UNIVERSITI PUTRA MALAYSIA

AGRICULTURE • INNOVATION • LIFE

KAEDAH PELAKSANAAN ISMS DI UNIVERSITI PUTRA MALAYSIA

15 JUN 2016 | Dewan Taklimat Serdang

PELAKSANAAN ISMS DI UPM:

2011

- Kelulusan Mesyuarat JPU bagi pelaksanaan ISMS di UPM

2012

- Pensijilan pertama dengan standard **MS ISO/IEC 27001:2007**
- Skop ISMS UPM merangkumi **perkakasan (*server* dan storan) dan data/maklumat untuk aplikasi kritikal Universiti (Laman Web Utama Univresiti, Sistem Pengurusan Kewangan, Sistem Aplikasi Pelajar dan Sistem Pengurusan Sumber Manusia)**

2014

- Pensijilan dengan standard **MS ISO/IEC 27001:2013**
- **Skop baru ISMS UPM merangkumi perkakasan (*server* dan storan) dan data/maklumat untuk aplikasi kritikal Universiti dengan penambahan kepada Sistem Maklumat Pelajar Siswazah, iGIMS.**

PELAKSANAAN ISMS DI UPM:

2015

- PELUASAN SKOP kepada **Proses Pendaftaran Pelajar Baharu Prasiswazah**

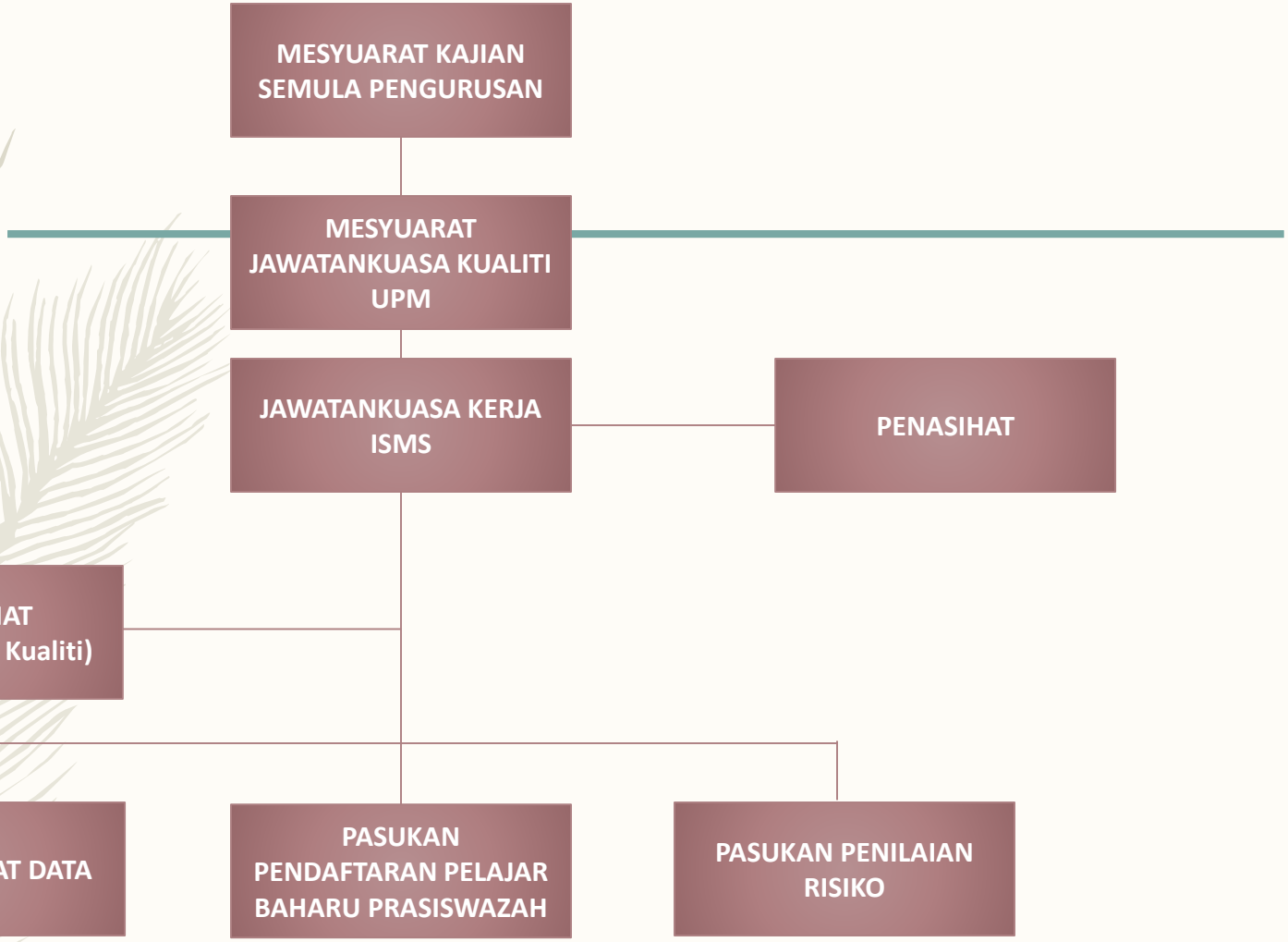
Skop Pensijilan ISMS:

i. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Maklumat Pelajar;

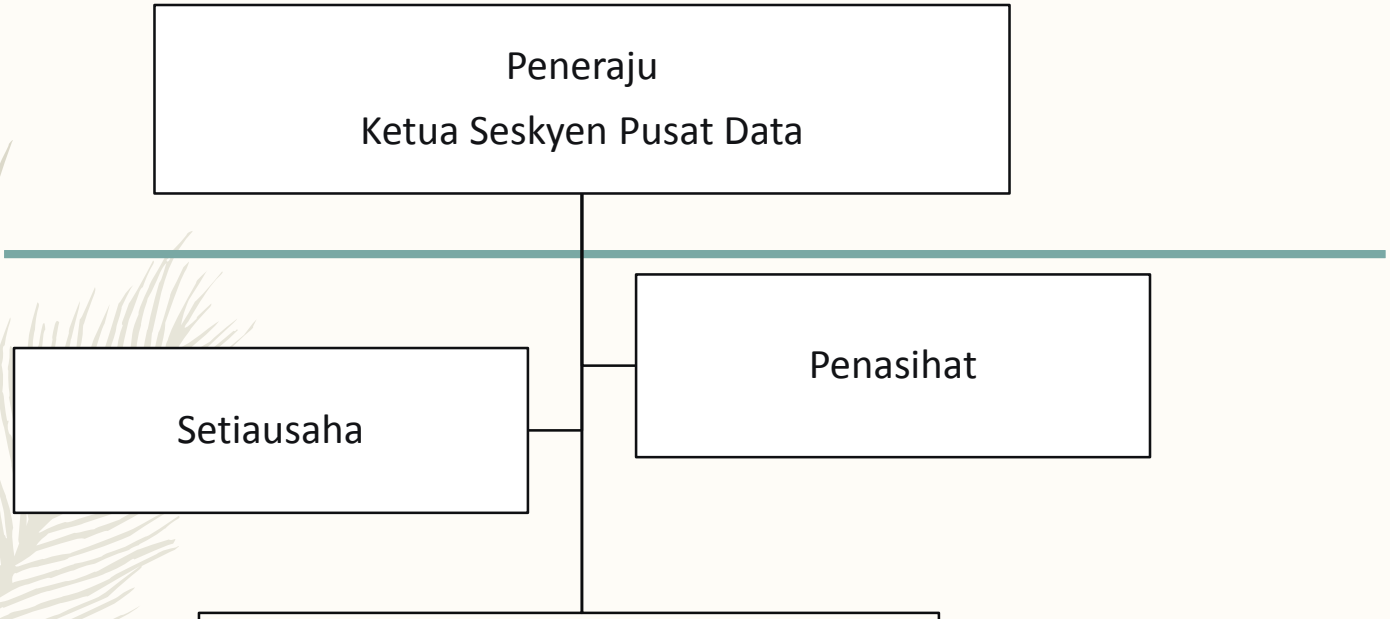
ii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan

