TAKLIMAT PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013 (REFRESHER)

1 APRIL 2022 | 9.00 PAGI | MENERUSI APLIKASI ZOOM MEETING

PENGISIAN TAKLIMAT

01 LATAR BELAKANG PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

02 PELAKSANAAN ISMS DI UNIVERSITI PUTRA MALAYSIA

03 CONTOH PENEMUAN AUDIT SIRIM ISMS

TAKLIMAT PELAKSANAAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

Ts. Shahril Iskandar Amir
Timbalan Wakil Pengurusan ISMS UPM

LATAR BELAKANG PELAKSANAAN ISMS

APA ITU ISMS?

Pendekatan yang bersistematik dan berstruktur di dalam pengurusan maklumat.

Objektif ISMS adalah untuk mengurus dan melindungi keselamatan maklumat dengan pematuhan kepada piawaian MS ISO/IEC 27001 bagi memberi jaminan kepada pihak berkepentingan dan pelanggan bahawa **maklumat yang berkaitan adalah dilindungi dan selamat** dari kerosakan, hilang dan disalahguna.

STANDARD MS ISO/IEC 27001:2013

KENAPA PERLU ISMS?

1. **Arahan MAMPU** hasil keputusan Mesyuarat Jemaah Menteri pada 24 Februari 2010

2. **Pemantauan oleh KPT**

3. Menyediakan satu **pendekatan yang teratur dan sistematik** dalam **menilai risiko** dan **mengawal keselamatan maklumat universiti** dari segi **kerahsiaan, integriti** dan **ketersediaan**

4. Memberikan **jaminan** dan **keyakinan** kepada pelanggan dan pihak berkepentingan mengenai **tahap keselamatan maklumat universiti**

KENAPA PERLU ISMS?

…sistem pengurusan berasaskan pendekatan risiko

Penyelewengan data dan maklumat

Sistem maklumat mudah dicerobohi?

SISTEM MAKLUMAT TIDAK KEMAS KINI?

KONSEP KESELAMATAN MAKLUMAT

menekankan kepada konsep atau **prinsip keselamatan maklumat** iaitu **pemeliharaan kerahsiaan, integriti dan ketersediaan**.

KONSEP KESELAMATAN MAKLUMAT

C

- Maklumat mesti **dilindungi** & **tidak boleh didedahkan sewenangnya atau dibiarkan diakses tanpa kebenaran yang sah**
- **Tidak disebar** sewenang-wenangnya

KERAHSIAAN (CONFIDENTIALITY)

I

- **Menjamin** setiap **maklumat adalah sah, tepat, lengkap & kemaskini**

INTEGRITI

- Memastikan **akses terhad kepada pengguna yang sah** dan **maklumat adalah dari sumber yang sah**

A

- Memastikan **ketersediaan maklumat** apabila diperlukan oleh pengguna
- Data/maklumat hendaklah **boleh diakses pada bila-bila masa**

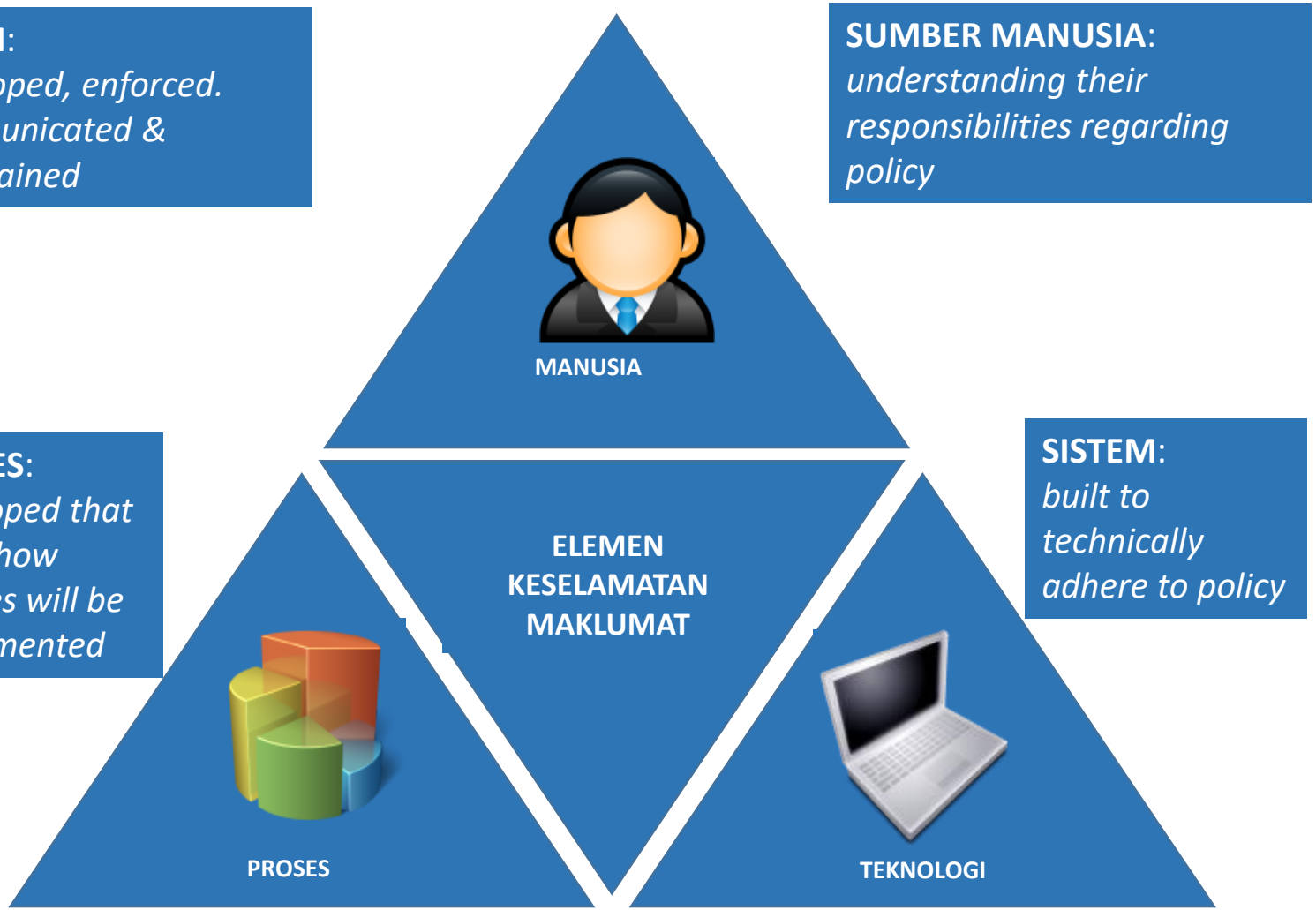
KETERSEDIAAN (AVAILABILITY)

ELEMEN KESELAMATAN MAKLUMAT

Dicapai dengan melaksanakan kawalan yang sesuai
(contoh: polisi, prosedur, garis panduan, amalan terbaik dan sebagainya)

POLISI:
developed, enforced. communicated & maintained

SUMBER MANUSIA:
understanding their responsibilities regarding policy

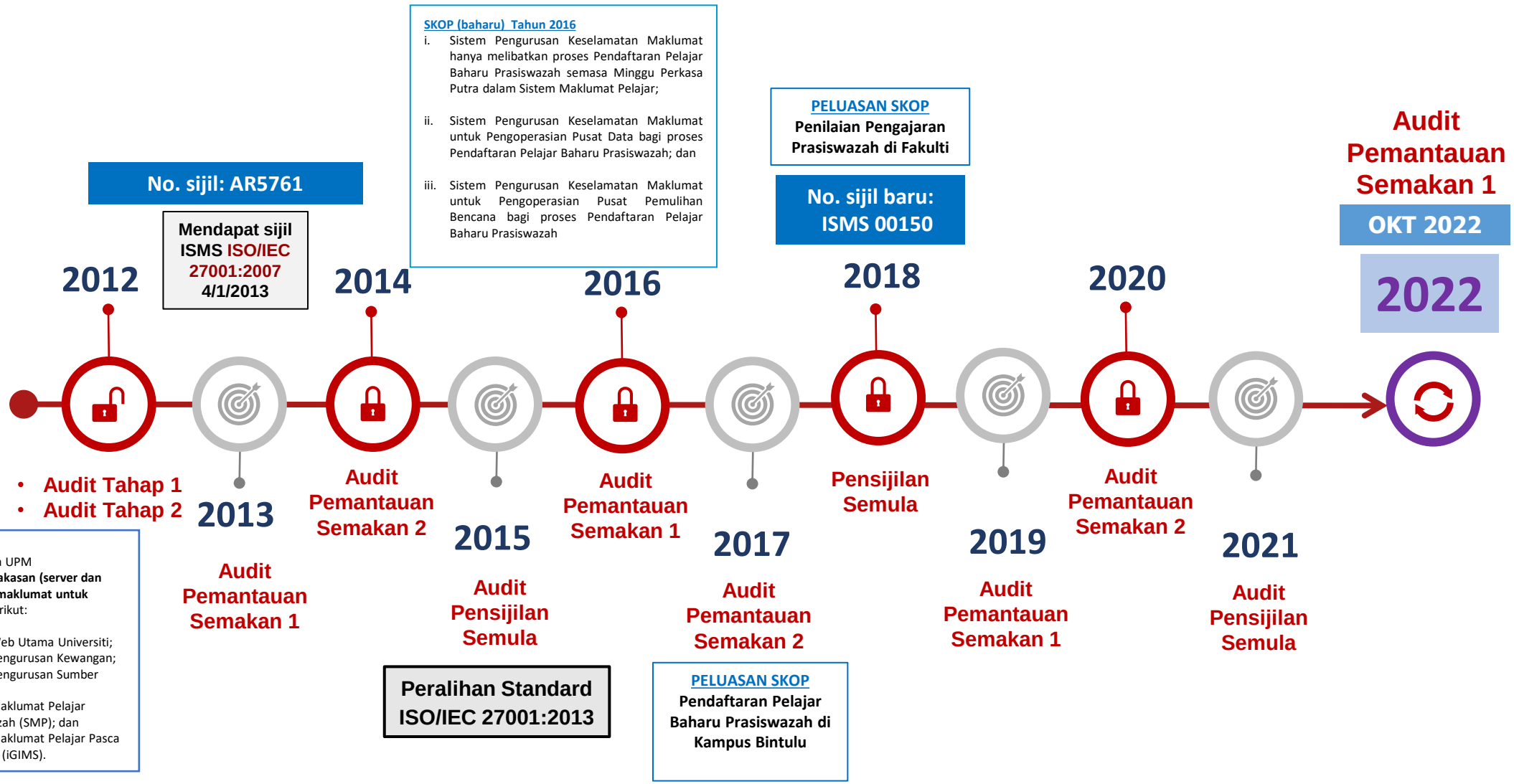


PROSES:
developed that show how policies will be implemented

SISTEM:
built to technically adhere to policy

PELAKSANAAN ISMS
Di UPM

PENGEKALAN PENSIJILAN ISO/IEC 27001



PENSIJILAN ISO/IEC 27001

TAHUN 2022:

UPM komited untuk pengekalan pensijilan

TELAH DIPERSIJILKAN DENGAN PENSIJILAN

(ISO/IEC 27001:2013)

MULAI TAHUN 2012 HINGGA KINI

INFORMATION SECURITY MANAGEMENT SYSTEMS
ISO
ISO/IEC 27001:2013

ISMS 00150

New!

SIRIM QAS INTERNATIONAL

SIJIL

SIRIM QAS International Sdn. Bhd. dengan ini mengesahkan bahawa

UNIVERSITI PUTRA MALAYSIA
43400 SERDANG
SELANGOR DARUL EHSAN
MALAYSIA

telah melaksanakan Sistem Pengurusan Keselamatan Maklumat yang menepati

ISO/IEC 27001:2013
Information Technology – Security Techniques – Information Security Management Systems – Requirements

Skop Pensijilan

1) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH MERANGKUMI AKTIVITI SEMAKAN TAWARAN HINGGA PENDAFTARAN KOLEJ KEDIAMAN.
2) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI.

