UNIVERSITI PUTRA MALAYSIA

AGRICULTURE • INNOVATION • LIFE

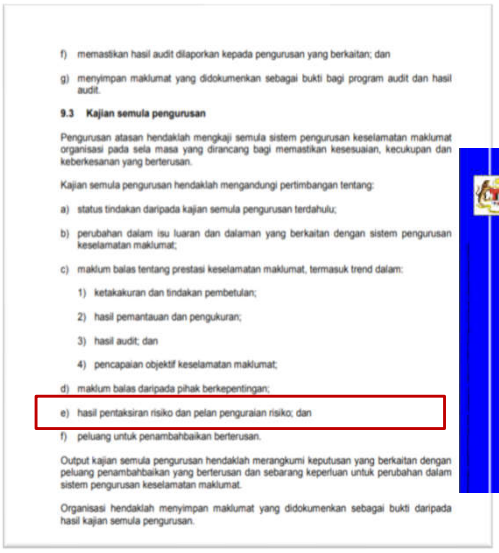
Agenda 8.2

PENILAIAN RISIKO DAN PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

LAPORAN TIMBALAN WAKIL PENGURUSAN ISMS

LATAR BELAKANG

Laporan penilaian risiko dan pelan pemulihan risiko keselamatan maklumat merupakan salah satu input berkaitan maklum balas prestasi keselamatan maklumat yang perlu dilaporkan semasa Mesyuarat Kajian Semula Pengurusan bagi memenuhi keperluan **Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) MS ISO/IEC 27001:2013 Klausa 9.3 (e) berhubung hasil pentaksiran risiko dan pelan penguraian risiko**



f) memastikan hasil audit dilaporkan kepada pengurusan yang berkaitan; dan

g) menyimpan maklumat yang didokumenkan sebagai bukti bagi program audit dan hasil audit.

9.3 Kajian semula pengurusan

Pengurusan atasan hendaklah mengkaji semula sistem pengurusan keselamatan maklumat organisasi pada sela masa yang dirancang bagi memastikan kesesuaian, kecukupan dan keberkesanan yang berterusan.

Kajian semula pengurusan hendaklah mengandungi pertimbangan tentang:

a) status tindakan daripada kajian semula pengurusan terdahulu;

b) perubahan dalam isu luaran dan dalaman yang berkaitan dengan sistem pengurusan keselamatan maklumat;

c) maklum balas tentang prestasi keselamatan maklumat, termasuk trend dalam:

1) ketakakuran dan tindakan pembetulan;

2) hasil pemantauan dan pengukuran;

3) hasil audit; dan

4) pencapaian objektif keselamatan maklumat;

d) maklum balas daripada pihak berkepentingan;

e) hasil pentaksiran risiko dan pelan penguraian risiko; dan

f) peluang untuk penambahbaikan berterusan.

Output kajian semula pengurusan hendaklah merangkumi keputusan yang berkaitan dengan peluang penambahbaikan yang berterusan dan sebarang keperluan untuk perubahan dalam sistem pengurusan keselamatan maklumat.

Organisasi hendaklah menyimpan maklumat yang didokumenkan sebagai bukti daripada hasil kajian semula pengurusan.

MALAYSIAN STANDARD

MS ISO/IEC 27001:2013 (BM)

Teknologi maklumat - Teknik keselamatan - Sistem pengurusan keselamatan maklumat - Keperluan
(Semakan pertama)
(ISO/IEC 27001:2013, IDT)
(Diterbitkan oleh Jabatan Standard Malaysia pada tahun 2017)

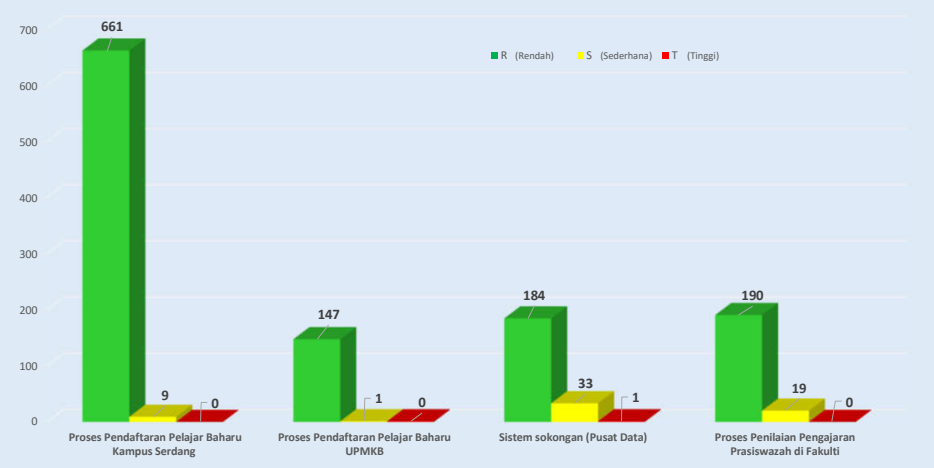
ICS: 35.040

© Hak cipta 2017
JABATAN STANDARD MALAYSIA

2

PENILAIAN RISIKO ISMS UPM TAHUN 2020

HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN JULAI 2020



Penilaian Risiko operasi ISMS yang dinilai melalui sistem MyRAM *(Malaysian Public Sector ICT Risk Assessment Methodology)* pada Julai 2020 melibatkan 879 aset dengan 1245 jumlah ancaman