iii. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah

STRUKTUR ORGANISASI ISMS UPM



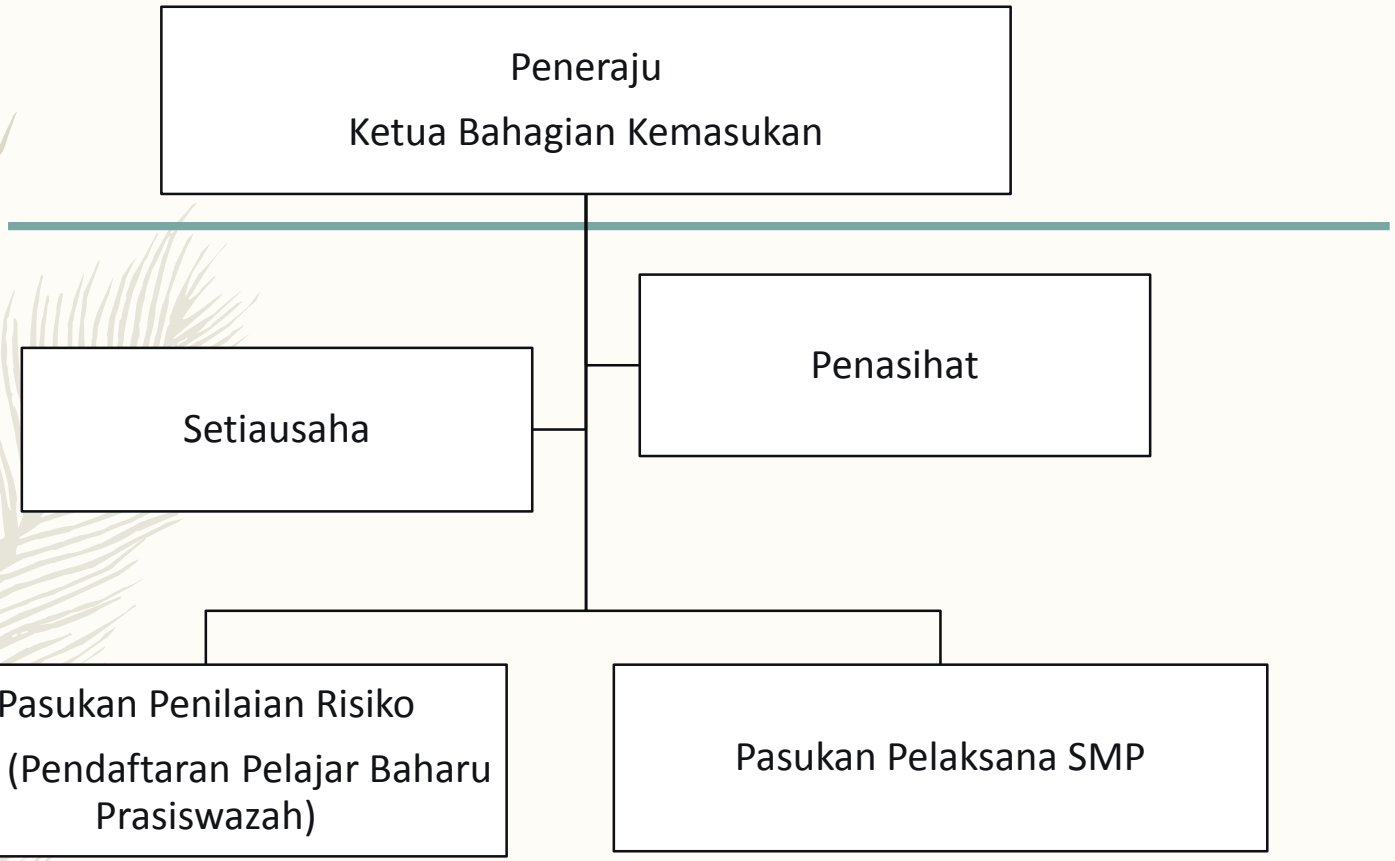
STRUKTUR ORGANISASI PASUKAN PUSAT DATA



- PTM Pusat Data
- PTM Data & Implementasi Aplikasi
- PTM Rangkaian & Telekomunikasi
- PTM Keselamatan ICT
- PTM Bahagian Governan

