



UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI



**Universiti
Putra
Malaysia**



AGENDA 8.3: Hasil Penilaian Risiko & Pelan Pemulihan Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS)

Mesyuarat Kajian Semula Pengurusan (MKSP) ISO Tahun 2021

19 November 2021 | 9.00 pagi | MENERUSI APLIKASI ZOOM MEETING

 UniPutraMalaysia

 @uputramalaysia

 uniputramalaysia

 universitiputramalaysia

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:

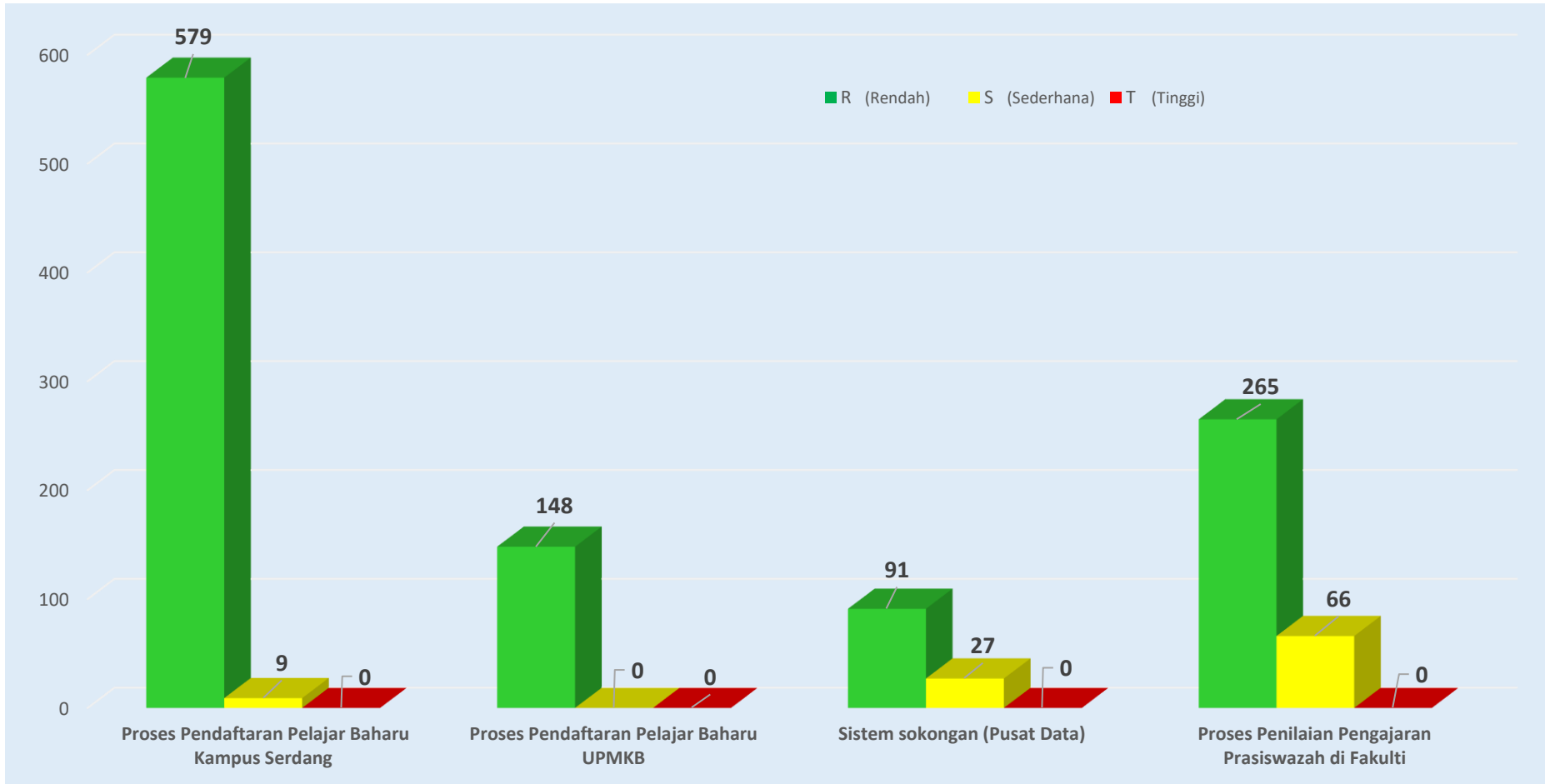
- a) status tindakan daripada kajian semula pengurusan terdahulu;
- b) perubahan dalam isu luaran dan dalaman yang berkaitan dengan sistem pengurusan keselamatan maklumat;
- c) maklum balas tentang prestasi keselamatan maklumat, termasuk trend dalam:
 - 1) ketakakuran dan tindakan pembetulan;
 - 2) hasil 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.