INI ADALAH MENEPATI PENYATAAN PEMAKAIAN: TARIKH KEMASKINI 04 SEPTEMBER 2018

Issue date : 05 Oktober 2018
Validity period : 04 Januari 2019 - 03 Januari 2022
Certification No. : ISMS 00150

Mohd Azanuddin Salleh
Pengarah Urusan
SIRIM QAS International Sdn. Bhd.

No. Pensijilan: AR 5761

DASAR PENGURUSAN KESELAMATAN MAKLUMAT

Rujuk: e-ISO SISTEM PENGURUSAN ISO UNIVERSITI PUTRA MALAYSIA

PADA menjalankan kuasa yang diberikan oleh seksyen 20(1) Perlembagaan UPM, Lembaga Pengarah Universiti membuat Dasar berikut:

DASAR UNIVERSITI PUTRA MALAYSIA (SISTEM PENGURUSAN KESELAMATAN MAKLUMAT) 2019

Universiti Putra Malaysia beriltizam mengadakan Sistem Pengurusan Keselamatan Maklumat yang berkesan melalui:

a. pematuhan kepada kehendak organisasi dan perundangan serta peraturan;
b. pembangunan objektif dan matlamat berdasarkan objektif keselamatan;
c. komitmen bagi memenuhi keperluan berkaitan keselamatan maklumat;
d. penilaian semula dan pengubahsuaian dasar, objektif dan sasaran untuk penambahbaikan berterusan.

Pemansuhan

Dasar Universiti Putra Malaysia (Sistem Pengurusan Keselamatan Maklumat) 2014 yang dibuat oleh Lembaga Pengarah Universiti (LPU) dalam Mesyuarat LPU pada 9 Disember 2014 (Minit LPU ke-103) adalah dimansuhkan.

Dibuat 10 Disember 2019
[Minit Mesyuarat LPU ke-138/04]
[UPM/PPUU/100-1/1/2 (DasarISMS/UPM.CQA.100-13/1/3]

TAN SRI DR. GHAUTH JASMON
Pengerusi Lembaga Pengarah Universiti Putra Malaysia

PERTANIAN • INOVASI • KEHIDUPAN

Universiti Putra Malaysia beriltizam mengadakan sistem pengurusan keselamatan maklumat yang berkesan melalui:

1. **pematuhan kepada kehendak organisasi dan perundangan serta peraturan;**
2. **pembangunan objektif dan matlamat berdasarkan objektif keselamatan;**
3. **komitmen bagi memenuhi keperluan berkaitan keselamatan maklumat; dan**
4. **penilaian semula dan pengubahsuaian dasar, objektif dan sasaran untuk penambahbaikan berterusan.**

Pernyataan Dasar Sistem Pengurusan Keselamatan Maklumat UPM yang dibuat oleh Lembaga Pengarah Universiti (LPU) pada 10 DISEMBER 2019

(Nota: LPU adalah pemegang kuasa pembuat dasar)

STRUKTUR PENGURUSAN KUALITI UPM

NAIB CANSELOR
Profesor Dr. Mohd Roslan Sulaiman

WAKIL PENGURUSAN UPM
Profesor Dr. Amin Ismail
(Pengarah, Pusat Jaminan Kualiti)

PENYELARAS ISO
Pn. Haslida Hassan
(Ketua Bahagian Pengurusan Kualiti Perkhidmatan, Pusat Jaminan Kualiti)

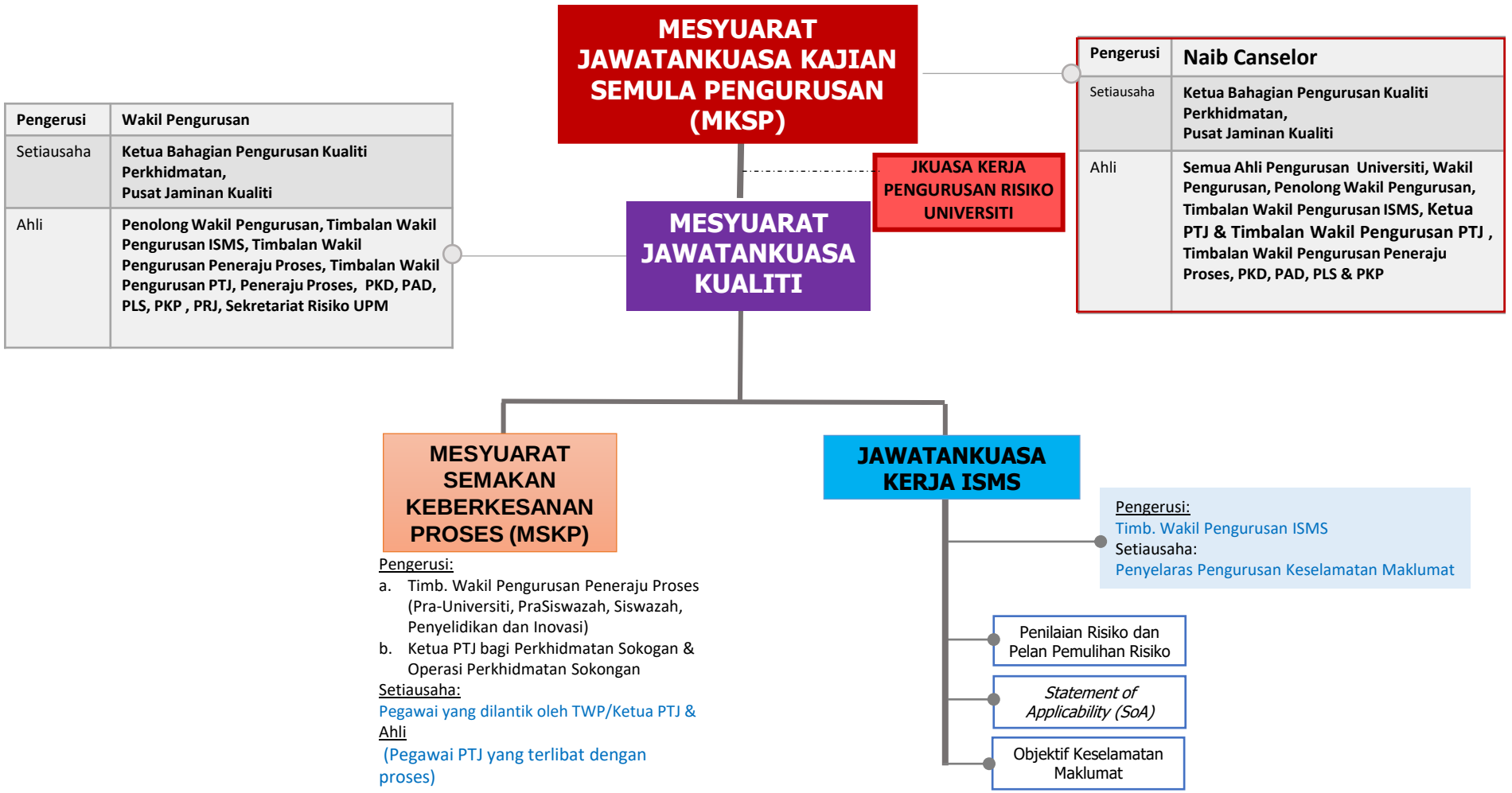
PENOLONG WAKIL PENGURUSAN UPM
Profesor Dr. Noor Azman Ali
(Timb. Pengarah, Pusat Jaminan Kualiti)

SISTEM PENGURUSAN KUALITI (QMS)
Timbalan Wakil Pengurusan terdiri daripada Pentadbir gred tertinggi di PTJ
- Pejabat, Fakulti, Institut, Akademi, Pusat dan Sekolah

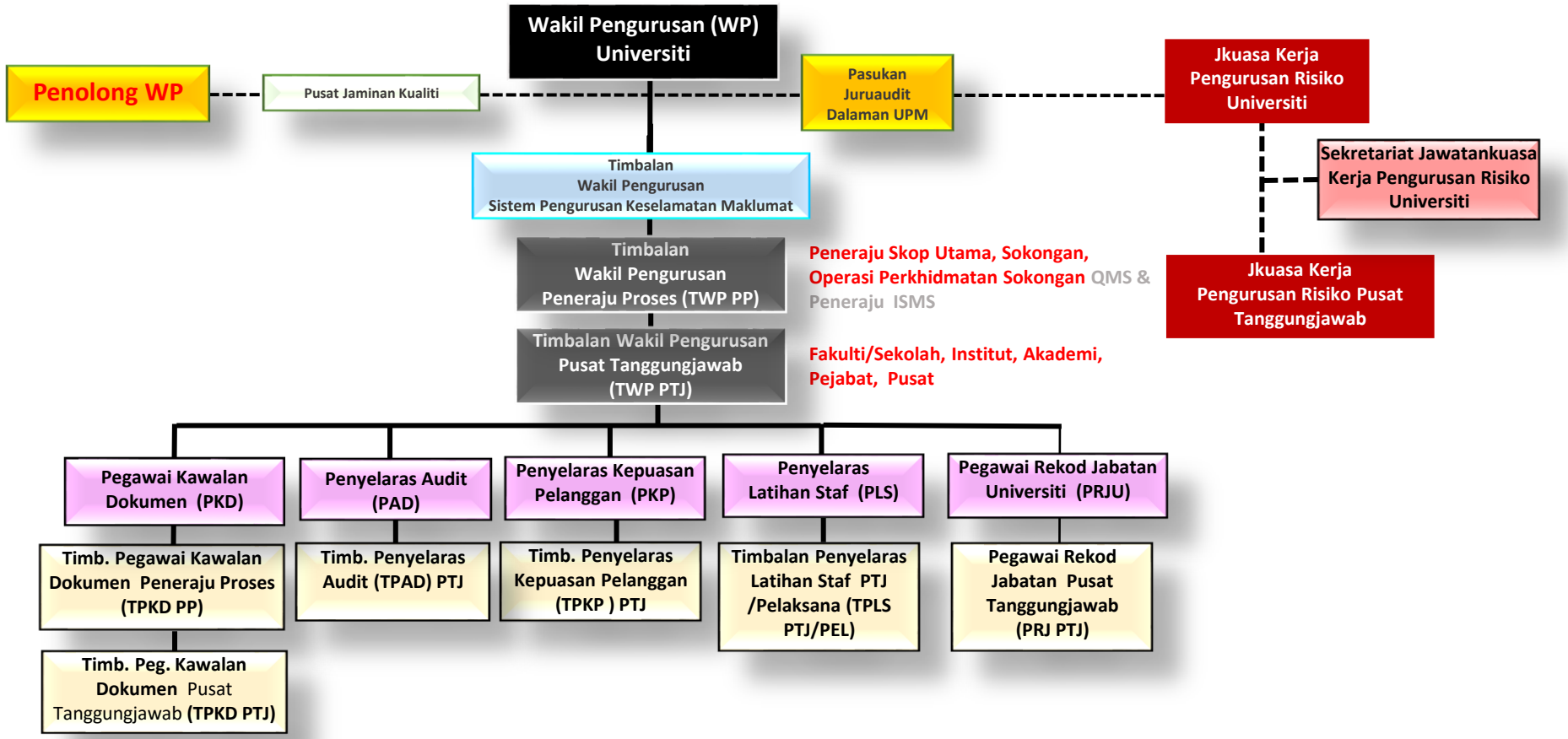
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
TIMBALAN WAKIL PENGURUSAN ISMS
Ts. Shahril Iskandar Amir
(Pusat Pembangunan Maklumat dan Komunikasi)

PENYELARAS ISMS
Pn. Shamriza Shari
(Pusat Jaminan Kualiti)

