



UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

PUTRA
PERTANIAN UNTUK RAKYAT

AGENDA 8.3 : HASIL PENILAIAN RISIKO DAN PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

**MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
ISO QMS & ISMS UPM TAHUN 2024**

**19 SEPTEMBER 2024 | 2.00 PETANG | DEWAN SENAT,
BANGUNAN CANSELORI PUTRA**

Berilmu Berbakti Pertanian • Inovasi • Kehidupan

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.

Penilaian risiko dilaksanakan dengan **tujuan** untuk menilai tahap risiko aset yang terlibat dalam proses melibatkan skop ISMS supaya pendekatan dan keputusan yang paling berkesan dikenalpasti bagi menyediakan perlindungan dan kawalan ke atas risiko aset berkenaan, berasaskan metodologi Penilaian Risiko Terperinci MyRAM (*Malaysian Public Sector ICT Risk Assessment Methodology*).

Pengemaskinian MyRAM dilaksanakan apabila berlaku perubahan atau penambahan aset di dalam skop ISMS yang terlibat. **Aset dinilai samada Rendah (Low), Sederhana (Medium) atau Tinggi (High)** berdasarkan ciri utama keselamatan iaitu **Kerahsiaan (Confidentiality), Integriti (Integrity)** dan **Ketersediaan (Availability)**.



