenkan? (Contohnya menyenaraikan siapa yang boleh mengakses maklumat)		
25. Adakah hak capaian pengguna sistem diberikan mengikut peranan dan skop tugas masing-masing?		
26. Adakah pihak pembekal atau pekerja sementara diawasi jika kerja itu melibatkan akses pada kemudahan pemprosesan data?		
27. Adakah hak akses kepada sistem ditarik balik sebaik sahaja pengguna bertukar keluar / bersara / berhenti / tamat perkhidmatan?		
28. Bolehkah data agensi diakses dan dihapuskan tanpa kebenaran rasmi?		
29. Adakah *user root* atau *administrator* dikawal dan dihadkan?		

NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
BIDANG 6. KRIPTOGRAFI		
30. Adakah agensi melindungi kerahsiaan, integriti dan kesahihan maklumat dengan kawalan penggunaan kriptografi?		
31. Adakah terdapat polisi bagi penggunaan kriptografi untuk melindungi maklumat?		
BIDANG 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN		
32. Adakah kawasan lokasi ICT dilindungi daripada sebarang ancaman, risiko pencerobohan, kecurian, kebakaran dan bencana alam?		
33. Adakah terdapat kawalan masuk fizikal ke premis-premis untuk kakitangan dan pelawat seperti pas keselamatan dan buku rekod pelawat?		
34. Adakah peralatan dan kemudahan ICT dilindungi secara fizikal?		
35. Adakah pelayan (*server)* dilindungi dari kegagalan sumber kuasa?		
36. Adakah pusat data diisytiharkan sebagai kawasan atau tempat larangan atau kawasan larangan / tempat larangan di bawah Akta Kawasan Larangan Tempat Larangan 1959 [*Akta 298*]?		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
BIDANG 8: PENGURUSAN OPERASI			
37.	Adakah prosedur operasi didokumenkan dan dikawal?		
38.	Adakah tugas dan tanggungjawab dalam pengujian dan pembangunan sistem diasingkan dari tugas pengoperasian?		
39.	Adakah perisian antivirus dipasang dan beroperasi di dalam semua pelayan, komputer peribadi dan komputer mudah alih?		
40.	Adakah paten perisian antivirus pada peralatan ICT dikemaskini dengan versi terkini?		
41.	Adakah wujud polisi untuk pematuhan bagi perisian berlesen?		
42.	Adakah agensi memasang sistem atau perisian keselamatan untuk melindungi daripada serangan perisian merbahaya / jahat (virus, trojan, malware dsb) ke atas aset ICT?		
43.	Adakah sistem jejak audit (*audit trail*) sistem direkod, dipantau dan disimpan bagi mengesan aktiviti yang dilarang?		
44.	Adakah peralatan ICT seperti komputer, peralatan komunikasi dan yang berkaitan diselenggara mengikut jadual yang ditetapkan?		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
45.	Adakah sandaran (*backup*) ke atas pangkalan data dilakukan secara berkala?		
46.	Adakah ujian pemulihan (*restore)* data dari sandaran dilakukan?		
47.	Sebelum pelupusan komputer dilakukan, adakah data dan maklumat dalam komputer dihapuskan / disanitasi mengikut peraturan yang ditetapkan?		
48.	Adakah agensi memberi peringatan kepada warganya dari semasa ke semasa cara dan amalan asas menjaga keselamatan komputer?		
49.	Adakah agensi mengeluarkan panduan ke atas kerahsiaan dan pengukuhan kata laluan?		
BIDANG 9: PENGURUSAN KOMUNIKASI			
50.	Adakah capaian kepada peralatan rangkaian dikawal dan dihadkan?		
51.	Adakah capaian internet dan sistem aplikasi melalui *firewall?*		
52.	Adakah agensi memasang *Web Content Filtering* untuk menyekat capaian dilarang?		
53.	Adakah penggunaan e-mel rasmi jabatan dipantau untuk memastikan etika penggunaan e-mel dan Internet diamalkan.		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
54.	Adakah jabatan melarang warganya memuat naik, memuat turun dan menyimpan perisian yang tidak berlesen, *online game*, lagu, video dan lain-lain yang menjejaskan prestasi internet?		
55.	Adakah tugas dan tanggungjawab komunikasi diasingkan daripada operasi?		
BIDANG 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM			
56.	Adakah ciri-ciri keselamatan diambil kira dalam perolehan, pembangunan dan penyelenggaraan sistem aplikasi?		
57.	Adakah semua peringkat kitaran pembangunan sistem aplikasi dilindungi bagi memastikan keselamatan maklumat?		
58.	Adakah pembangunan sistem secara pihak ketiga dipantau bagi memastikan mengikut spesifikasi dan perjanjian dipatuhi?		
59.	Adakah terdapat pengurusan perubahan (*Change Request)* pembangunan aplikasi secara pihak ketiga diambil kira dalam perjanjian?		
60.	Adakah penilaian risiko dan pengurusan risiko di guna pakai untuk menganalisis kawalan? (Merujuk kepada pekeliling / garis panduan yang terkini)		