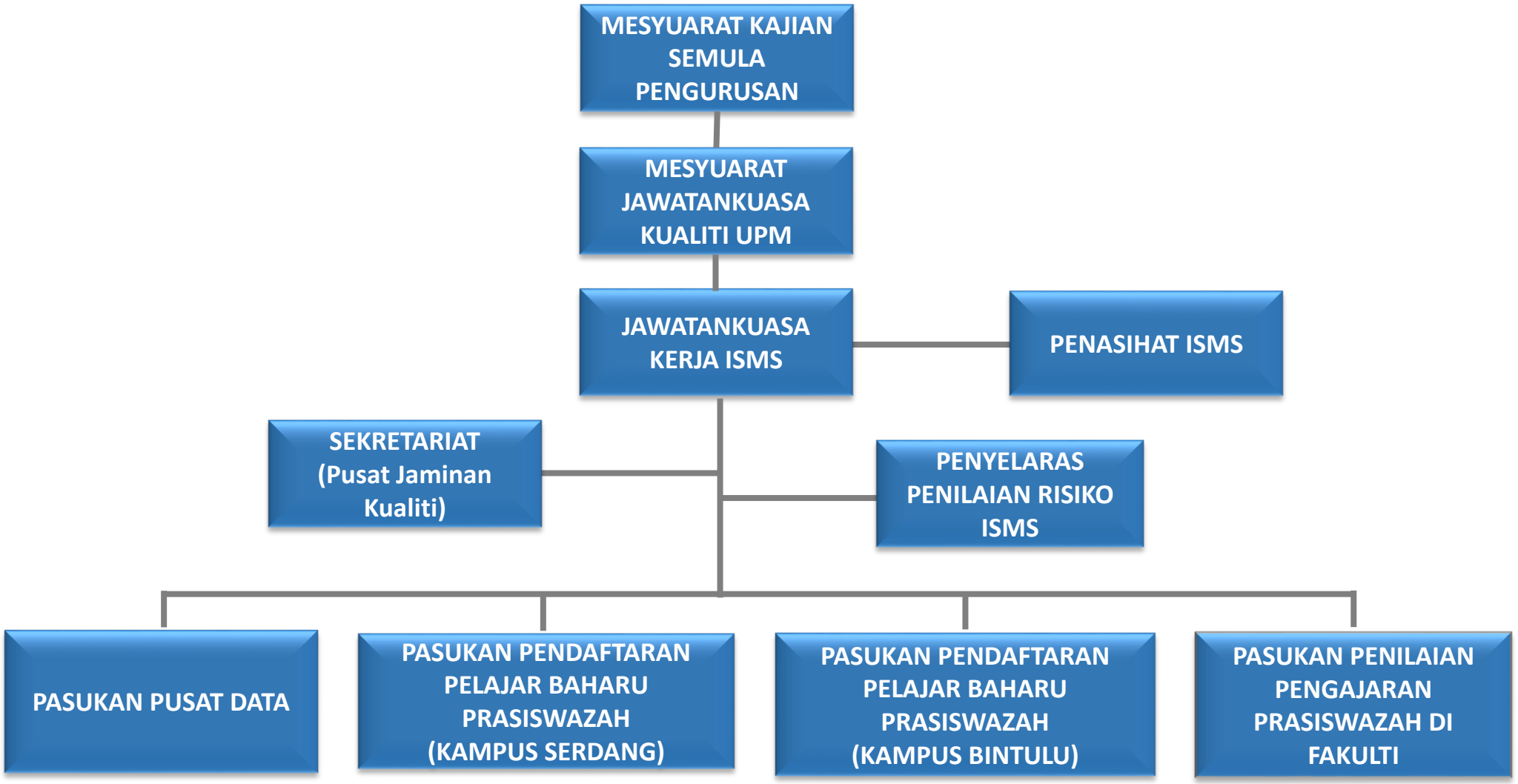
PENGURUSAN & PEMANTAUAN KESELURUHAN KUALITI UPM



STRUKTUR ORGANISASI JAMINAN KUALITI PERKHIDMATAN UPM



STRUKTUR KESELAMATAN MAKLUMAT UPM



STRATEGI PELAN PELAKSANAAN ISMS UPM

1. Tentukan halatuju
2. Tentukan pihak yang berkepentingan kepada UPM
3. Kenalpasti hubung kait skop ISMS
4. Selarikan objektif ISMS dengan strategi UPM
5. Menukarkan polisi keselamatan maklumat tahap tertinggi
6. Melakukan perubahan Risk Assessment (RA)
7. Kenalpasti status kawalan SoA
8. Mendapatkan pengesahan daripada Risk Owner
9. Merancang komunikasi secara sistematik
10. Kenal pasti polisi dan prosedur baru
11. Penyusunan semula kawalan
12. Pengukuran dan pelaporan

13. **PENSIJILAN ISMS**

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 Universiti, 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 Kampus Serdang**

2017

- **PELUASAN ENTITI Proses Pendaftaran pelajar baharu Prasiswazah ke Kampus Bintulu**

2018

- **PELUASAN SKOP** kepada **Proses Penilaian Pengajaran Prasiswazah di Fakulti**

- **PELAKSANAAN KAEDAH BAHARU** iaitu **Sistem Kad-Maya (Putra VID)** bagi **kawalan keselamatan pelajar dalam Proses Pendaftaran Pelajar Baharu**

2022

- **Gerak kerja ke arah PERLUASAN SKOP Proses Pendaftaran Pelajar Baharu Sepenuh Masa Siswazah Tahun 2023**

SKOP PENSIJILAN

1) Sistem Pengurusan Keselamatan Maklumat bagi **Proses Pendaftaran Pelajar Baharu Prasiswazah Merangkumi Aktiviti Semakan Tawaran hingga Pendaftaran Kolej Kediaman**

2) Sistem Pengurusan Keselamatan Maklumat bagi **Proses Penilaian Pengajaran Prasiswazah di Fakulti**

KECUALI:
Pendaftaran kursus dan aktiviti kemasukan pendaftaran pelajar baharu prasiswazah untuk:

i. **Pengajian Jarak Jauh;**
ii. **Program untuk Eksekutif; dan**
iii. **Antarabangsa.**

SIRIM QAS INTERNATIONAL

SIJIL

SIRIM QAS International Sdn. Bhd. dengan ini mengesahkan bahawa

UNIVERSITI PUTRA MALAYSIA
43400 SERDANG
SELANGOR DARUL EHSAN
MALAYSIA

telah melaksanakan Sistem Pengurusan Keselamatan Maklumat yang menepati

ISO/IEC 27001:2013
Information Technology – Security Techniques – Information Security Management Systems – Requirements

Skop Pensijilan

1) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH MERANGKUMI AKTIVITI SEMAKAN TAWARAN HINGGA PENDAFTARAN KOLEJ KEDIAMAN.
2) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI.

INI ADALAH MENEPATI PENYATAAN PEMAKAIAN:
TARIKH KEMASKINI 04 SEPTEMBER 2018

Issue date : 05 Oktober 2018
Validity period : 04 Januari 2019 - 03 Januari 2022
Certification No. : ISMS 00150

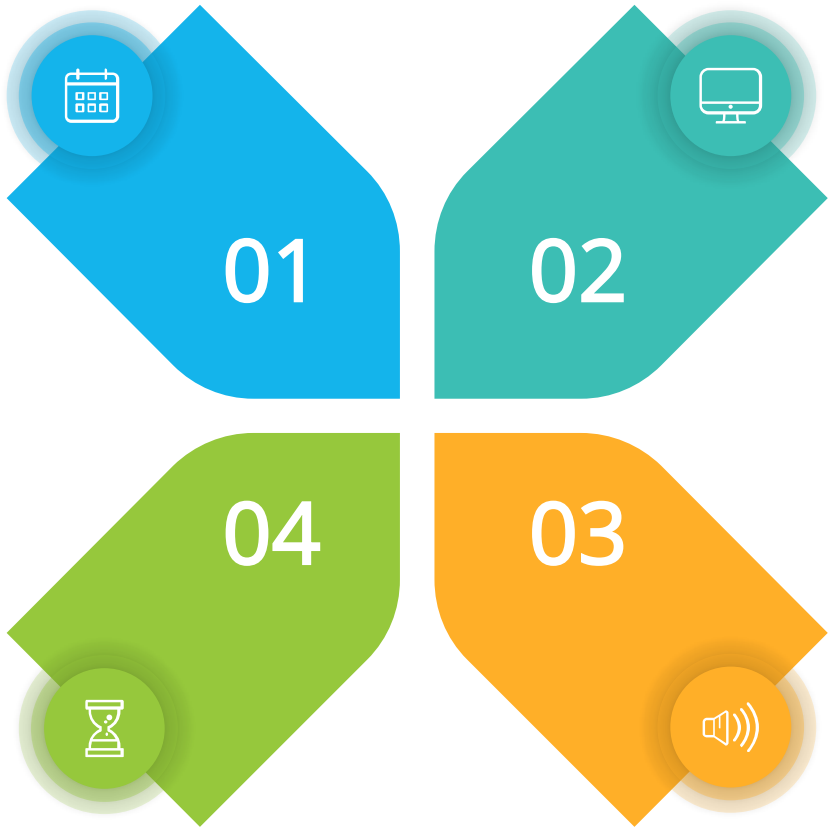
Mohd Azanuddin Salleh
Pengarah Urusan
SIRIM QAS International Sdn. Bhd.

Penganugerahan sijil ini tertakluk kepada peraturan-peraturan dan syarat-syarat seperti ternyata dalam Perjanjian Pensijilan.

Nota:
UPM masih menunggu pengeluaran Sijil ISMS terkini daripada pihak SIRIM selepas berjaya melepasi Audit Pensijilan Semula pada tahun 2021.

OBJEKTIF KESELAMATAN MAKLUMAT

Memastikan tahap keyakinan pelajar baharu terhadap keselamatan maklumat semasa proses pendaftaran

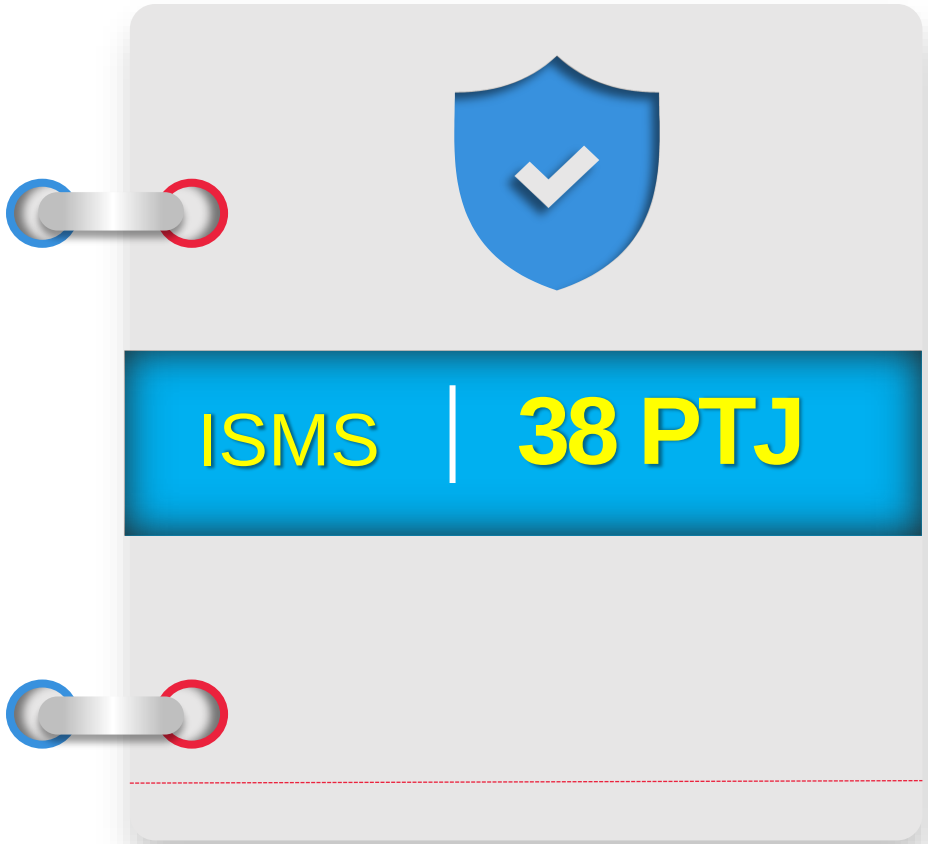


Memastikan ketersediaan aplikasi Penilaian Pengajaran (BlastTA) untuk urusan penilaian pengajaran