3

3

PENILAIAN RISIKO ISMS UPM

HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN JULAI 2020

Bil.	Nama Proses	Bil Aset	Bil Ancaman	Bil. Tahap Risiko (Bilangan Ancaman)		
				R	S	T
1.	Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang	551	670	661	9	0
2.	Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB	74	148	147	1	0
3.	Sistem sokongan (Pusat Data)	180	218	184	33	1
4.	Proses Penilaian Pengajaran Prasiswazah di Fakulti	74	209	190	19	0
	JUMLAH	**879**	**1245**	**1182**	**62**	**1**

4

4

PENILAIAN RISIKO ISMS UPM

PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN JULAI 2020

Bil	Nama Proses	Punca Dominan	Kawalan Sediaada (Existing Safeguard)	Kawalan yang dirancang (Planned Safeguard) & Cadangan tarikh Tindakan	Pelan Pemulihan Risiko (Risk Treatment Plan) & Cadangan tarikh Tindakan
1.	**Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang**	**(a) Pengesahan Pendaftaran Pelajar Baharu Prasiswazah di Kolej Kediaman**			
		Gangguan Perkhidmatan Rangkaian ICT	Pelaksanaan proses pendaftaran secara manual. Masukkan maklumat yang diperlukan ke dalam SMP selepas rangkaian pulih berdasarkan bilangan pelajar baharu yang hadir.	Tiada	Tiada
		(b) Kad Pelajar Baharu Prasiswazah			
		Software vulnerabilities or errors	Salinan Pendua. Arahan Kerja Perkhidmatan Sokongan ICT.	Tiada	Tiada
		(c) Pengesahan Laporan Pemeriksaan Kesihatan Pelajar Baharu Prasiswazah			
		Hardware malfunction	Penyelenggaraan berkala UPM/OPR/iDEC/P003: Penyelenggaraan ICT. Pelaksanaan DRP ICT.	Tiada	Tiada
		(d) Pembayaran Yuran Pelajar Baharu Prasiswazah			
		Non-availability of the mobile communication network	Pengurusan perubahan kepada Servis Pembekal. Kepelbagaian servis telco.	Tiada	Tiada
		(e) Proses Muatnaik Data Tawaran Pelajar UPU			
		Loss of data confidentiality/ integrity as a result of IT user error	Perancangan Operasi dan Kawalan • Melindungi data dengan kata laluan • Arahan Kerja Urusan Pengambilan Pelajar Baharu (UPM/PU/PS/AK005) Perkara H :Tawaran Kemasukan (Perdana dan Rayuan)	Tiada	Tiada

5

PENILAIAN RISIKO ISMS UPM

PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN JULAI 2020

Bil	Nama Proses	Punca Dominan	Kawalan Sediaada (Existing Safeguard)	Kawalan yang dirancang (Planned Safeguard) & Cadangan tarikh Tindakan	Pelan Pemulihan Risiko (Risk Treatment Plan) & Cadangan tarikh Tindakan
2.	**Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB**	*SMP - Software malfunctions* Gangguan Perkhidmatan Punca Kuasa Elektrik	Pendaftaran dilakukan secara manual dengan merujuk senarai nama pelajar dan surat tawaran. Menyediakan genset sebagai sumber elektrik kedua.	Tiada	Tiada
3.	**Sistem sokongan (Pusat Data)**	Bangunan iDEC Beta • *Flash flood(H)* • *Lightning(M)* • *Fire(M)* • *Power Failure(M)* *Hardware malfunction(M)* • *DR Standby Genset* • *DR Centralised UPS* • *DR Precision Cooling Unit* • *DC Standby Genset*	Pelaksanaan DRP ICT • Pengesahan keadaan keselamatan bangunan oleh PPPA dan OSH UPM • Prosedur Penyelenggaraan ICT: • GPKTMK Perkara 11.3 (e): Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003: Prosedur Penyelenggaraan ICT	Permohonan kepada PPPA penyelenggaraan sistem perparitan iDEC Beta.	Permohonan RMK12 bagi Pusat Data Baharu akan diketengahkan pada permohonan RMK-12 secara berfasa. Tarikh: Jan 2021
4.	**Proses Penilaian Pengajaran Prasiswazah di Fakulti**	• *Power failure* • *Failure of the IT system* • *Threat posed by internal staff during maintenance or administration work* • *Hardware malfunctions*	• Peralatan Sokongan • Perancangan kesinambungan keselamatan informasi • Prosedur operasi berdokumentasi • Penyelenggaraan Peralatan • GPKTMK Perkara 11.3 (e): Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003: Prosedur Penyelenggaraan ICT	Tiada	Tiada

6

6

SYOR

Mesyuarat diminta mengambil makluman dan perhatian:

1. **Laporan Penilaian Risiko dan Pelan Pemulihan Risiko** Keselamatan Maklumat Tahun 2020 (semakan Julai 2020); dan

2. mengambil perhatian terhadap **tindakan kawalan dan pelan pemulihan risiko** yang digunakan oleh setiap peneraju ISMS dalam menyediakan **perlindungan dan kawalan** keberkesanan Sistem Pengurusan Keselamatan Maklumat di UPM.

7

7