- PTM Pusat Data
- PTM Data & Implementasi Aplikasi
- PTM Rangkaian & Telekomunikasi
- PTM Keselamatan ICT
- Semua pegawai Operasi Pusat Data

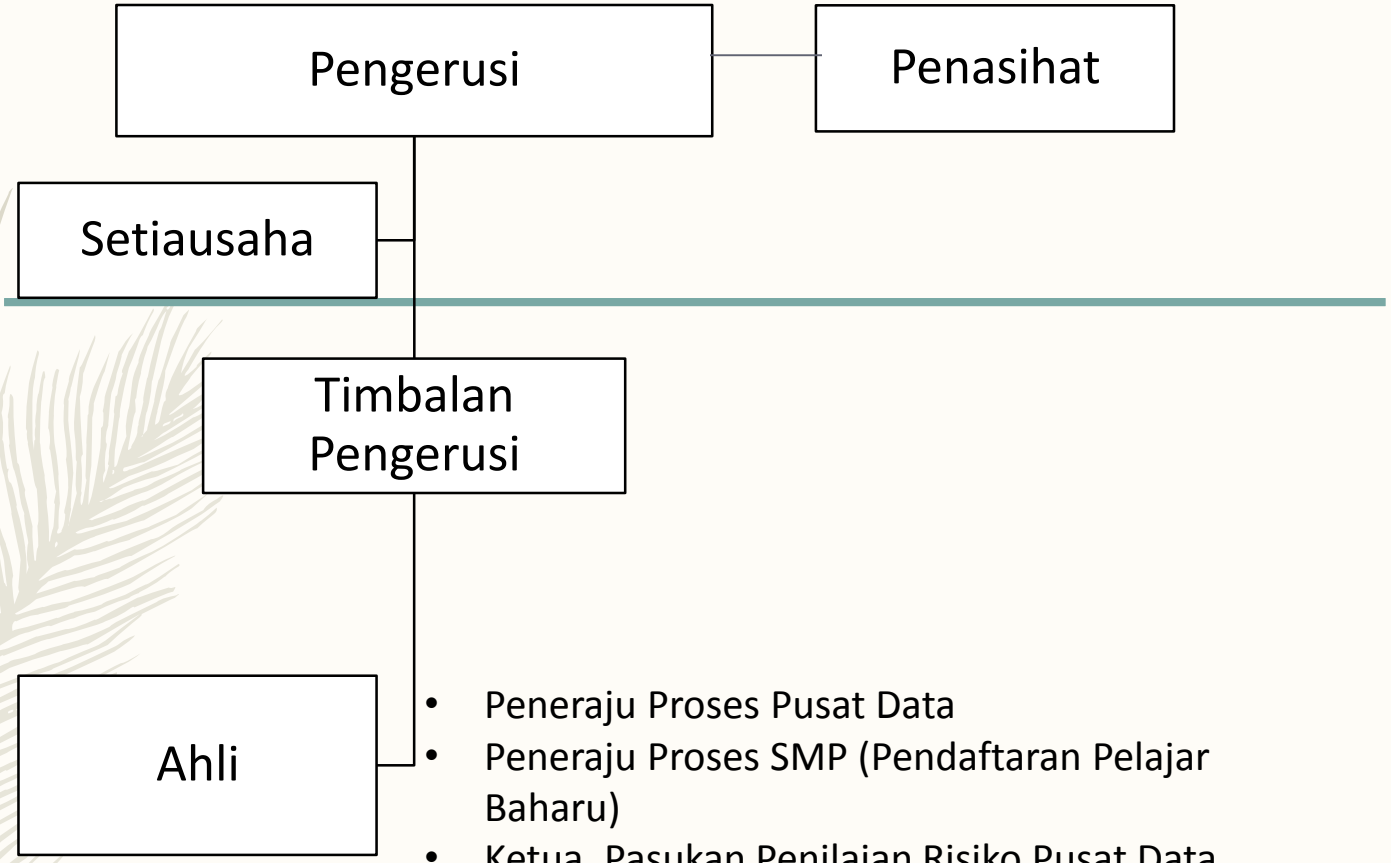
STRUKTUR ORGANISASI PASUKAN PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH



- Pegawai operasi (kolej,PKU,BKU,Bursar)
- Ketua Bahagian Operasi Aplikasi, iDEC
- Ketua Seskyen Operasi Aplikasi, iDEC

- Wakil PTJ (Kolej, PKU, BKU, Bursar)
- Ketua Bahagian Operasi Aplikasi, iDEC
- Ketua Seskyen Operasi Aplikasi, iDEC
- Pegawai Operasi ICT Bahagian Akademik

STRUKTUR ORGANISASI PASUKAN PENILAIAN RISIKO



- Peneraju Proses Pusat Data
- Peneraju Proses SMP (Pendaftaran Pelajar Baharu)
- Ketua, Pasukan Penilaian Risiko Pusat Data
- Ketua, Seksyen Pusat Data
- Ketua, Seksyen Operasi Aplikasi
- PTM Rangkaian & Telekomunikasi
- PTM Data & Implementasi Aplikasi
- Pentadbir Sistem SMP
- Pentadbir Sistem Kewangan
- Pegawai Keselamatan ICT

PROSES PERKHIDMATAN

Pendaftaran Pelajar Baharu Prasiswazah

- Menyemak Tawaran
- Menerima Salinan pendua slip bayaran yuran
- Menerima borang permohonan kad pelajar
- Mengesah status kesihatan
- Pengesahan pendaftaran
- Pendaftaran kolej

PROSES PERKHIDMATAN

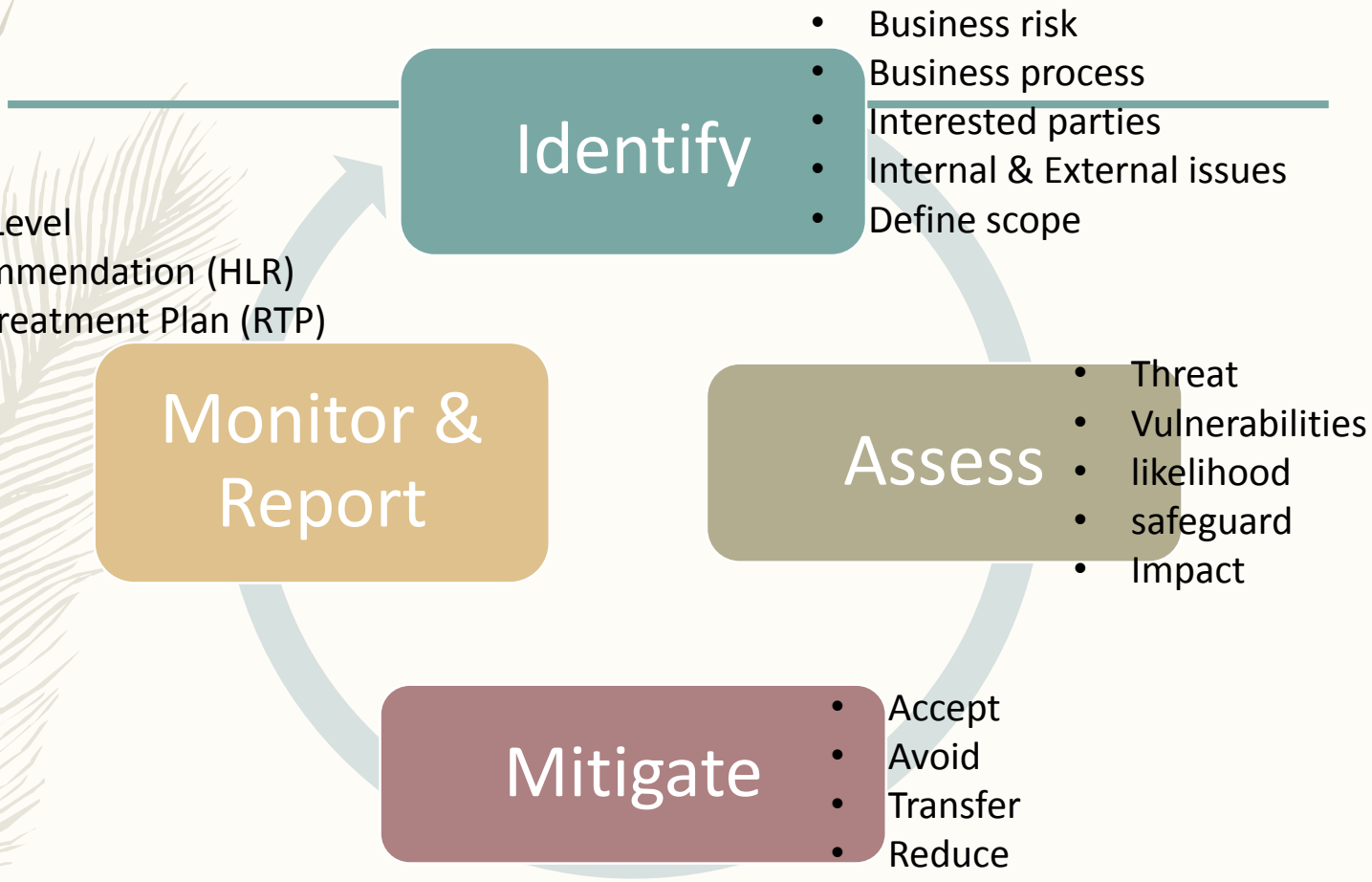
Operasi Pusat Data & Pusat Pemulihan Bencana