Memastikan keyakinan pelajar terhadap keselamatan maklumat penilaian pengajaran berada pada tahap baik

Memastikan ketersediaan aplikasi Sistem Maklumat Pelajar (SMP) untuk urusan pendaftaran pelajar baharu

PUSAT TANGGUNGJAWAB (PTJ) TERLIBAT



e-ISO SISTEM PENGURUSAN ISO UNIVERSITI PUTRA MALAYSIA

MUAT TURUN

- Takwim Aktiviti ISO
- Minit Mesyuarat:
  + Jawatankuasa Kerja ISMS UPM
  + Jawatankuasa Kualiti UPM
  + Kajian Semula Pengurusan (MKSP)
- Laporan/Tindakan Susulan MKSP
- Slaid Pembentangan
- Senarai Kod Proses dan PTJ Pengurusan ISO
- Buku Keperluan Standard ISO
- Sijil Sistem Pengurusan ISO
- Penggunaan Logo ISO
- Nota Akreditasi Makmal ISO/IEC 17025
- Garis Panduan Pengurusan Risiko UPM
- Kad Kecil Dasar Kualiti dan Objektif Kualiti UPM
- Senarai Juruaudit Dalaman ISO UPM
- Senarai PTJ di Bawah Skop Pensijilan ISO
- Senarai Fasilitator ISO & Inovasi UPM

PUSAT TANGGUNGJAWAB (PTJ) TERLIBAT

Pusat Tanggungjawab
1. Pusat Jaminan Kualiti (CQA)
2. Pejabat Pendaftar
3. Pejabat Bursar
4. Pusat Strategi dan Perhubungan Korporat (PSPK)
5. Pejabat Penasihat Undang-Undang (PPUU)
6. Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan (PPKKP)
7. UPM Kampus Bintulu
8. Semua Fakulti & Sekolah Perniagaan dan Ekonomi (14 PTJ)
9. Bahagian Hal Ehwal Pelajar (BHEP)

Pusat Tanggungjawab
10. Bahagian Perumahan dan Penempatan UPM (BPP)
11. Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik (BKAD)
12. Semua Kolej Kediaman (9 PTJ)
13. Pusat Pembangunan Maklumat dan Komunikasi (iDEC)
14. Perpustakaan Sultan Abdul Samad (PSAS)
15. Bahagian Keselamatan Universiti (BKU)
16. Pusat Kesihatan Universiti (PKU)
17. Pusat Pembangunan Akademik (CADe)

DOKUMEN RUJUKAN UTAMA ISMS UPM

PORTAL SISTEM PENGURUSAN ISO UPM (e-ISO)

CERTIFIED TO ISO 9001:2015 CERT. NO. : QMS 00794

CERTIFIED TO ISO/IEC 27001:2013 CERT. NO. : ISMS 00150

Kemaskini terkini pada 1 Disember 2021

LATARBELAKANG ISO

- Sistem Pengurusan Kualiti (QMS) ISO 9001
- Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001

OBJEKTIF KUALITI & OBJEKTIF ISMS

OBJEKTIF KUALITI

- Petunjuk Prestasi Utama (KPI) UPM
- Pelan Tindakan Peringkat Fungsian dan Aras
- Piagam Pelanggan

OBJEKTIF ISMS

- Objektif Sistem Pengurusan Keselamatan Maklumat

DASAR ISO

- Dasar Kualiti
- Dasar ISMS

MODEL PENDEKATAN PROSES ISO

- Model Pendekatan Proses SPK

PENGURUSAN RISIKO ISO

- Dokumen Risiko Operasi Sistem Pengurusan Kualiti (QMS)
- Dokumen Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS)

KAWALAN DOKUMEN DAN REKOD ISO

- Graf Statistik Dokumen ISO UPM
- Jadual/Laporan Terperinci Statistik Dokumen Mengikut Peneraju
- Senarai Utama Dokumen Terkawal ISO
- Dokumen Rujukan ISO
  - + Dokumen Rujukan Pelaksanaan Sistem Pengurusan Keselamatan Maklumat - Kemaskini 1/12/2021
  - + Penyata Pemakaian (Statement of Applicability (SoA)) - Kemaskini 1/12/2021
  - + Panduan Penilaian Risiko Aset Sistem Pengurusan Keselamatan Maklumat
- Dokumen Rujukan Luaran/Dalaman Lain
- Cadangan Pindaan/Tambahan Dokumen (CPD)
  - + Jadual Tindakan Kuatkuasa Dokumen ISO 2022
  - + Surat Hebahan Perubahan Dokumen
  - + Senarai Perincian/Perubahan Dokumen
  - + Panduan Penyediaan/Pindaan Dokumen
- Pengurusan Rekod Universiti
- Dokumen Skop Sistem Pengurusan Kualiti dan Pihak Berkepentingan Pusat Tanggungjawab
- Dokumen Sistem Pengurusan Keselamatan Maklumat
  - + Pihak Berkepentingan ISMS & Keperluan Mereka
  - + Isu Dalaman & Isu Luaran ISMS

SWAAKREDITASI SELF-ACCREDITATION MQA/SA/0004 2010

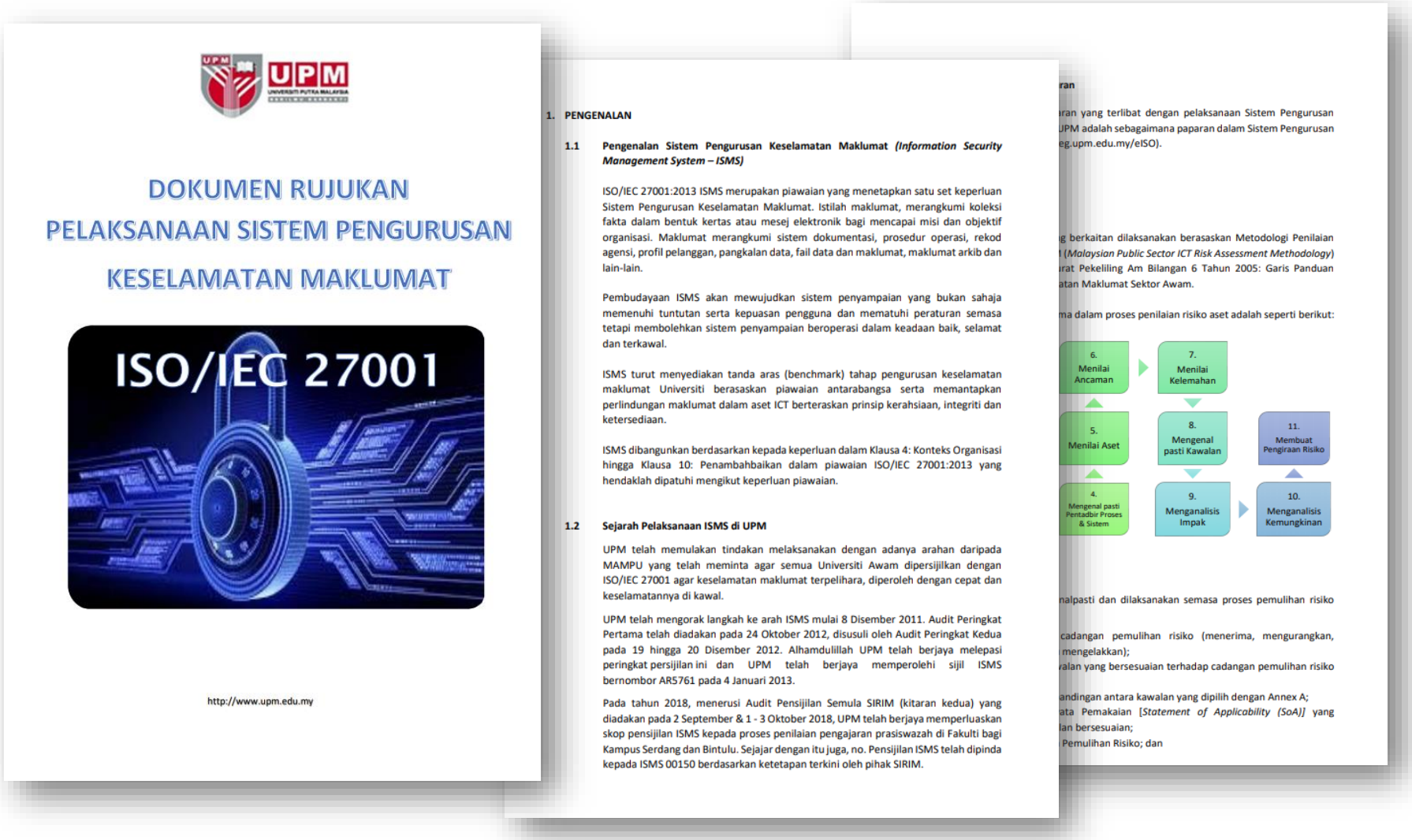
...DITASI (PENGURUSAN KUALITI ...)

- ...editasi Program Pengajian

MUAT TURUN

- Takwim Aktiviti ISO
- Minit Mesyuarat:
  - + Jawatankuasa Kerja ISMS UPM
  - + Jawatankuasa Kualiti UPM
  - + Kajian Semula Pengurusan (MKSP)
- Laporan/Tindakan Susulan MKSP
- Slaid Pembentangan
- Senarai Kod Proses dan PTJ Pengurusan ISO
- Buku Keperluan Standard ISO
- Sijil Sistem Pengurusan ISO
- Penggunaan Logo ISO
- Nota Akreditasi Makmal ISO/IEC 17025
- Garis Panduan Pengurusan Risiko UPM
- Kad Kecil Dasar Kualiti dan Objektif Kualiti UPM
- Senarai Juruaudit Dalaman ISO UPM
- Senarai PTJ di Bawah Skop Pensijilan ISO
- Senarai PTJ Diaudit SIRIM Tahun 2015 - 2020
- Senarai Fasilitator ISO & Inovasi UPM

DOKUMEN RUJUKAN PELAKSANAAN ISMS UPM



Merupakan Dokumen Rujukan Utama Pelaksanaan ISMS di UPM yang mengandungi maklumat seperti Dasar, Skop Pensijilan, PTJ terlibat, Pihak Berkepentingan dan Keperluan Mereka, Isu Dalaman & Luaran, Pengurusan Risiko, Penyata Pemakaian (SoA), Jawatankuasa dan Peranan serta SOP terlibat dengan pelaksanaan ISMS di UPM.

DOKUMEN PENYATA PEMAKAIAN (SOA)

Dokumen Penyata Pemakaian (Statement of Applicability (SoA)) menggariskan objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013 selaras dengan keperluan Sistem Pengurusan Keselamatan Maklumat di Universiti Putra Malaysia.

PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

1.0 PENGENALAN

Dokumen Penyata Pemakaian (*Statement of Applicability* (SoA)) menggariskan objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013 selaras dengan keperluan Sistem Pengurusan Keselamatan Maklumat di Universiti Putra Malaysia.

2.0 TUJUAN

Dokumen ini bertujuan untuk menetapkan proses yang perlu dipatuhi dalam menyediakan SoA.