HASIL PENILAIAN RISIKO & PELAN PEMULIHAN RISIKO ISMS

HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021



Penilaian Risiko operasi ISMS yang dinilai melalui sistem MyRAM (Malaysian Public Sector ICT Risk Assessment Methodology) pada Mac 2021 melibatkan **776** aset dengan **1185** jumlah ancaman



HASIL PENILAIAN RISIKO & PELAN PEMULIHAN RISIKO ISMS

HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021

Bil.	Nama Proses	Bil. Aset	Bil. Ancaman	Tahap Risiko (Berdasarkan Jumlah Ancaman)		
				Rendah	Sederhana	Tinggi
01	Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang	472	588	579	9	0
02	Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB	74	148	148	0	0
03	Sistem Sokongan (Pusat Data)	88	118	91	27	0
04	Proses Penilaian Pengajaran Prasiswazah di Fakulti	142	331	265	66	0
		776	1185	1083	102	0



HASIL PENILAIAN RISIKO & PELAN PEMULIHAN RISIKO ISMS

PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021

Nama Proses	Punca Dominan	Kawalan Sediaada (Existing Safeguard)	Rawatan (Treatment)	Pelan Pemulihan Risiko (Risk Treatment Plan) & Cadangan tarikh Tindakan
Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang	PutraVID API (Medium) <i>T4.20 – Software vulnerabilities or errors</i>	<i>A.12.3.1 – Information backup</i> Arahan Kerja Perkhidmatan Sokongan ICT	Tiada	Tiada
	Petugas Muat Naik Data Pelajar (Medium) <i>T3.3 - Carelessness/negligence in handling information and operating the IT system</i>	<i>A.7.2.2 – Information security awareness, education and training</i> Latihan & kursus yang berkaitan dan <i>backup</i> staf	Tiada	Tiada
	Pangkalan Data SMP (Medium) <i>T2.3 - Loss, destruction, disclosure and falsification of sensitive organisational records/information</i>	<i>A.9.4.1 - Information access restriction</i> • GPKTMK Perkara 9.0 : Kawalan Akses • UPM/ISMS/OPR/P003: Prosedur Kawalan dan Pemantauan Capaian ke Sistem Di Pusat Data	Tiada	Tiada
		<i>A.12.3.1 – Information backup</i> UPM/ISMS/OPR/AK02-Arahan Kerja Pengurusan Backup	Tiada	Tiada
	Mesin Terminal Pembayaran (Low) <i>T4.36 - Non-availability of the mobile communication network</i>	<i>8.1 - Operational planning and control</i> Kepelbagaian servis rangkaian telco	Perjanjian dengan pembekal perkhidmatan (CIMB)	Jun 2011 - Dis 2026
Online Payment (Low) <i>T4.23 - Failure of a database</i>	<i>8.3 - Information security risk treatment</i> Hubungi bank yang berkaitan	Perjanjian dengan pembekal perkhidmatan (CIMB)	Jun 2011 - Dis 2026	



HASIL PENILAIAN RISIKO & PELAN PEMULIHAN RISIKO ISMS

PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021

Nama Proses	Punca Dominan	Kawalan Sediaada (Existing Safeguard)	Rawatan (Treatment)	Pelan Pemulihan Risiko (Risk Treatment Plan) & Cadangan tarikh Tindakan
Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB	SMP (Low) <i>T4.1 - Software malfunctions</i>	<i>A.12.3.1 - Information backup</i> Pendaftaran boleh dilakukan manual dengan merujuk senarai nama pelajar dan surat tawaran.	Tiada	Tiada
	Senarai Pendaftaran (Low) <i>T3.3 - Carelessness/ negligence in handling information and operating the IT system</i>	<i>8.1 - Operational planning and control</i> Cetakan semula dengan merujuk rekod dalam komputer.	Tiada	Tiada
Sistem sokongan (Pusat Data)	DC Standby Genset (Medium) <i>T4.2 - Hardware malfunctions</i>	<i>A.11.2.4 - Equipment maintenance</i> Pemantauan dan penyelenggaraan berkala <ul style="list-style-type: none"> • GPKTMK Perkara 11.3(e) : Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003 : Prosedur Penyelenggaraan ICT • SOK/PYG/GP02 : Garis Panduan Penyelenggaraan Berkala (PPPA) 	<i>A.15.2.1 - Monitoring and review of supplier services</i> Perkhidmatan penyelenggaraan Genset oleh PPPA	Apr 2020 - Apr 2022
	Bangunan iDEC Beta (Medium) <i>T1.19 - Flash flood</i>	<i>6.1.1 - General</i> Permohonan Pusat Data Baru telah dikemukakan semula pada RMK12 Rolling Plan 2 Tahun 2022 pada 3 Feb 2021 ke KPT melalui PPPA	<i>A.11.1.4 - Protecting against external and environmental threats</i> 1. Penyelenggaraan sistem perparitan oleh PPPA 2. Permohonan RMK12 secara berfasa	Jan 2021 - Dis 2021
Proses Penilaian Pengajaran Prasiswazah di Fakulti	Pelayan Aplikasi BLASTTA (Low) <i>T1.9 - Failure of the IT system</i>	<i>A.11.2.4 - Equipment maintenance</i> Prosedur Penyelenggaraan ICT: <ul style="list-style-type: none"> • GPKTMK Perkara 11.3 (e) : Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003 : Prosedur Penyelenggaraan ICT Penyelenggaraan Berkala 	Tiada	Tiada



Mesyuarat diminta mengambil makluman dan perhatian:

1. **Laporan Penilaian Risiko dan Pelan Pemulihan Risiko** Keselamatan Maklumat Tahun 2021 (semakan Mac 2021);
2. Sebanyak **1083 aset dengan risiko tahap rendah, 102 risiko tahap sederhana** dan **tiada aset dengan tahap tinggi direkodkan**; dan
3. 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.







UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI




Terima Kasih

 UniPutraMalaysia

 @uputramalaysia

 uniputramalaysia

 universitiputramalaysia

PERTANIAN • INOVASI • KEHIDUPAN
BERILMU BERBAKTI
WITH KNOWLEDGE WE SERVE