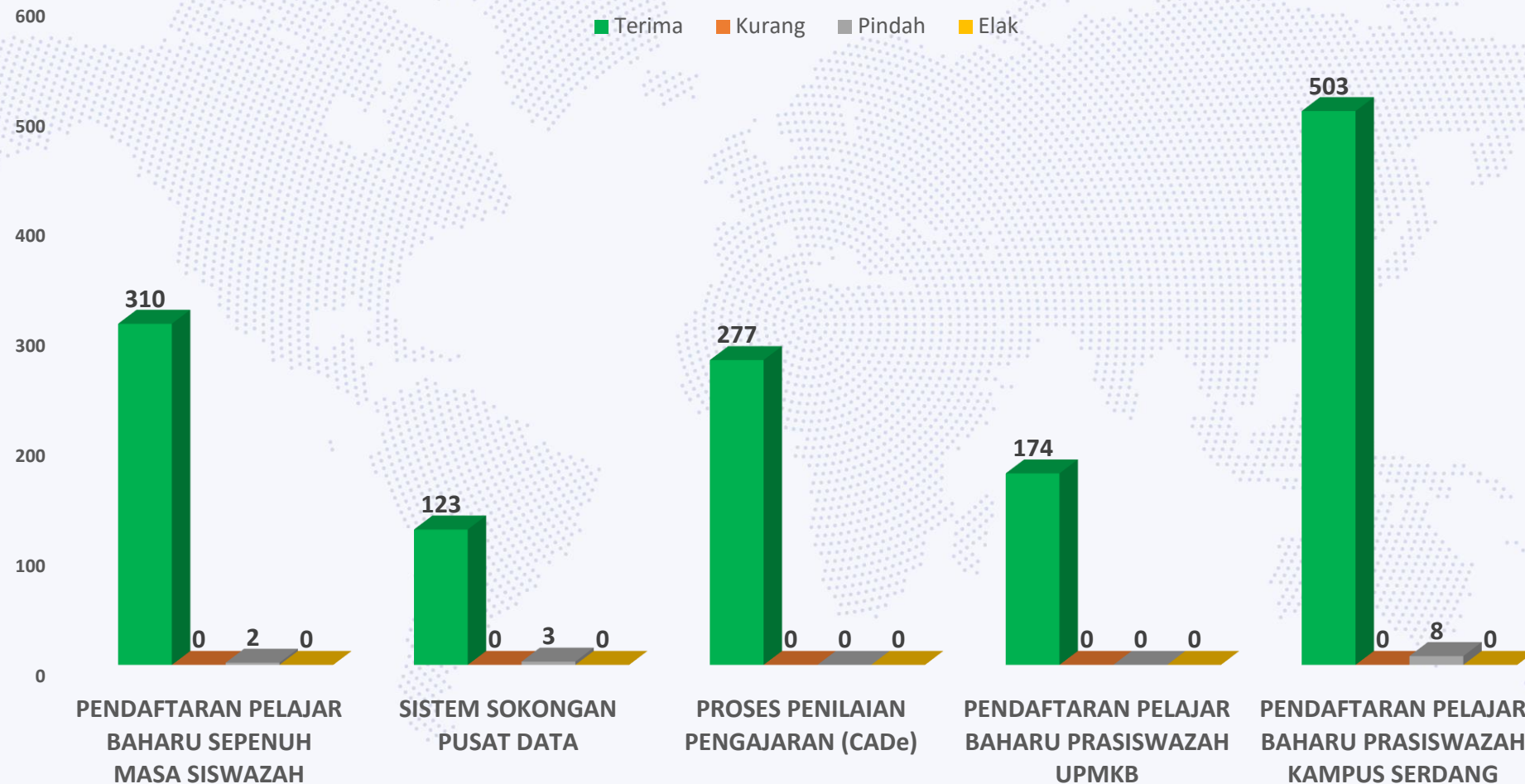
PASUKAN ISMS SERDANG DAN BINTULU



HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2024

Bil.	Nama Proses	Bil Aset	Bil Ancaman	Bil. Tahap Risiko (Bilangan Ancaman)		
				R	S	T
1.	Proses Pendaftaran Pelajar Baharu Siswazah	192	312	299	13	0
2.	Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang	334	511	504	7	0
3.	Proses Pendaftaran Pelajar Baharu Prasiswazah UPMKB	104	174	174	0	0
4.	Sistem sokongan (Pusat Data)	83	126	99	27	0
5.	Proses Penilaian Pengajaran Prasiswazah di Fakulti	116	277	277	0	0
	JUMLAH	829	1400	1353	47	0