3.0 PROSES PENYATA PEMAKAIAN (SoA)

3.1 PENYEDIAAN SoA

Proses yang terlibat dalam penyediaan SoA merangkumi:

(a) Memahami keperluan SoA dalam Standard MS ISO/IEC 27001:2013.

(b) Menyediakan kandungan SoA dengan mengambil kira aspek berikut:

(i) Menyenaraikan semua objektif kawalan dan kawalan di Annex A dalam Standard MS ISO/IEC 27001:2013;

(ii) Memberi jawapan **"Ya"** dengan justifikasi pemilihan kepada objektif kawalan dan kawalan selaras dengan **penemuan Pelan Pemulihan Risiko**;

(iii) Memberi jawapan **"Ya"** kepada objektif kawalan dan kawalan **yang sedang dilaksanakan**;

(iv) Memberi jawapan **"Separa"** kepada kawalan yang **masih dalam pembangunan;**

(v) Menyenaraikan **nama prosedur / panduan / dokumen** yang dirujuk bagi menyokong pelaksanaan objektif kawalan dan kawalan tersebut; dan

(vi) Memberi jawapan **"Tidak"** kepada objektif kawalan dan kawalan yang **tidak dipilih** dengan alasan pengecualiannya.

(c) Membentangkan cadangan awal SoA dalam Mesyuarat Jawatankuasa Kerja ISMS.

3.2 PELAKSANAAN SoA

Pelaksanaan SoA hendaklah mengambil kira aspek berikut:

(a) Memaklumkan kepada semua pengguna ISMS berhubung penguatkuasaan dokumen SoA;

(b) Melaksanakan program kesedaran pematuhan semua peraturan Polisi ISMS selaras dengan keperluan SoA;

PENYATA PEMAKAIAN
(STATEMENT OF APPLICABILITY)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

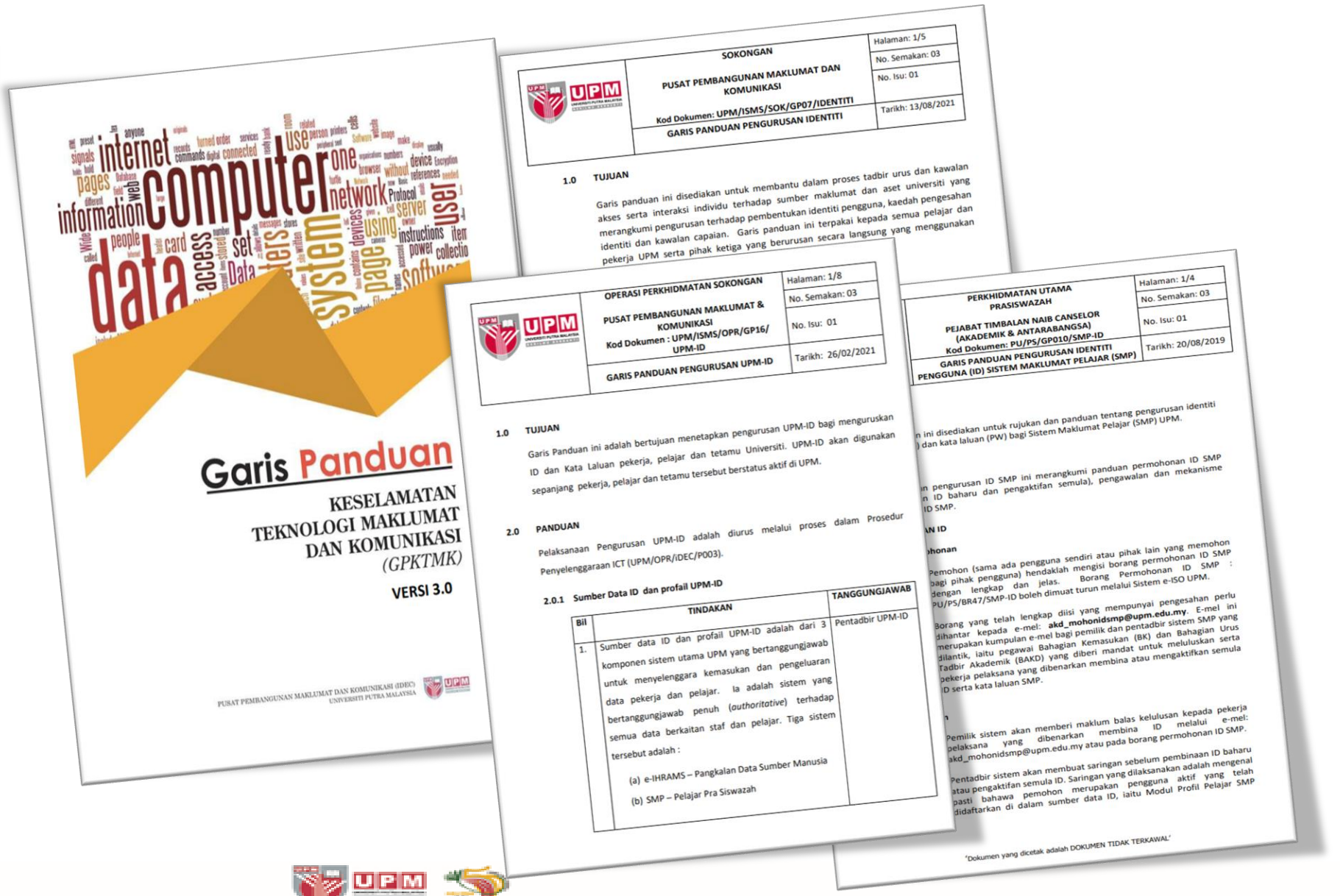
Lampiran A: SoA Pensijilan MS ISO/IEC 27001:2013 ISMS Universiti Putra Malaysia

Kawalan ISO/IEC 27001:2013			Pemilik Proses	Terpakai (Ya/Tidak)	Dilaksanakan (Ya/Separa/ Tidak)	Justifikasi	Kawalan Semasa
Klausa	**Sek**	**Objektif Kawalan/ Kawalan**					
A.5 DASAR KESELAMATAN MAKLUMAT	A.5.1	**Hala tuju pengurusan untuk keselamatan maklumat** Menyediakan hala tuju dan sokongan pengurusan untuk keselamatan maklumat menurut keperluan perniagaan serta undang-undang dan peraturan yang berkaitan.					
	A.5.1.1	**Dasar keselamatan maklumat** Satu set dasar untuk keselamatan maklumat hendaklah ditakrifkan, diluluskan oleh pengurusan, diterbitkan dan disampaikan kepada kakitangan dan pihak luaran yang berkaitan.	Pusat Jaminan Kualiti	YA	YA	Memastikan kawalan keselamatan maklumat dibangunkan dan disahkan oleh Pengurusan Atasan dan disampaikan kepada umum.	• Dasar ISMS UPM - diluluskan oleh Pengerusi Lembaga Pengarah Universiti - dikomunikasi menerusi Portal eISO UPM
	A.5.1.2	**Kajian semula dasar untuk keselamatan maklumat** Dasar untuk keselamatan maklumat hendaklah dikaji semula pada sela masa yang dirancang atau jika berlaku perubahan yang ketara bagi memastikan kesesuaian, kecukupan dan keberkesanannya berterusan.	Pusat Jaminan Kualiti	YA	YA	Memastikan dasar sentiasa terkini berdasarkan skop dan pelaksanaan ISMS.	• Semakan berkala dilaksanakan semasa Mesyuarat Kajian Semula Pengurusan ISMS UPM

SOP KAWALAN ID DAN KATA LALUAN

e-ISO SISTEM PENGURUSAN ISO UNIVERSITI PUTRA MALAYSIA

1. Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK)
2. Garis Panduan Pengurusan Identiti (UPM/ISMS/SOK/GP07 /IDENTITI)
3. Garis Panduan Pengurusan UPM-ID (UPM/ISMS/OPR/ GP16/UPM-ID)
4. Garis Panduan Pengurusan Identiti Pengguna (ID) Sistem Maklumat Pelajar (SMP)(PU/PS/GP010/ SMP-1D)



DOKUMENTASI ISMS UPM

BAGAIMANA INGIN RUJUK DOKUMEN ISMS?

