



**BAHAGIAN AUDIT DALAM  
JABATAN PERDANA MENTERI**

***SELF ASSESSMENT* PENGURUSAN ICT**

**TEMPOH PENILAIAN : 1 JULAI 2017 HINGGA 30 JUN 2018**

Pejabat Yang Dinilai : Bahagian Teknologi Maklumat  
Jabatan .....

Perkara Yang Diaudit : Kawalan Kemudahan ICT

Objektif Audit : Untuk memastikan kawalan kemudahan ICT di  
senggara dengan baik dan sistematik.

Perkara yang dinilai dalam tempoh yang dinyatakan mengenai kawalan kemudahan ICT yang memerlukan maklumat/ulasan/tindakan.

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
1.	Perisian komputer	Memastikan perisian yang diperoleh oleh Jabatan / Bahagian telah diterima dan digunakan selaras dengan pekeliling.  Peraturan : - PK 2/2013 Kaedah Perolehan Kerajaan Lampiran 2.7, Perolehan Perisian Microsoft Oleh Agensi Kerajaan Kecuali Institusi Pendidikan	i. Adakah perisian Microsoft yang digunakan mempunyai lesen yang sah?	Semua perisian Microsoft berlesen yang digunakan hendaklah mempunyai lesen yang sah.	
			ii. Adakah dokumen lesen perisian disimpan dengan baik?	Lesen berbentuk <i>hardcopy</i> atau digital disimpan dengan selamat.	
2.	Pusat Data	Pengurusan dan kawalan keselamatan pusat data  Peraturan : - Pekeliling Am Bil 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan - Garis Panduan MAMPU: <i>Electronic Government Activities Act 2007</i> - Garis Panduan MAMPU: Arahan Teknologi Maklumat Disember 2007 - Garis Panduan Penyimpanan dan Pemeliharaan Rekod Elektronik Sektor Awam - Akta Arkib Negara 2003, Bahagian IV Pengurusan Rekod	i. Adakah pusat data mempunyai kawalan keselamatan dan persekitaran yang baik?	Pusat data mempunyai kawalan akses pintu, kamera litar tertutup(CCTV), kebakaran, susun atur kabel dan sistem penyejukan yang beroperasi dengan baik.	
			ii. Adakah pusat data mempunyai <i>Standard Operating Procedure (SOP)</i> ?	SOP pusat data disediakan.	
			iii. Adakah pusat data mempunyai rekod pegawai keluar masuk?	Rekod keluar masuk manual/elektronik disediakan.	
			iv. Adakah data dibuat <i>backup</i> berjadual?	Backup berjadual secara berkala, harian, mingguan, bulanan dan tahunan.	
			v. Adakah <i>tape backup</i> disimpan di lokasi lain ( <i>Disaster Recovery</i> )?	Tape backup disimpan di luar kawasan pejabat	
			vi. Adakah ujian <i>restoration backup</i> dibuat secara berjadual?	Jadual restoration backup disediakan secara berkala	
			vii. Adakah perkakasan mempunyai penyenggaraan berjadual ( <i>preventive maintenance</i> )?	Semua perkakasan ICT mempunyai jadual PM.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
3.	Pelan Kesenambungan Perkhidmatan	Peraturan : - Surat KP MAMPU 22 Januari 2010 :Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam	i. Adakah agensi merancang dan menyediakan bajet bagi melaksanakan PKP agensi?	Penyediaan bajet PKP.	
			ii. Adakah PKP agensi disediakan?	PKP boleh disediakan secara dalaman atau secara <i>outsourc</i> e.	
			iii. Pengurusan Atasan agensi melantik Peneraju pelaksanaan PKP dan meluluskan penubuhan Pasukan PKP?	Pasukan ditubuhkan dan peneraju dilantik.	
			iv. Adakah proses, peranan dan tanggungjawab ahli pasukan ditentukan dan latihan diberi untuk melaksanakan tugas?	Tugas pasukan dan tanggungjawab ahli ditetapkan.	
			v. Adakah Sesi pendedahan PKP kepada Pengurusan Atasan sekali setahun atau apabila berlaku perubahan Pengurusan Atasan diadakan oleh Koordinator PKP?	Sesi pendedahan dilaksanakan oleh Koordinator PKP sekurang-kurangnya sekali setahun kepada pengurusan.	
			vi. Adakah terma rujukan program PKP diluluskan oleh Jawatankuasa Pemandu PKP?	TOR PKP diluluskan oleh Jawatankuasa Pemandu PKP.	
			vii. Adakah status kemajuan pelaksanaan program PKP dilaporkan dalam mesyuarat Pengurusan Atasan?	Mesyuarat membincangkan kemajuan program PKP.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
4.	Rangkaian	Pengurusan rangkaian dan keselamatan rangkaian dikawal dengan baik.  Peraturan : - Surat Pekeliling Am Bil.3 Tahun 2009 Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam - Surat Arahan Ketua Setiausaha Negara bertarikh 20 Oktober 2006 : Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) Di Agensi-Agensi Kerajaan  - Garis Panduan MAMPU: <i>Standard, Policies and Guidelines - Channels Framework Version 1.0</i> , Ogos 2003	i. Adakah <i>Network Topology</i> dikemas kini?	<i>Network topology</i> hendaklah menunjukkan LAN, WAN, VPN, Firewall, Zon dan subnetting.	
			ii. Adakah keperluan perkakasan mencukupi bagi semua pegawai yang dirangkaikan?	Keperluan perkakasan mencukupi berdasarkan keperluan pegawai melaksanakan tugas.	
			iii. Adakah <i>SOP</i> rangkaian dan infrastruktur ICT disediakan?	<i>SOP</i> rangkaian dan infrastruktur disediakan.	
5.	Keselamatan	Menjelaskan mekanisme pelaporan insiden keselamatan teknologi maklumat dan komunikasi ICT.  Peraturan : - Garis Panduan MAMPU: Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia ( <i>MyMis</i> )(MAMPU 2000)  - Surat Pekeliling Am Bil.3 Tahun	i. Adakah agensi melaksanakan penilaian risiko	Penilaian risiko dilaksanakan sekurang-kurang sekali setahun atau sekiranya terdapat perubahan	
			ii. Adakah agensi melaksanakan penilaian tahap keselamatan rangkaian dan sistem ICT	Penilaian tahap keselamatan rangkaian dan sistem ICT dilaksanakan sekurang-kurang sekali setahun.	
			iii. Adakah pasukan pengendali insiden (CERT) ditubuhkan?	Pasukan CERT ditubuhkan berdasarkan salah satu model CERT yang ditetapkan.	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