HASIL PENILAIAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2024

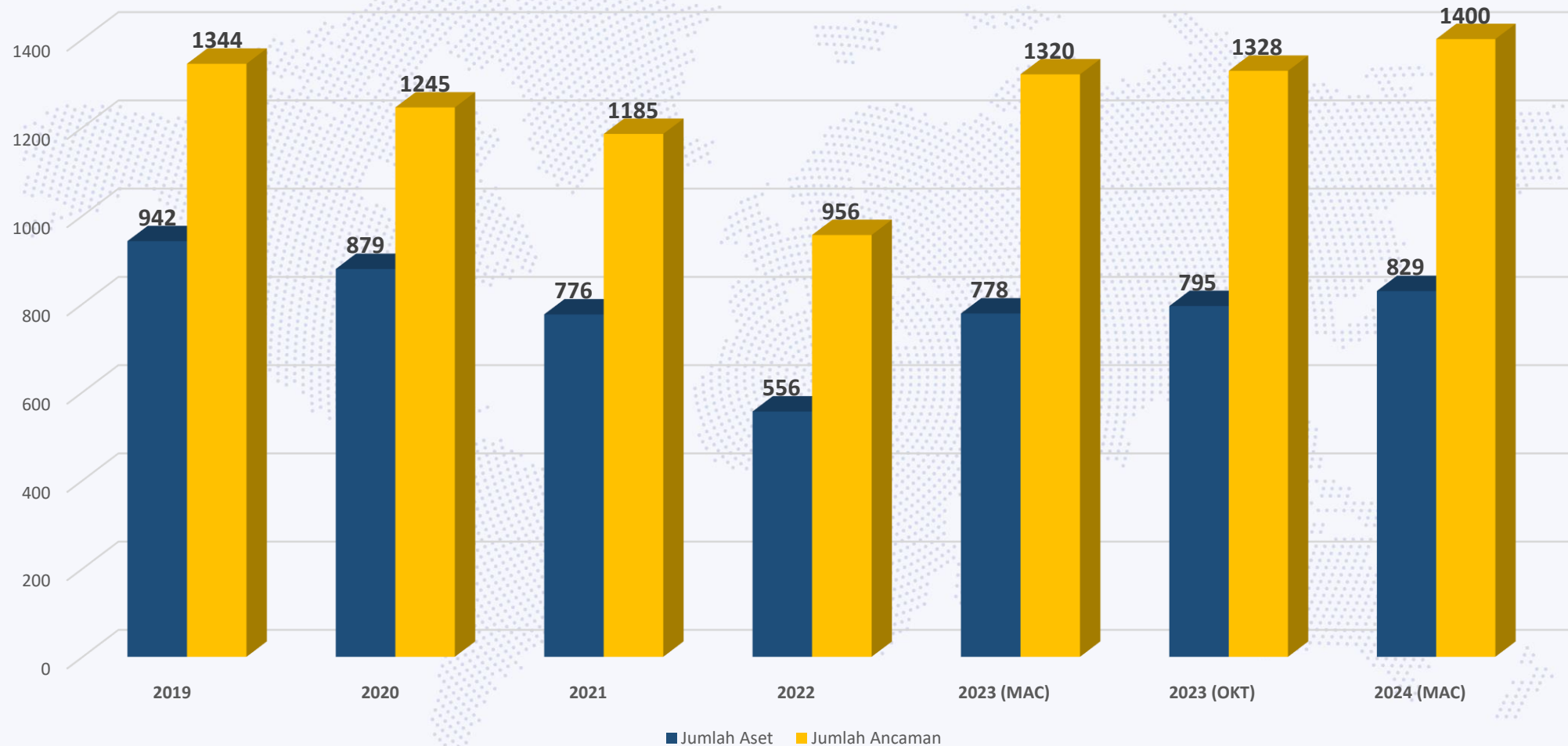


PENILAIAN RISIKO ISMS TAHUN 2024

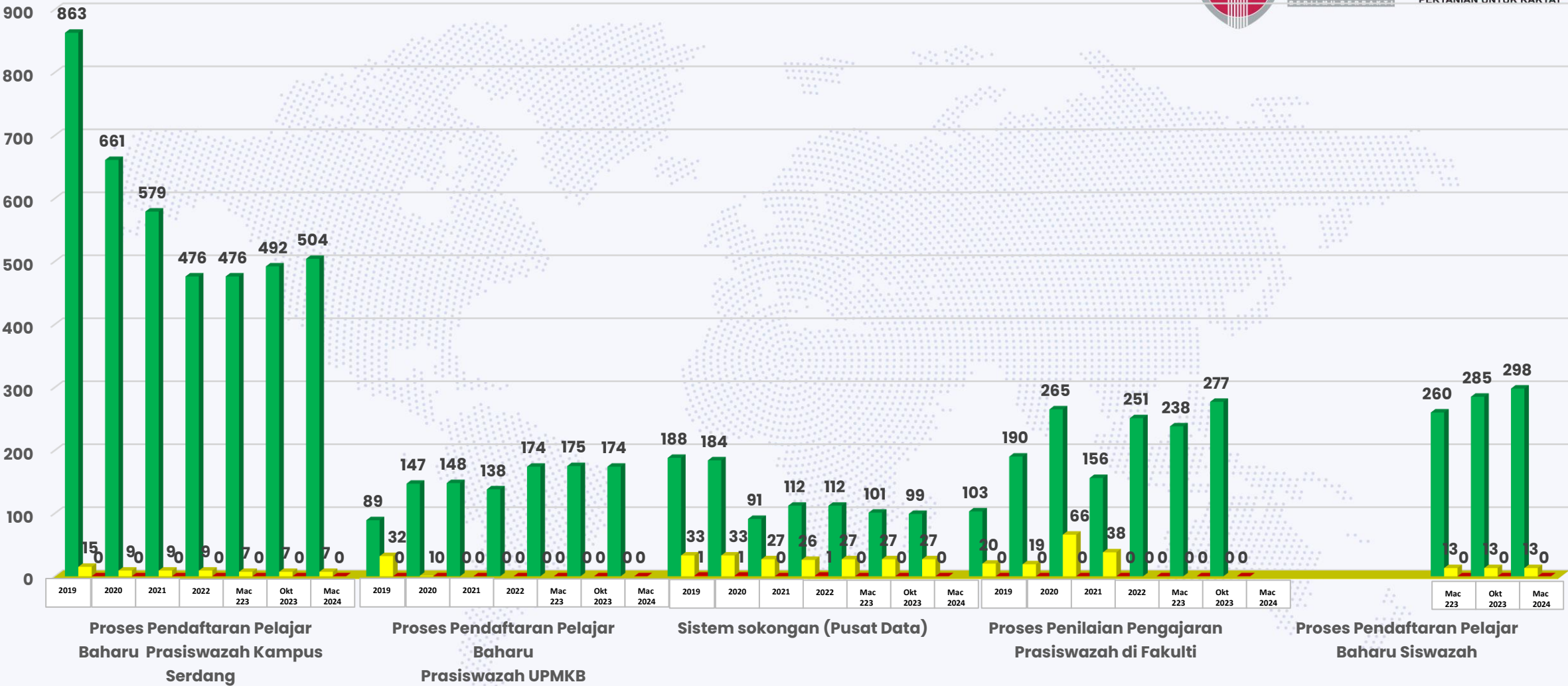


UPM
UNIVERSITI PUTRA MALAYSIA
BERILMU BERBAKTI

PUTRA
PERTANIAN UNTUK RAKYAT



PENILAIAN RISIKO ISMS TAHUN 2024



PELAN PEMULIHAN RISIKO ISMS TAHUN 2024



PASUKAN	NAMA ASET	BILANGAN ASET	THREAT	EXISTING SAFEGUARD	RISK LEVEL	ACTION	TREATMENT	RESIDUAL RISK
Pasukan Pendaftaran Prasiswazah Serdang	Pej Bursar – Bank Statement	3	T4.3 – Failure of a local area network or wide area network (LAN and WAN)	A.7.4 – Communication 1. Hubungi Bank yang berkaitan 2. Hubungi pihak IDEC	L	Transfer	Refer to Payment Service Agreement with CIMB Bank	L
			T4.27 – Failure or malfunction of a network component	A.7.4 – Communication 1. Hubungi Bank yang berkaitan 2. Hubungi pihak IDEC	L	Transfer	Refer to Payment Service Agreement with CIMB Bank	L
	Pej Bursar – Online Payment	1	T4.23 – Failure of a database	A.8.3 – Information security risk treatment Hubungi bank yang berkaitan	L	Transfer	Refer to Payment Service Agreement with CIMB Bank	L
			T4.27 – Failure or malfunction of a network component	A.8.3 – Information security risk treatment Hubungi bank yang berkaitan	L	Transfer	Refer to Payment Service Agreement with CIMB Bank	L
Pasukan Pendaftaran Pelajar Baharu Sepenuh Masa Siswazah	i-PUTRA STARS	1	T4.3 – Failure of a local area network or wide area network (LAN and WAN)	A.6.1.3 – Contact with authorities melaporkan kepada EMGS sekiranya berlaku masalah dengan sistem STARS	M	Transfer	A6.1.3 – Contact with authorities HUBUNGI EMGS	L
	PKU – RHB Terminal Machine	1	T4.3 – Failure of a local area network or wide area network (LAN and WAN)	A.6.1.3 – Contact with authorities Melaporkan masalah kepada Help Desk RHB Mesin	L	Transfer	Rujuk Perjanjian perkhidmatan dengan RHB Bank	L