1

Layari laman sesawang
http://www.reg.upm.edu.my/eISO

DOKUMENTASI ISMS UPM

2

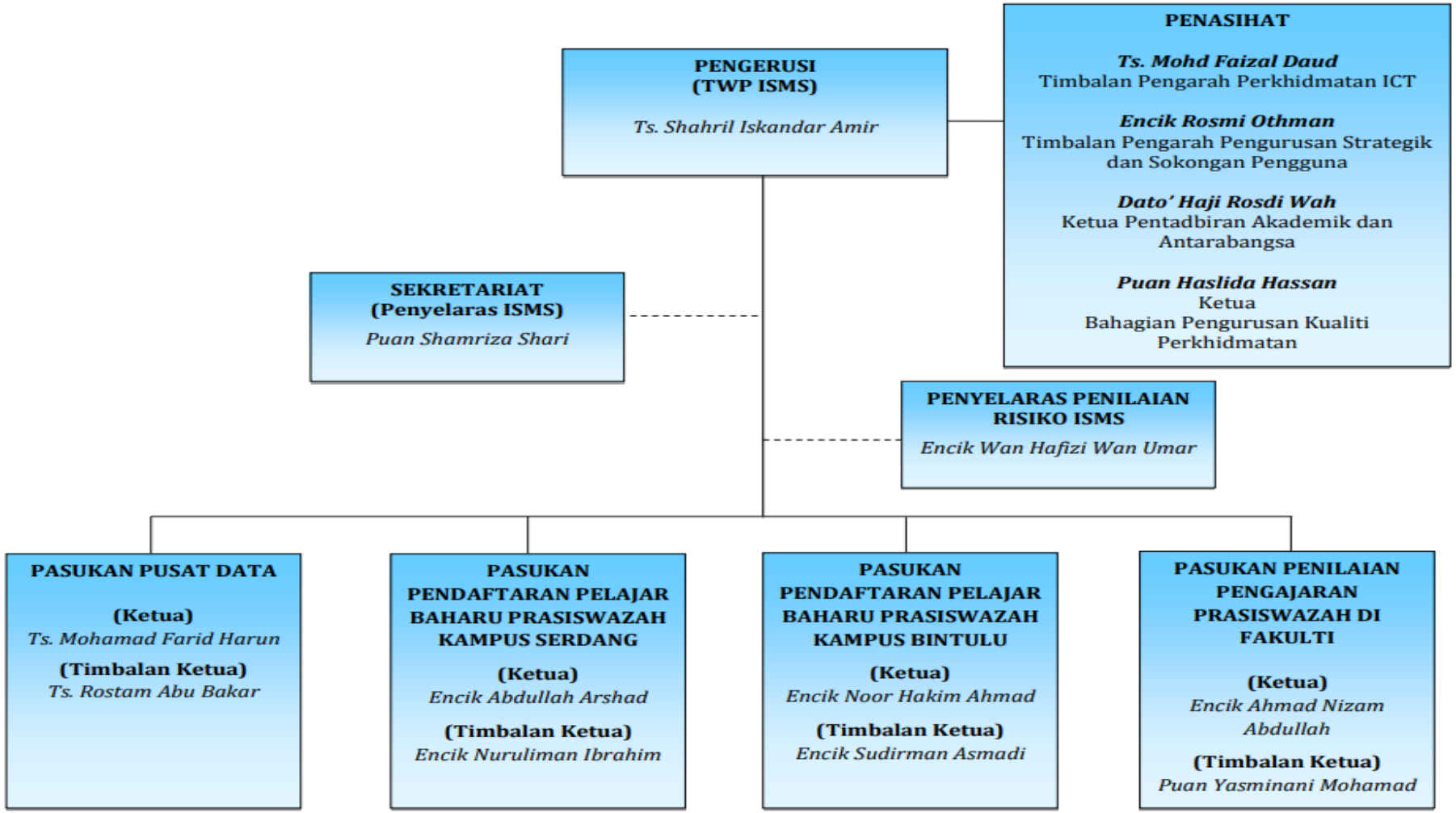
Klik pada dokumen ISMS ISO/IEC 27001

Bil.	Kod Dokumen	Nama Dokumen
1.	Prosedur	
	1. UPM/ISMS/OPR/P001	PROSEDUR PENGOPERASIAN PENGURUSAN PUSAT DATA BARU!
	2. UPM/ISMS/OPR/P002	PROSEDUR PEMANTAUAN OPERASI PUSAT DATA
	3. UPM/ISMS/OPR/P003	PROSEDUR KAWALAN DAN PEMANTAUAN CAPAIAN KE SISTEM DI PUSAT DATA
2.	Arahan Kerja	
	1. UPM/ISMS/OPR/AK07	ARAHAN KERJA PELUPUSAN PITA BACKUP DAN LAIN-LAIN MEDIA SIMPANAN BARU!
3.	Garis Panduan	
	1. UPM/ISMS/OPR/GP01/ PENYELENGGARAAN OPERASI	GARIS PANDUAN PENYELENGGARAAN OPERASI PUSAT DATA
	2. UPM/ISMS/OPR/GP02/ PENYEDIAAN SERVER	GARIS PANDUAN PENYEDIAAN SERVER DI PUSAT DATA
	3. UPM/ISMS/OPR/GP03/KAWALAN AKSES	GARIS PANDUAN KAWALAN AKSES KE PUSAT DATA
	4. UPM/ISMS/OPR/GP05/ PEMANTAUAN OPERASI	GARIS PANDUAN PEMANTAUAN OPERASI PUSAT DATA
	5. UPM/ISMS/OPR/GP06/ PEMANTAUAN CAPAIAN	GARIS PANDUAN PEMANTAUAN CAPAIAN KE SISTEM
	6. UPM/ISMS/OPR/GP08/MAKLUMAT LOG	GARIS PANDUAN PERLINDUNGAN MAKLUMAT LOG SERVER
	7. UPM/ISMS/OPR/GP09/TAHAP KESELAMATAN	GARIS PANDUAN PENILAIAN TAHAP KESELAMATAN
	8. UPM/ISMS/OPR/GP13/AGIHAN RANGKAIAN	GARIS PANDUAN PENGURUSAN PENGAGIHAN RANGKAIAN
	9. UPM/ISMS/OPR/GP14/BACKUP	GARIS PANDUAN PENGURUSAN BACKUP PANGKALAN DATA DAN APLIKASI BARU!
	10. UPM/ISMS/OPR/GP16 UPM-ID	GARIS PANDUAN PENGURUSAN UPM-ID

STRUKTUR ORGANISASI JAWATANKUASA KERJA ISMS UPM

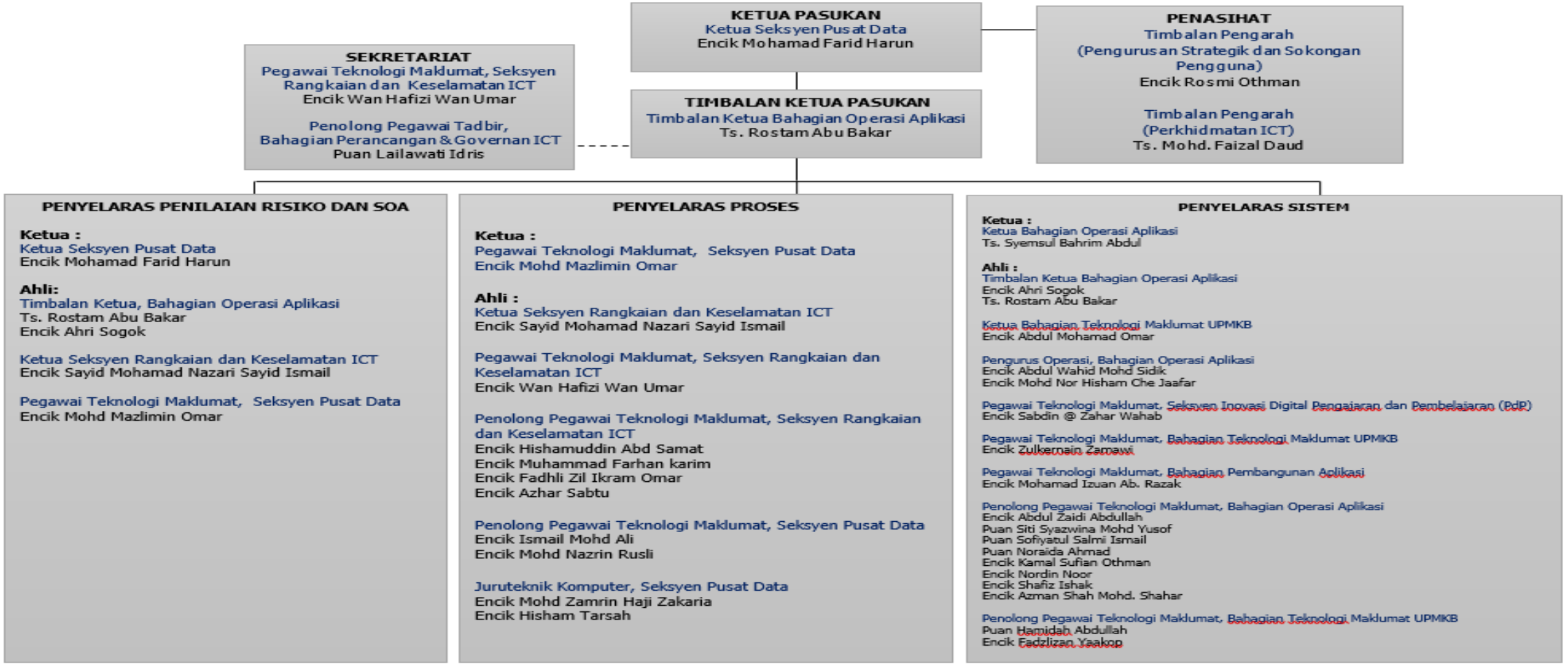
Kemaskini: 7 Februari 2022

STRUKTUR JAWATANKUASA KERJA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001:2013



STRUKTUR ORGANISASI PASUKAN ISMS UPM

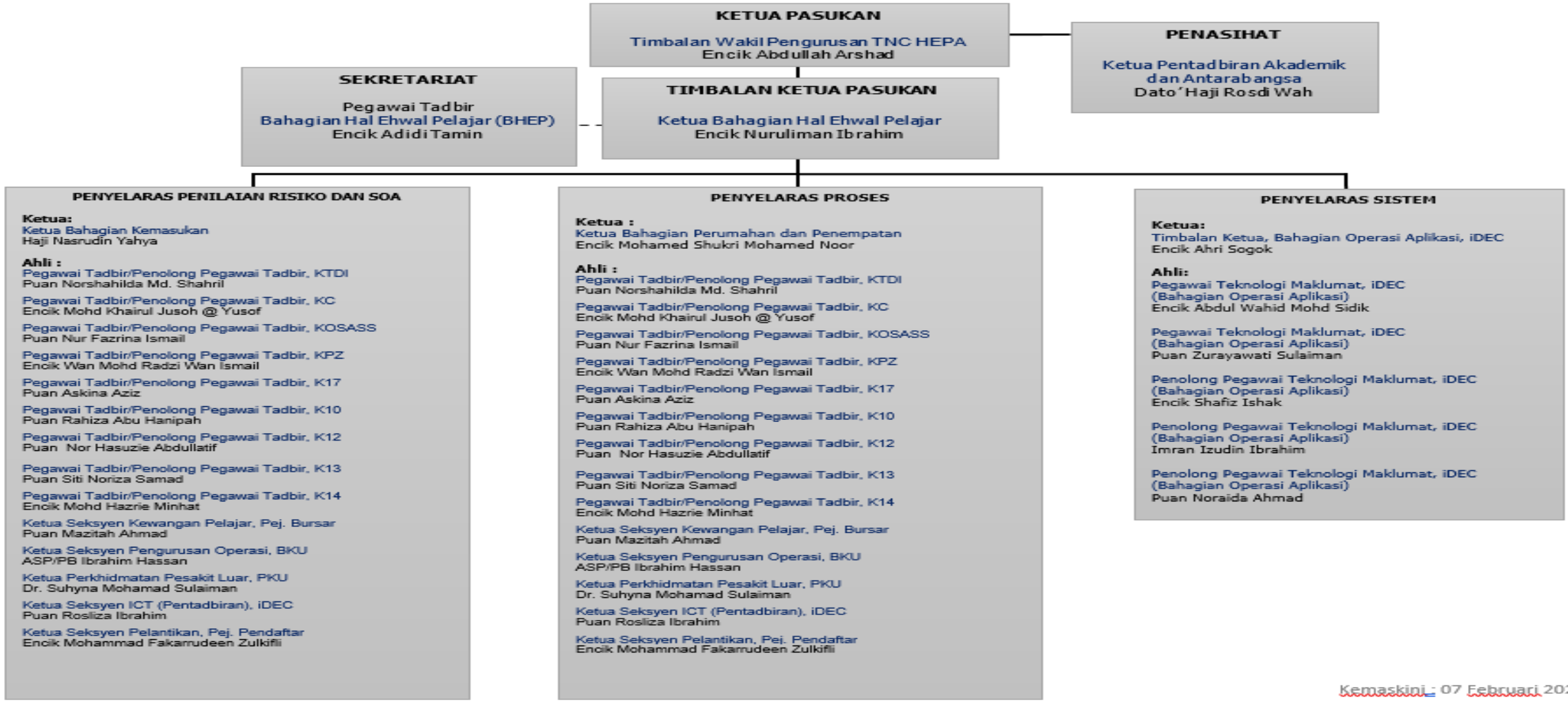
STRUKTUR ORGANISASI PASUKAN PUSAT DATA



Kemaskini: 01.07.2021

STRUKTUR ORGANISASI PASUKAN ISMS UPM

STRUKTUR ORGANISASI PASUKAN PENDAFTARAN PELAJAR BAHARU PRASISWAZAH KAMPUS SERDANG



Kemaskini : 07 Februari 2022

STRUKTUR ORGANISASI PASUKAN ISMS UPM

STRUKTUR ORGANISASI PASUKAN PENDAFTARAN PELAJAR BAHARU PRASISWAZAH KAMPUS BINTULU

SEKRETARIAT
Pegawai Tadbir, Fakulti Kemanusiaan, Pengurusan dan Sains
Cik Nurul Haziqah Hasan

Pegawai Tadbir, Fakulti Sains Pertanian dan Perhutanan
Encik Dexter Alvin Anak Menari

KETUA PASUKAN
Timbalan Wakil Pengurusan
Encik Noor Hakim Ahmad

TIMBALAN KETUA PASUKAN
Ketua Bahagian Pengurusan Akademik & Penyelidikan
Encik Sudirman Asmadi

PENASIHAT
Pengarah UPMKB
Prof Madya Dr. Shahrul Razid Sarbini

PENYELARAS PENILAIAN RISIKO DAN SOA

Ketua:
Pegawai Tadbir, Bahagian Pentadbiran
Encik Mohd Amaludin Salleh

Ahli:
1. Pegawai Tadbir, BHEP
   Encik Mohamad Syukri Mohamad Adnan
2. Pegawai Teknologi Maklumat, BTM
   Encik Zulkernain Zamawi

PENYELARAS PROSES

Ketua:
Pegawai Tadbir, Bahagian Hal Ehwal Pelajar (BHEP)
Encik Mohamad Syukri Mohamad Adnan

Ahli:
1. Pegawai Psikologi, BHEP
   Puan Hairunisah Abdul Rahman
2. Pegawai Tadbir, Kolej Sri Rajang
   Puan Rosidah Basir
3. Pegawai Perubatan, Bahagian Kesihatan Pelajar
   Dr. Muhammad Amru Badrul Hisam
4. Pegawai Kewangan, Bahagian Kewangan
   Puan Sharinah Muztaba