NAMA BIDANG KESELAMATAN	JAWAPAN	CATATAN
61. Adakah terdapat proses permohonan *change request* secara rasmi?		
BIDANG 11: HUBUNGAN PEMBEKAL		
62. Adakah semua pembekal perlu mematuhi keperluan keselamatan maklumat dalam Dasar Keselamatan ICT / Polisi Keselamatan Siber?		
63. Adakah agensi mengambil kira keperluan keselamatan maklumat rantaian bekalan (*supply chain*) untuk menangani risiko perkhidmatan dan kesinambungan bekalan produk ICT dalam kontrak / perjanjian dengan pembekal serta pihak ketiga?		
64. Adakah peruntukan keselamatan ICT dinyatakan di dalam kontrak ICT?		
65. Adakah pihak agensi sentiasa memantau, mengkaji semula dan mengaudit kerja-kerja perkhidmatan pembekal?		
66. Adakah pengurusan perubahan perjanjian dengan pembekal diambilkira dan dinyatakan dalam kontrak?		
BIDANG 12: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT		
67. Adakah agensi mewujud dan menubuhkan Pasukan Tindak Balas Insiden Keselamatan Siber (*Cyber Security Incident Response Team*, CSIRT) dan memaklumkan penubuhan kepada Agensi Keselamatan Siber		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
	Negara (*National Cyber Security Agency*, NACSA)?		
68.	Adakah agensi mempunyai prosedur pengurusan dan pengendalian insiden?		
69.	Adakah insiden keselamatan siber yang berlaku di agensi dilaporkan kepada NACSA?		
70.	Adakah pengguna dimaklumkan mengenai proses pelaporan insiden keselamatan di agensi?		
BIDANG 13: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN (PKP)			
71.	Adakah terdapat proses Pengurusan Kesinambungan Perkhidmatan yang dibangunkan oleh agensi?		
72.	Adakah Pengurusan Kesinambungan Perkhidmatan diuji?		
73.	Adakah latihan dan program kesedaran Pengurusan Kesinambungan Perkhidmatan diadakan kepada warga agensi?		
74.	Adakah agensi mewujudkan kemudahan lewahan (*redundancy)* untuk ketersediaan pemprosesan maklumat yang diuji dari semasa ke semasa?		

NAMA BIDANG KESELAMATAN		JAWAPAN	CATATAN
75.	Adakah agensi mempunyai kemudahan Pusat Pemulihan Bencana (*Disaster Recovery Centre*, DRC) untuk sistem aplikasi kritikal bagi memastikan kesinambungan sistem penyampaian perkhidmatan Kerajaan?		
76.	Apakah tindakan agensi jika ujian Pengurusan Kesinambungan Perkhidmatan gagal?		
BIDANG 14: PEMATUHAN			
77.	Adakah semua warga agensi membaca, memahami dan mematuhi DKICT / PKS dengan menandatangani Akuan Pematuhan Dasar / Polisi Keselamatan?		
78.	Adakah perundangan dan peraturan-peraturan semasa mengenai keselamatan ICT yang berkuatkuasa disebarkan kepada warga agensi untuk dipatuhi?		
79.	Adakah pelanggaran dasar / polisi keselamatan siber agensi dikenakan tindakan tatatertib yang ditetapkan?		
80.	Adakah audit ICT dirancang dan dilaksanakan secara berkala?		