Sistem Sokongan Pusat Data	SDC-DR Standby Genset	1	T4.2 – Hardware malfunctions	A.11.2.4 – Equipment maintenance Pemantauan dan penyelenggaraan berkala • GPKTMK Perkara 11.3(e) : Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003 : Prosedur Penyelenggaraan ICT • SOK/PYG/GP02 : GP Penyelenggaraan Berkala (PPPA)	L	Transfer	A15.2.1 – Monitoring and review of supplier services Perjanjian perkhidmatan dengan pihak berkaitan A11.2.4 – Equipment maintenance Penyelenggaraan berkala oleh pihak vendor	L
	SDC-DC Standby Genset	2	T4.2 – Hardware malfunctions	A.11.2.4 – Equipment maintenance Pemantauan dan penyelenggaraan berkala • GPKTMK Perkara 11.3(e) : Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003 : Prosedur Penyelenggaraan ICT • SOK/PYG/GP02 : GP Penyelenggaraan Berkala (PPPA)	L	Transfer	A15.2.1 – Monitoring and review of supplier services Perkhidmatan penyelenggaraan Genset oleh PPPA A11.2.4 – Equipment maintenance Penyelenggaraan berkala oleh pihak vendor	L

Ahli Mesyuarat Kajian Semula Pengurusan diminta mengambil maklum dan perhatian berhubung:

1. **Laporan Penilaian Risiko dan Pelan Pemulihan Risiko Keselamatan Maklumat terkini (semakan Mac 2024);**
2. **Hasil penilaian ke atas 829 aset mencatatkan 1353 risiko tahap rendah, 47 risiko tahap sederhana dan tiada risiko tahap tinggi;**
3. **Perbandingan bilangan aset, bilangan ancaman dan tahap risiko ISMS dari tahun 2019 hingga 2024 (Mac 2024)** bagi setiap pasukan ISMS; dan
4. **Tindakan kawalan dan pelan pemulihan risiko** yang digunakan oleh setiap pasukan ISMS dalam menyediakan perlindungan dan kawalan keberkesanan Sistem Pengurusan Keselamatan Maklumat di UPM **dipantau secara berkala melalui *The Malaysian Public Sector Information Security Risk Assessment System (MyRAM)* setakat 2024.**
5. **Penggunaan *tools kit* baharu bagi penilaian risiko, tindakan kawalan dan pelan pemulihan risiko akan mula dilaksanakan untuk tahun 2025 selaras dengan peralihan standard baharu ISO/IEC 27001:2022 yang berkuat kuasa pemakaiannya pada tahun 2025.**



Pertanian • Inovasi • Kehidupan
Berilmu Berbakti

Terima Kasih