PENYELARAS SISTEM

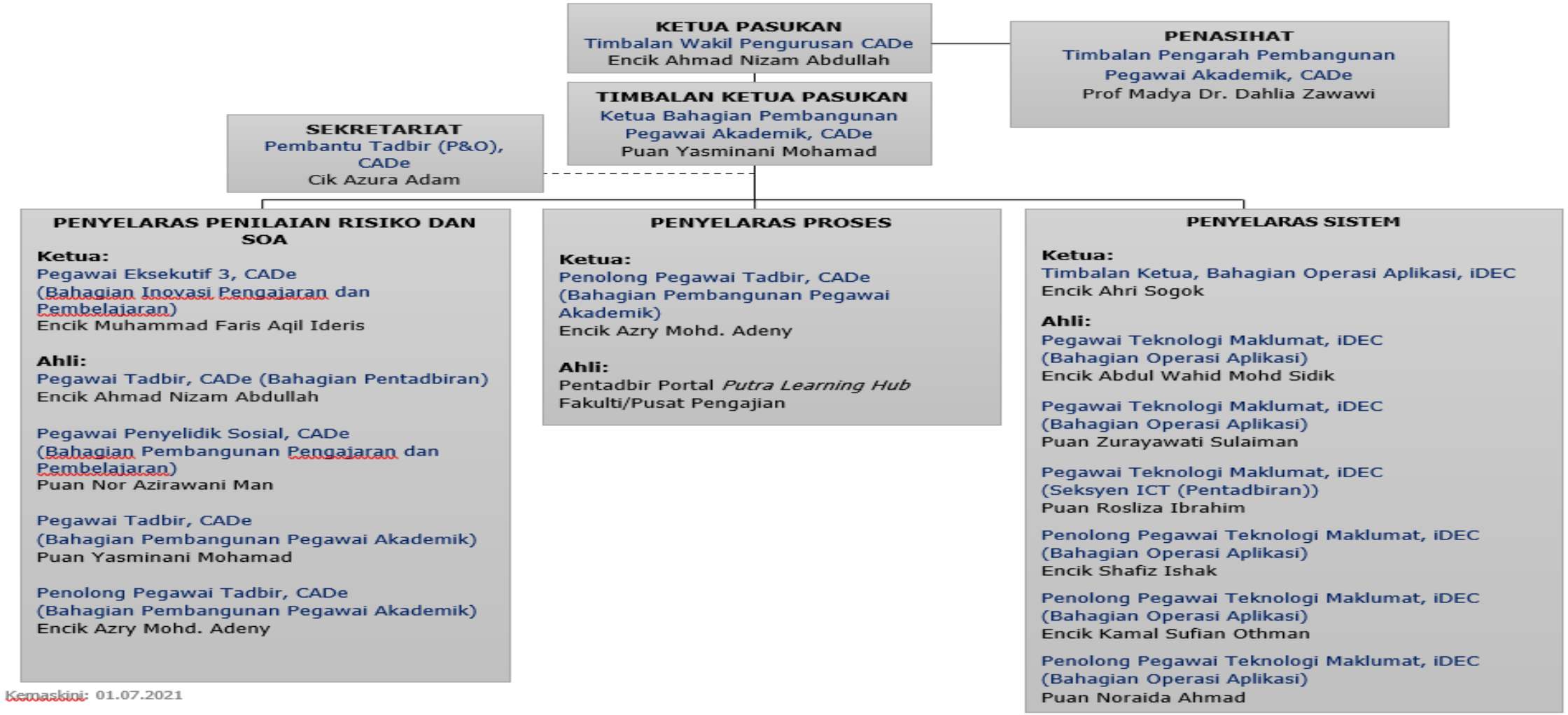
Ketua:
Ketua, Bahagian Teknologi Maklumat (BTM)
Encik Abdul Mohammad Omar

Ahli:
1. Pegawai Teknologi Maklumat, BTM
   Encik Zulkernain Zamawi
2. Penolong Pegawai Teknologi Maklumat BTM (Sistem Kewangan)
   Puan Hamidah Abdullah
3. Penolong Pegawai Teknologi Maklumat BTM (Sistem SMP)
   Encik Roslan Ismail

Kemaskini: 11 Mac 2022

STRUKTUR ORGANISASI PASUKAN ISMS UPM

STRUKTUR ORGANISASI PASUKAN PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI



Kemaskini: 01.07.2021

PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH

Skop Pensijilan:
Sistem Pengurusan Keselamatan Maklumat bagi **Proses Pendaftaran Pelajar Baharu Prasiswazah Merangkumi Aktiviti Semakan Tawaran hingga Pendaftaran Kolej Kediaman**

Peneraju:
Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang (BHEP & entiti terlibat)
&
Pasukan Pendaftaran Pelajar Baharu Prasiswazah Kampus Bintulu (UPMKB)

1. Terima data pelajar yang lengkap daripada UPU KPT
2. Penentuan kolej kediaman untuk bakal pelajar
3. Keluar surat tawaran kepada bakal pelajar melalui Sistem eDaftar
4. Pengesahan pendaftaran pelajar melalui Sistem eSMP
5. Pendaftaran kolej kediaman

PROSES PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI

Skop Pensijilan:
Sistem Pengurusan Keselamatan Maklumat bagi **Proses Penilaian Pengajaran Prasiswazah di Fakulti**

Peneraju:
Pasukan Penilaian Pengajaran Prasiswazah di Fakulti (CADe)

1. Tetapkan jadual penilaian pengajaran dalam Sistem *Teaching Assessment*
2. Kemaskini Data Penilaian Pengajaran dalam dalam Sistem *Teaching Assessment*
3. Buat hebahan kepada Fakulti/ Pensyarah/Pelajar
4. Pelajar membuat penilaian dalam tempoh yang ditetapkan
5. Jana laporan penilaian pengajaran dalam Sistem *Teaching Assessment*
6. Cetak dan sahkan laporan penilaian pengajaran keseluruhan
7. Edar laporan penilaian pengajaran kepada pensyarah yang berkenaan

PELAKSANAAN PENILAIAN RISIKO ISMS

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 metadologi 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).**

PENGURUSAN RISIKO TERHADAP ASET ICT

PERKAKASAN

PERISIAN

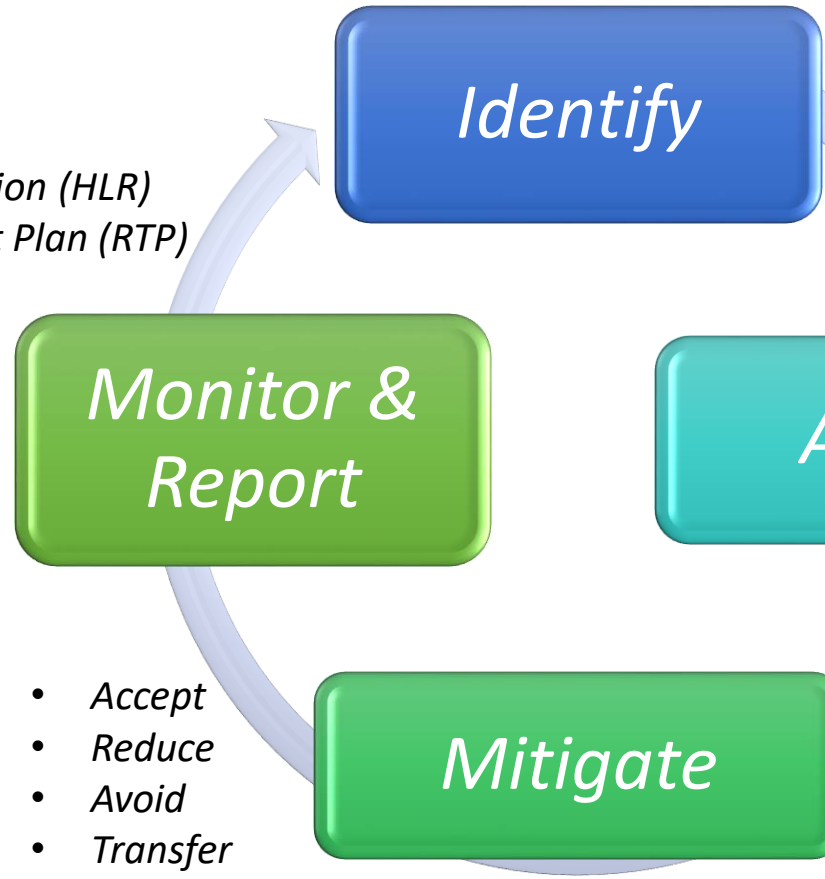
DATA/MAKLUMAT

SUMBER MANUSIA

PERKHIDMATAN

PENILAIAN RISIKO ISMS UPM

Proses Pengurusan Risiko



- *Business risk*
- *Business process*
- *Interested parties*
- *Internal & External issues*
- *Define scope*

- *Threat*
- *Vulnerabilities*
- *likelihood*
- *safeguard*
- *Impact*

- *Accept*
- *Reduce*
- *Avoid*
- *Transfer*

- *High Level Recommendation (HLR)*
- *Risk Treatment Plan (RTP)*
- *KPI*

PELAN PEMULIHAN RISIKO ISMS

TERIMA RISIKO TANPA SEBARANG PELINDUNGAN/ KAWALAN

Keputusan ini ditentukan jika **implikasi terhadap risiko adalah RENDAH (LOW)**

LAKSANA KAWALAN UNTUK KURANGKAN RISIKO

Keputusan ini ditentukan sekiranya **implikasi terhadap risiko adalah KRITIKAL** samada **TINGGI (HIGH)** atau **SEDERHANA (MEDIUM)**. Pengurangan risiko dapat dilaksanakan melalui penambahbaikan dari segi operasi, prosedur, fizikal, individu atau teknikal

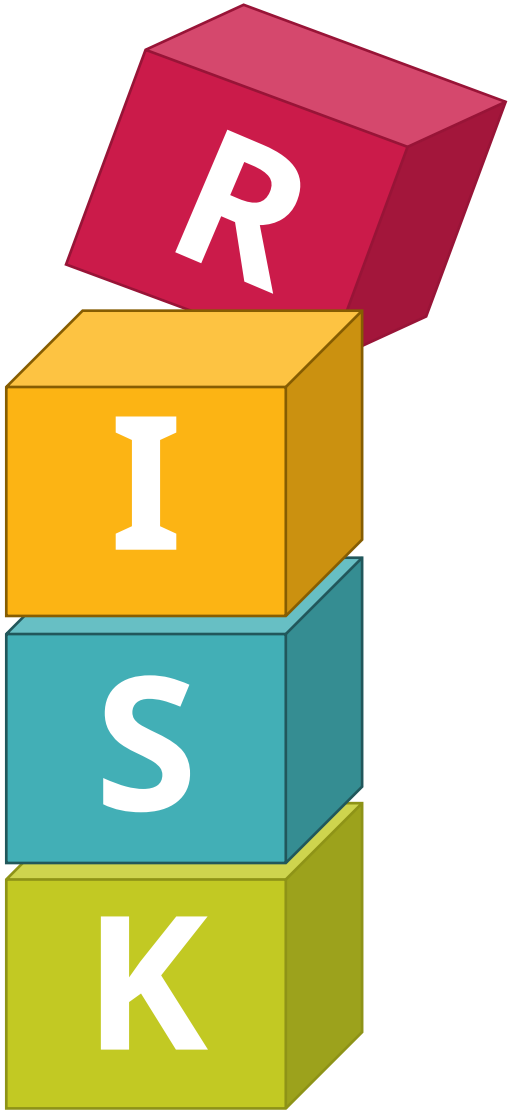
PINDAHKAN RISIKO KEPADA ENTITI LAIN

Keputusan ini ditentukan sekiranya **implikasi terhadap risiko tersebut boleh dipindahkan** dengan mewujudkan perjanjian (SLA) antara kedua pihak