LAMPIRAN B

Panduan Pengumpulan Artifak Berdasarkan Metodologi Kitar Hayat Serangan

Kitar Hayat Serangan *(Attack Life Cycle)*	**Jenis Bukti Artifak**
Tinjauan *(Recon)*	*Threat intelligence feeds*, maklumat perbualan melalui forum web gelap, e-mel pancingan peringkat awal yang digunakan untuk cubaan menceroboh.
Percubaan serangan awal *(Initial Attack)*	Laporan pengguna, log pelayan e-mel, log daripada peralatan keselamatan rangkaian yang digunakan oleh agensi dalam mengesan cubaan pencerobohan.
Mewujudkan kedudukan *(Establish Foothold)*	Log daripada perisian sistem hasad dan log analisis tingkah laku *(behavioral analysis)* daripad*a* hos / pelayan.
Enable persistence	Log yang menunjukkan penggunaan *local privilege accounts* dan penciptaan akaun tambahan yang lain (akan digunakan oleh penggodam untuk masuk semula kemudian).
Tinjauan pengesanan	Log trafik rangkaian dan log tembok api yang menunjukkan aktiviti keluar masuk yang mencurigakan.
Lateral movement	Log kawalan akses pada hos yang dikenal pasti, pemasangan *tools* / perisian penggodaman dan / atau penggunaan *administrative tools* pada hos / pelayan.
Penukaran capaian *(Escalate privileges)*	Log kawalan akses *(Access control)* daripada *central directory system dan* log trafik rangkaian

Kitar Hayat Serangan *(Attack Life Cycle)*	**Jenis Bukti Artifak**
	ke pangkalan data capaian daripada pengguna yang disyaki telah diceroboh.
Mengenal pasti dan akses sasaran (*Identify and access targets)*	Akses luar biasa dan / atau penggunaan sistem, akses keluar ke pelayan *command and control.*
Penyusupan data *(Exfiltration data)*	Saiz data dibawa keluar dari agensi ke destinasi yang mencurigakan *command and control* serta pola transaksi data yang luar biasa.
Penghapusan bukti *(Remove evidence)*	Mencari kemungkinan penggunaan perisian pemadaman selamat (*secure erasure tools)* yang mungkin dipasang di hos dan analisis jurang masa log di hos / pelayan.

LAMPIRAN C

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 syarikat pembekal menawarkan perkhidmatan yang boleh memenuhi keperluan spesifik agensi?			
4.	Adakah syarikat pembekal tiada kaitan dengan syarikat yang membekalkan infrastruktur rangkaian dan sistem ICT di agensi?			
5.	Adakah syarikat pembekal menjalankan penyelidikan sendiri?			
6.	Apakah kelayakan pakar perunding syarikat pembekal? (Sila isi butiran dalam ruang huraian)			
7.	Apakah tahap pengalaman pasukan ujian yang dicadangkan? (Berapa lama telah membuat pengujian dan apakah latar belakang mereka?) (Sila isi butiran dalam ruangan huraian)			
8.	Adakah personel syarikat pembekal ditauliahkan CISSP, CISA atau yang setaraf?			
9.	Adakah personel syarikat pembekal menyumbang kepada industri keselamatan ICT? (Contoh: kertas kerja, penasihat, penceramah umum dan sebagainya)			

BIL	PERKARA	YA	TIDAK	HURAIAN
10.	Adakah vitae kurikulum ahli pasukan yang akan menyertai projek agensi ada disediakan?			
11.	Apakah pendekatan syarikat pembekal dalam projek ini?			
12.	Adakah syarikat pembekal mempunyai metodologi yang standard seperti OSSTM dan OWASP?			
13.	Adakah pembekal pernah melaksanakan Penilaian Tahap Keselamatan di agensi Sektor Awam?			
14.	Bolehkah agensi mendapat contoh laporan Penilaian Tahap Keselamatan daripada pembekal untuk menilai hasil kerja pembekal?			
15.	Adakah syarikat pembekal *outsource* atau menggunakan pihak pembekal yang lain dalam melaksanakan aktiviti PTK?			
16.	Adakah terdapat rujukan dari pelanggan-pelanggan yang berpuas hati dengan perkhidmatan pembekal dalam sektor keselamatan ICT?			
17.	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).			