- Pelaksanaan operasi Pusat Data
- Penyelenggaraan fasiliti Pusat Data
- Pemantauan operasi Pusat Data
- Penyenggaraan perkhidmatan operasi server di Pusat Data
- Pemantauan capaian sistem di Pusat Data
- Kawalan keselamatan di Pusat Data
- Tindakan kecemasan di Pusat Data

STRATEGI PELAN PELAKSANAAN

PENILAIAN RISIKO

Proses Pengurusan Risiko



PENILAIAN RISIKO

Aset dinilai berasaskan kerahsiaan, integriti dan ketersediaan (C I A)

ASSET GROUP	ASSET COUNT	ASSET VALUE			IMPACT LEVEL			RISK LEVEL		
		Low	Med	High	Low	Med	High	Low	Med	High
Hardware	67	0	53	14	7	43	17	231	125	1
Software	39	2	2	35	4	35	0	78	0	0
People	218	150	50	18	155	60	3	349	50	0
Information and Data	58	1	43	14	1	43	14	42	16	0
Services (supporting)	91	34	31	26	42	44	5	93	22	0
Services (accessibility)	54	18	0	36	18	0	36	35	41	11
TOTAL	**527**	**205**	**179**	**143**	**227**	**225**	**75**	**828**	**254**	**12**

PENILAIAN RISIKO

Keperluan penilaian risiko dalam pelaksanaan ISMS adalah berdasarkan kepada standard MS ISO/IEC 27001:2013, iaitu:
Klausa 6.1 : Actions to address risk and opportunities
Klausa 8.2 : Information security risk assessment
Klausa 8.3 : Information security risk treatment

BIL.	OUTPUT PENILAIAN RISIKO JUMLAH ASET= 527	PUNCA DOMINAN	PELAN PEMULIHAN
1.	Aset berisiko tinggi	Lokasi Pusat Data di bangunan yang berumur lebih 50 tahun, kedudukan di aras bawah dan keluasan yang terhad untuk menapung keperluan server	Cadangan pembangunan Pusat Data baharu dengan memohon peruntukan melalui RMK11.
		Pembayaran yuran secara tunai bagi pelajar yang tidak membuat pembayaran melalui bank	Sifar bayaran yuran pendaftaran secara tunai melalui kaedah pembayaran secara online melalui kemudahan “Jom PAY”
		Laporan kesihatan oleh pelajar yang dijalankan daripada Pusat Perubatan luar	Pemeriksaan perubatan perlu dilaksanakan di PKU sahaja dan penyimpanan data secara format digital sepenuhnya.