		<p>2009 Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam</p> <ul style="list-style-type: none"> <li>- Surat Pekeliling Am Bil. 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam</li> </ul>	iv. Adakah Insiden keselamatan dilaporkan sewajarnya?	Insiden keselamatan dilaporkan dan difailkan.	
		<ul style="list-style-type: none"> <li>- Surat Pekeliling Am Bil. 4 Tahun 2006 : Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (Ict) Sektor Awam</li> </ul>	v. Adakah SOP Pengurusan Pengendalian Insiden Keselamatan ICT CERT Agensi disediakan dan dijadikan rujukan?	SOP pengurusan insiden disediakan selarasa dengan Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam	
		<ul style="list-style-type: none"> <li>- Pekeliling Am Bil.1 Tahun 2001 : Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT)</li> <li>- Pekeliling Am Bil. 3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan</li> <li>- Surat Arahan Ketua Pengarah MAMPU Berkaitan Pengaktifan Fail Log Server.( Rujukan : MAMPU.702-1/1/7 Jld.3(48) bertarikh 23 Mac 2009)</li> </ul>	vi. Adakah fail log server dan aplikasi diaktifkan?	<p>Fail log yang perlu diaktifkan adalah:</p> <ul style="list-style-type: none"> <li>• Fail log sistem pengoperasian</li> <li>• Fail log servis (cth:web, ftp, mel dll)</li> <li>• Fail log aplikasi (audit trail)</li> <li>• Fail log rangkaian (switch, firewall, router, IDS/IPS dll.)</li> </ul>	
6.	Internet dan e-mail	Pengurusan Internet dan E-mel dilaksanakan dan dikawal penggunaannya dengan baik.	i. Adakah pentadbir sistem dilantik bagi menguruskan kawalan akses Internet dan e-mel?	Pentadbir Sistem ICT bertanggungjawab menguruskan kawalan akses internet dan e-mel	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
		Peraturan : - Pekeliling Kemajuan Pentadbiran Awam Bil.1 Tahun 2003 : Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-agensi Kerajaan - Surat Arahan Ketua Pengarah MAMPU: Penggunaan Media Jaringan Sosial Di Sektor Awam (19 Nov. 2009) - Pekeliling Am Bil.3 Tahun 2000 : Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan (ICT) - Dasar Keselamatan ICT(DKICT) 24 Mei 2010 Versi 5.3	ii. Adakah terdapat kawalan akses semasa penggunaan Internet dan e-mel kepada sensitiviti maklumat (eg. pornografi) diberi perhatian?  iii. Adakah program-program kesedaran keselamatan ICT diberikan kepada semua pengguna agar penggunaan Internet dan e-mel dapat dilaksanakan dengan cara yang betul dan selamat.	Senarai sekatan akses penggunaan internet terhadap maklumat sensitif disedia dan dikemaskinikan.  Program Keselamatan ICT telah dihebahkan kepada semua pegawai menggunakan salah satu medium hebahan.	
7.	Laman Web	Pengurusan Laman Web mengikut peraturan pekeling.  Peraturan : - Pekeliling Am Bil.1 Tahun 2006: "Pengurusan Laman Web/Portal Sektor Awam" - Surat Arahan Ketua Pengarah MAMPU: Panduan Penyediaan Berita <i>Online</i> dan Penyiaran Berita <i>Online</i> Di Laman Web/Portal Agensi-Agensi Kerajaan - (11 September 2009)	i. Adakah perkhidmatan dan maklumat agensi yang bersesuaian boleh dicapai melalui myGovernment ?  ii. Adakah struktur tadbir urus laman web/portal di agensi diwujudkan ?  iii. Adakah laman web yang dibangunkan mematuhi prinsip dan ciri-ciri asas laman web/portal;  iv. Adakah agensi melaksanakan tugas-tugas penyenggaraan laman web/portal	Laman web agensi boleh dicapai melalui laman web myGovernment.  Jawatankuasa tadbir urus laman web diwujudkan.  Mematuhi kesemua ciri-ciri asas mandatori  1. Menyenggara server dan memastikannya berfungsi dengan baik 2. Menyemak dan memperbaiki broken	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
				<p>links. Terdapat perisian yang boleh menyemak broken links bagi laman web/portal. Contoh perisian adalah WebExact yang boleh dicapai di alamat berikut:  <a href="http://webxact.watchfire.com/">http://webxact.watchfire.com/</a>.3.            3. Membetulkan kesilapan dan mengemaskini maklumat            4. Memaparkan maklumat terkini.            Contoh:            pekeliling baru, dasar baru dan sebagainya.            5. Menambah kandungan baru.            6. Menambahbaik susun atur, gambar dan grafik.            7. Mengurus pangkalan data laman web/portal.</p>	
			<p>v. Adakah penyediaan dan penyiaran berita <i>online</i> mematuhi garis panduan dan menggunakan teknologi <i>Really Simple Syndicate</i> (RSS)?</p>	<p>Penyiaran berita online disediakan mengikut peraturan dan menggunakan RSS.</p>	
			<p>vi. Adakah langkah-langkah keselamatan laman web/portal agensi dilaksanakan?</p>	<p>Semua ukuran pematuhan di bawah mestilah dipatuhi untuk dikira sebagai Patuh.             Ciri-ciri keselamatan laman web dilaksanakan di mana berkaitan adalah:</p>	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
				<ol style="list-style-type: none"> <li>1. Membezakan kategori maklumat umum dan maklumat dilindungi</li> <li>2. <i>Backup/Restore</i> <ul style="list-style-type: none"> <li>- Menyimpan 3 generasi <i>backup</i></li> <li>- Menyimpan <i>backup</i> di lokasi berlainan</li> </ul> </li> <li>3. Penduaan</li> <li>4. Kawalan keselamatan secara pentadbiran <ul style="list-style-type: none"> <li>- Dasar/Standard/Prosedur /Garis Panduan</li> </ul> </li> <li>5. Kawalan Keselamatan Logikal/Teknikal <ul style="list-style-type: none"> <li>- <i>Firewall Intrusion Prevention System, Intrusion Detection System, Access Control List</i></li> </ul> </li> <li>6. Kawalan Keselamatan Fizikal <ul style="list-style-type: none"> <li>- Kawalan keselamatan rangkaian, aplikasi, <i>patching</i>, pengasingan tugas pelayan web, pengauditan dan AWRS</li> </ul> </li> <li>7. Pengesahan kuasa (<i>authorization</i>)</li> </ol>	



Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
				8. Pengesahan capaian ( <i>authentication</i> ) - Penggunaan ID/Kata laluan - Penggunaan sijil digital/token  9. <i>Encryption</i>  10 . Protokol rangkaian keselamatan - <i>Secure Socket Layer</i>  11. Penamatan sesi.	
8.	Blog	Pelaksanaan Blog Bagi Agensi Sektor Awam mengikut peraturan yang ditetapkan.  Peraturan : - Surat Arahan Ketua Pengarah MAMPU : Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam (17 Julai 2009)	Sekiranya Agensi tidak mempunyai blog sila jawab TB bagi semua soalan no 8.  i. Adakah pasukan pengendali blog dilantik?  ii. Adakah blog mewajibkan pengguna mendaftar nama dan alamat e-mel?  iii. Adakah domain „blog” menggunakan nama agensi?	Pasukan pengendali blog ditubuhkan di bawah jawatankuasa Induk Pengurusan Laman Web/Portal.  Blog mesti mewajibkan pengguna mendaftar nama dan e-mel.  Blog hendaklah menggunakan alamat domain mengandungi : domain“blog.<agensi>.gov.my atau <nama blog>blog.<agensi>.gov.my	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
			iv. Adakah kriteria mandatori blog dipatuhi?	Kriteria mandatori merangkumi: <ol style="list-style-type: none"> <li>1. Papar perkataan „Blog Rasmi“;</li> <li>2. Menggunakan jata dan logo rasmi jabatan;</li> <li>3. Mengandungi pengenalan blog agensi;</li> <li>4. Kandungan hanya perkara berkaitan bidang kuasa agensi;</li> <li>5. Mempunyai „<i>disclaimer</i>“ dan „dasar privasi“ dan „dasar keselamatan“;</li> <li>6. Memaparkan „hak cipta terpelihara“</li> <li>7. Memaparkan maklumat perhubungan Pasukan Pengendali Blog seperti alamat e-mel dan nombor telefon;</li> <li>8. Mempunyai pautan blog yang telah diarkib.</li> <li>9. Ada pautan ke laman web agensi dan pautan ke blog daripada laman web agensi</li> </ol>	
			v. Adakah blog memastikan larangan kandungan dipatuhi?	Larangan kandungan yang dilarang adalah: <ol style="list-style-type: none"> <li>1. Pautan ke iklan komersial.</li> <li>2. Mengandungi maklumat rahsia dan isu sensitif perkauman, politik dan agama.</li> <li>3. Kandungan menjejaskan imej kerajaan dan bercanggah dengan dasar kerajaan;</li> <li>4. Kandungan berunsur fitnah,</li> </ol>	