PENILAIAN RISIKO

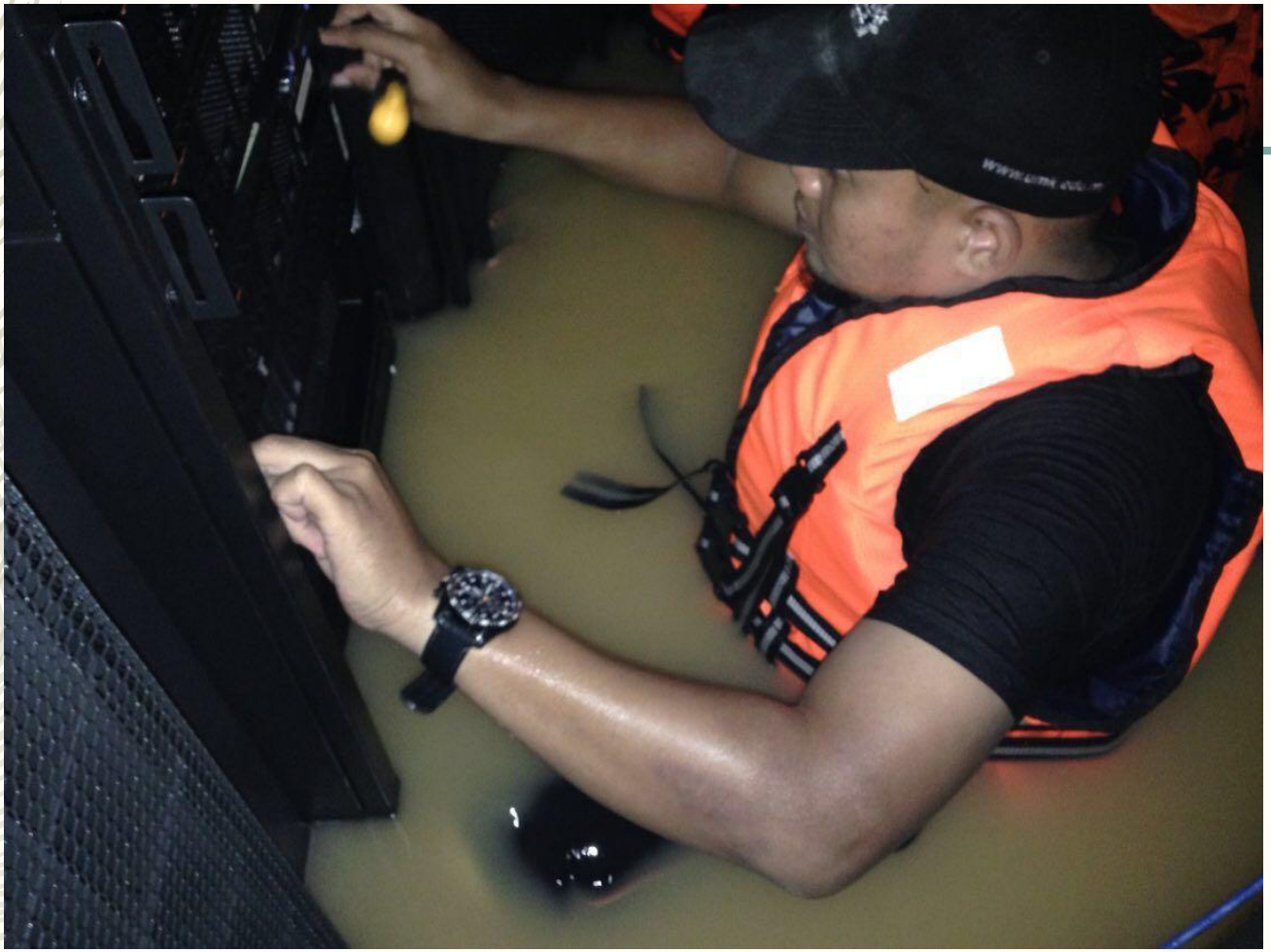
BIL.	OUTPUT PENILAIAN RISIKO JUMLAH ASET= 527	PUNCA DOMINAN	PELAN PEMULIHAN
2.	Aset berisiko sederhana	Masih terdapat komputer lama (sistem pengoperasian (OS) yang telah luput) yang digunakan oleh pihak Kolej untuk tujuan pendaftaran pelajar yang berisiko dari aspek keselamatan	Kajian semula keperluan komputer kolej dengan mengambil kira penggantian komputer lama dengan sistem pengoperasian (OS) luput yang tidak selamat dalam aspek keselamatan.
		Pelaksanaan naik taraf elektrik Pusat Pemulihan Data	Naik taraf siap Disember 2015.
3.	Aset berisiko rendah	Hampir semua proses pendaftaran pelajar baharu dilaksana berdasarkan arahan kerja yang wujud di dalam Sistem Pengurusan Kualiti.	Tidak perlu pelan pemulihan
		Penambahbaikan dengan mewujudkan bilik khas bagi penyimpanan x-ray oleh Pusat Kesihatan Universiti.	
		Kepelbagaian kaedah pembayaran yuran pengajian telah diwujudkan oleh Pejabat Bursar.	

PENILAIAN RISIKO

Pelaksanaan kawalan di pelan pemulihan risiko

BIL.	PERKARA	TINDAKAN KAWALAN	TAHAP RISIKO SEBELUM	TAHAP RISIKO SELEPAS	PELAN PEMULIHAN RISIKO
1.	Bangunan yang menempatkan Pusat Data Utama di IDEC Beta dijangka akan menjadi ancaman kepada kesinambungan perkhidmatan Pusat Data/ICT, berdasarkan risiko berikut: a) Usia bangunan melebihi 50 tahun serta tidak pernah melalui proses pemeriksaan layak diduduki. b) Kedudukan Pusat Data di aras bawah (G floor) adalah berisiko tinggi (banjir) serta tidak mematuhi garis panduan pembangunan Pusat Data oleh pihak Uptime Institute (keperluan : aras satu). c) Pendawaian elektrik yang telah berusia lebih 30 tahun, berisiko menjadi punca kebakaran. d) Keluasan Pusat Data sekarang yang terhad (penuh) sudah tidak mampu menampung peningkatan pertambahan Server universti yang perlu diurus dimasa hadapan.	a) Membuat pemeriksaan bangunan selamat diduduki oleh pihak PPPA b) Memastikan persekitaran bangunan tersebut tidak berisiko untuk mengalami banjir dengan pihak PPPA *metigation* mengelakkan banjir di kawasan persekitaran. c) Naiktaraf pendawaian elektrik berusia lebih 30 tahun telah dilaksanakan d) Kemaskini susunatur pusat data dengan polisi perolehan server baharu mestilah dari jenis '*Rack Mounted'* sahaja.	H	M	Cadangan pembangunan Pusat Data baharu dengan memohon peruntukan melalui RMK11.

Kesan banjir di salah sebuah Universiti Awam di pantai timur semasa banjir besar tahun lepas



PENILAIAN RISIKO

Pelaksanaan kawalan di pelan pemulihan risiko

BIL.	PERKARA	TINDAKAN KAWALAN	TAHAP RISIKO SEBELUM	TAHAP RISIKO SELEPAS	PELAN PEMULIHAN RISIKO
2.	UPM masih menerima pembayaran yuran secara tunai bagi pelajar yang tidak membuat pembayaran melalui bank	a) Mengeluarkan surat kuasa kepada setiap pegawai yang membuat kutipan di setiap zon. b) Mengambil insuran bagi *cash in transit* dan pegawai yang membawa tunai dalam proses transit.	H	M	Sifar bayaran yuran pendaftaran secara tunai melalui kaedah pembayaran secara online melalui kemudahan “Jom PAY”
3.	Penerimaan laporan kesihatan oleh pelajar yang dijalankan daripada Pusat Perubatan luar	Memastikan setiap laporan perubatan dan xray pelajar diletakkan dalam sampul surat x-ray dan disimpan secara berkumpulan di dalam kotak khas.	H	M	Pemeriksaan perubatan perlu dilaksanakan di PKU sahaja dan penyimpanan data secara format digital sepenuhnya.

UNIVERSITI PUTRA MALAYSIA

AGRICULTURE • INNOVATION • LIFE

Terima Kasih | *Thank You*