Bil.	Dokumen/ Perkara Diaudit	Kriteria Audit	Senarai Semak/ Prosedur Audit	Ukuran Pematuhan	Status Pematuhan (√/ X/TB)
				hasutan dan menyalahi undang-undang. 5. Pautan kepada blog/laman web yang tidak berkaitan.	
9.	Perkhidmatan Kios dan SMS	<p>Pengurusan Perkhidmatan Kios dan SMS di senggara dengan teratur.</p> <p>Peraturan :</p> <ul style="list-style-type: none"> <li>- Pekeliling Kemajuan Pentadbiran Awam Bil. 2 Tahun 2008: Panduan Menambah Baik Penyampaian Perkhidmatan Menerusi Penggunaan Kios Di Agensi-agensi Kerajaan</li> <li>- Pekeliling Kemajuan Pentadbiran Awam Bil. 3 Tahun 2008: Panduan Penambahbaikan Sistem Penyampaian Perkhidmatan Kerajaan Menerusi Perkhidmatan Pesanan Ringkas (SMS)</li> </ul>	<p>i. Adakah kajian persekitaran, analisis keperluan dan Penyediaan <i>System Requirement Study (SRS)</i> dijalankan sebelum melaksanakan perkhidmatan secara kios?</p> <p>ii. Adakah program promosi dilaksanakan bagi memperkenalkan penggunaan sistem kios dan/atau SMS?</p> <p>iii. Adakah penilaian bagi menentukan keberkesanan perkhidmatan menerusi kios dan/atau SMS dilaksanakan</p> <p>iv. Adakah Jawatankuasa Pemandu ICT atau Jawatankuasa lain yang bersesuaian mentadbir urus penggunaan sistem kios dan SMS?</p>	<p>Dokumen kajian dan SRS disediakan.</p> <p>Program kesedaran dan penggunaan kios dan/atau SMS telah dihebahkan .</p> <p>Program penilaian dilaksanakan bagi menilai keberkesanan perkhidmatan menerusi dan/atau dan</p> <p>Pelaksanaan kios dan SMS dilaporkan dalam mesyuarat JPICT atau Jawatankuasa lain yang bersesuaian.</p>	

## Nota :

T.B.	-	Tidak Berkenaan
ICT	-	<i>Information Communication Technology</i>
SOP	-	<i>Standard Operating Procedure</i>
CIO	-	<i>Chief Information Officer</i>
SMS	-	<i>Short Message Service</i>