ELAK RISIKO APABILA TIADA PILIHAN LAIN

Keputusan ini ditentukan kerana **tiada kawalan yang dapat ditentukan** samada untuk mengurangkan atau memindahkan risiko kepada pihak ketiga

PENILAIAN RISIKO PASUKAN ISMS



PASUKAN ISMS SERDANG DAN BINTULU

- Pasukan Pendaftaran Pelajar Baharu (Kampus Serdang)
- Pasukan Pendaftaran Pelajar Baharu (Kampus Bintulu)
- Pasukan Pusat Data
- Pasukan Penilaian Pengajaran Prasiswazah di Fakulti

PENILAIAN RISIKO ISMS UPM

e-ISO SISTEM PENGURUSAN ISO
UNIVERSITI PUTRA MALAYSIA

LATARBELAKANG ISO

- Sistem Pengurusan Kualiti (QMS) ISO 9001
- Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO 27001

OBJEKTIF KUALITI & OBJEKTIF ISMS

OBJEKTIF KUALITI

- Petunjuk Prestasi Utama (KPI) UPM
- Pelan Tindakan Peringkat Fungsian dan Aras
- Piagam Pelanggan

OBJEKTIF ISMS

- Objektif Sistem Pengurusan Keselamatan Maklumat

DASAR ISO

- Dasar Kualiti
- Dasar ISMS

MODEL PENDEKATAN PROSES ISO

- Model Pendekatan Proses SPK

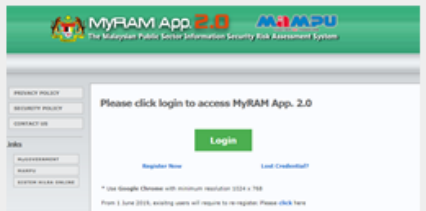
PENGURUSAN RISIKO ISO

- Dokumen Risiko Operasi Sistem Pengurusan Kualiti (QMS)
- Dokumen Risiko Sistem Pengurusan Keselamatan Maklumat (ISMS)

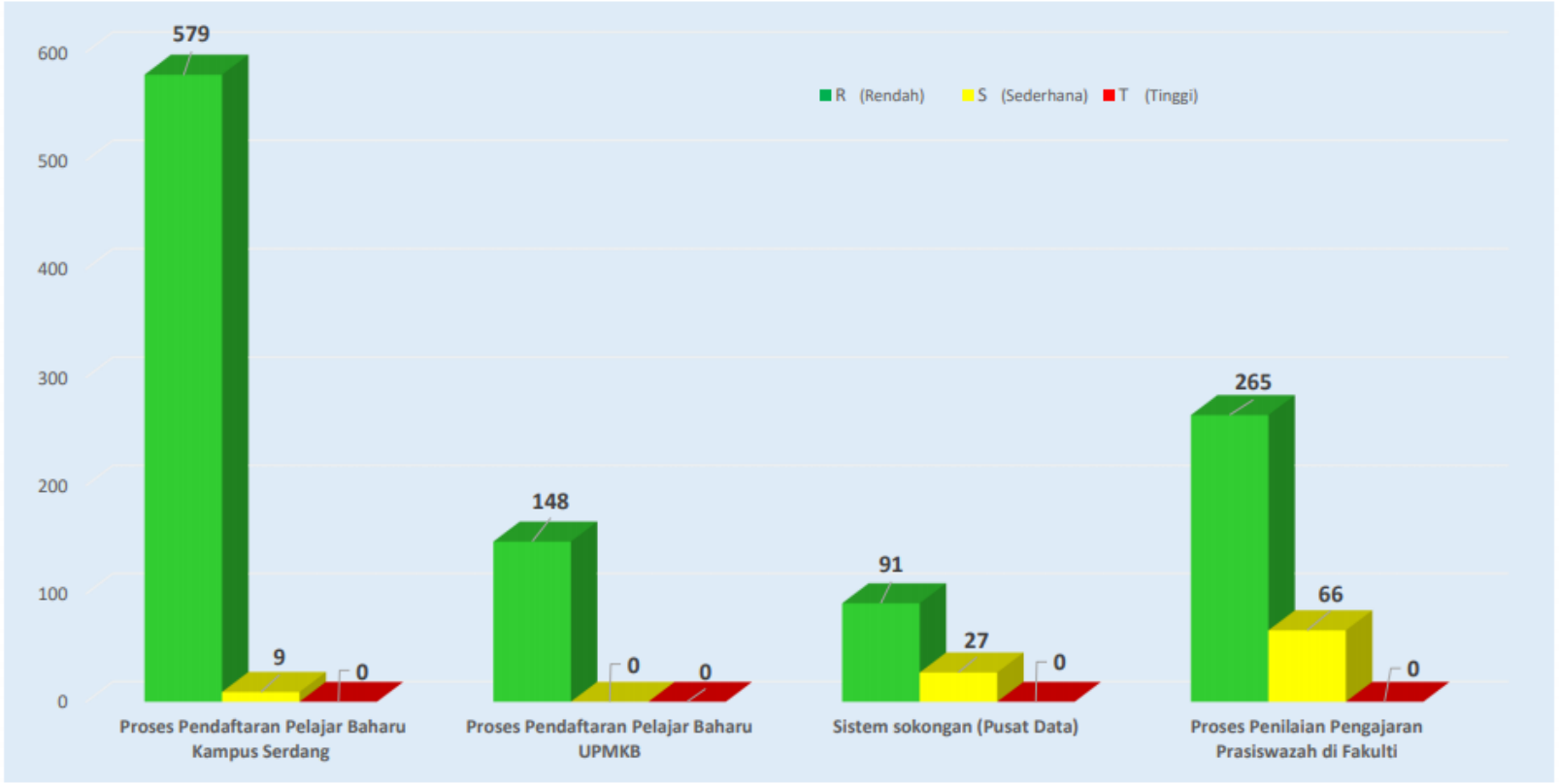
SENARAI DOKUMEN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) MS ISO/IEC 27001 UNIVERSITI PUTRA MALAYSIA

1.	**Dokumen Risiko ISMS Tahun 2017**
	+ Dokumen Risiko ISMS Semakan September 2017
2.	**Dokumen Risiko ISMS Tahun 2018**
	+ Dokumen Risiko ISMS Semakan Januari 2018
	+ Dokumen Risiko ISMS Semakan September 2018
3.	**Dokumen Risiko ISMS Tahun 2019**
	+ Dokumen Risiko ISMS Semakan April 2019
	+ Dokumen Risiko ISMS Semakan Ogos 2019
4.	**Dokumen Risiko ISMS Tahun 2020**
	+ Dokumen Risiko ISMS Semakan Julai 2020
5.	**Dokumen Risiko ISMS Tahun 2021**
	+ Dokumen Risiko ISMS Semakan Mac 2021

* Untuk perincian, sila rujuk Laporan Penilaian Risiko setiap Peneraju ISMS menerusi *The Malaysian Public Sector Information Security Risk Assessment System* (MYRAM) di pautan https://myram.mampu.gov.my.



CONTOH LAPORAN PENILAIAN RISIKO ISMS UPM



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

Untuk perincian, sila rujuk Laporan Penilaian Risiko setiap Peneraju ISMS menerusi *The Malaysian Public Sector Information Security Risk Assessment System* (MYRAM) di pautan https://myram.mampu.gov.my.

CONTOH LAPORAN PENILAIAN RISIKO PASUKAN ISMS TAHUN 2021

PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021

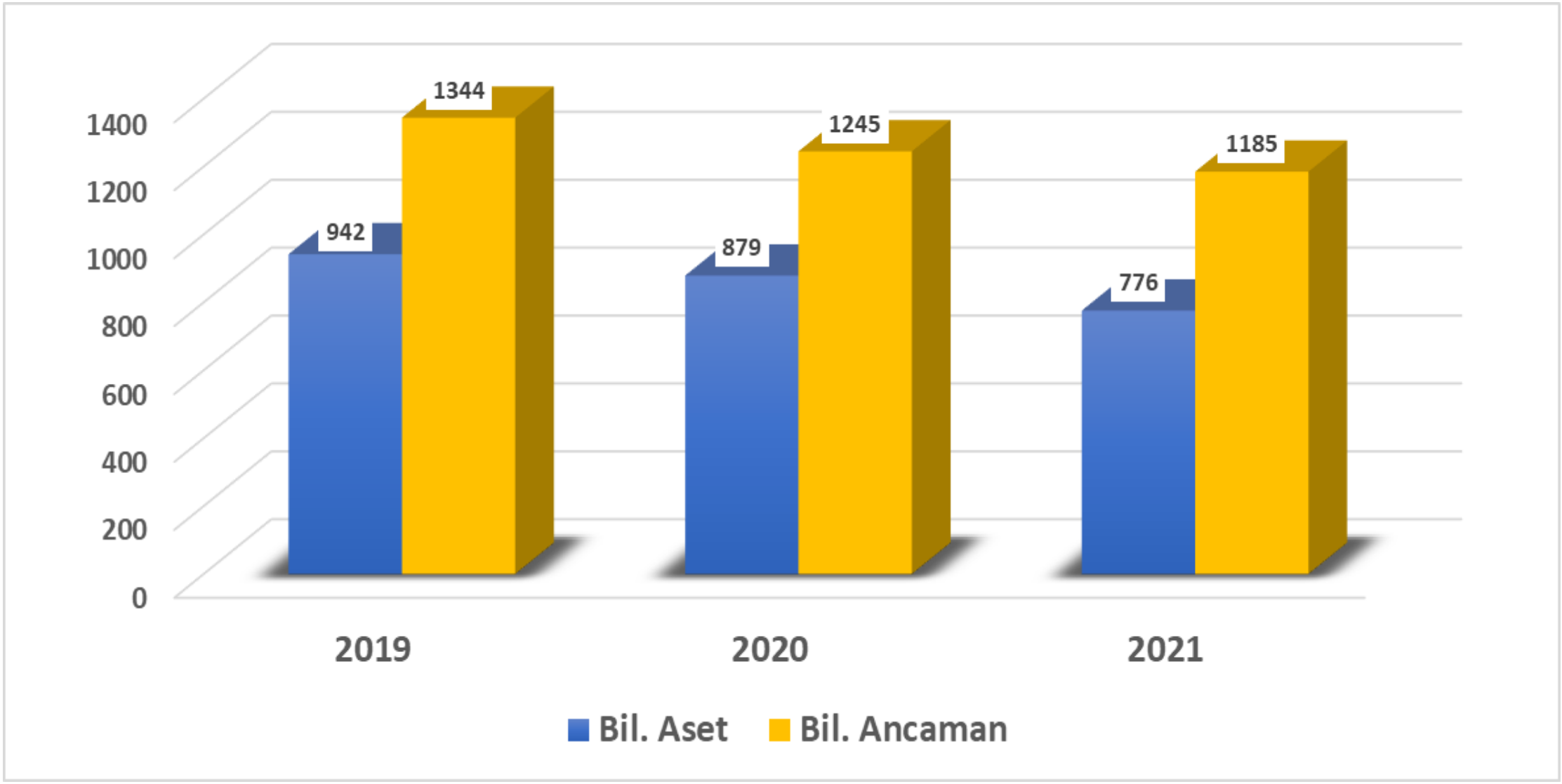
Nama Proses	Punca Dominan	Kawalan Sediaada (Existing Safeguard)	Rawatan (Treatment)	Pelan Pemulihan Risiko (Risk Treatment Plan) & Cadangan tarikh Tindakan
Proses Pendaftaran Pelajar Baharu Prasiswazah Kampus Serdang	**PutraVID API *(Medium)*** *T4.20 – Software vulnerabilities or errors*	*A.12.3.1 –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

CONTOH LAPORAN PENILAIAN RISIKO PASUKAN ISMS TAHUN 2021

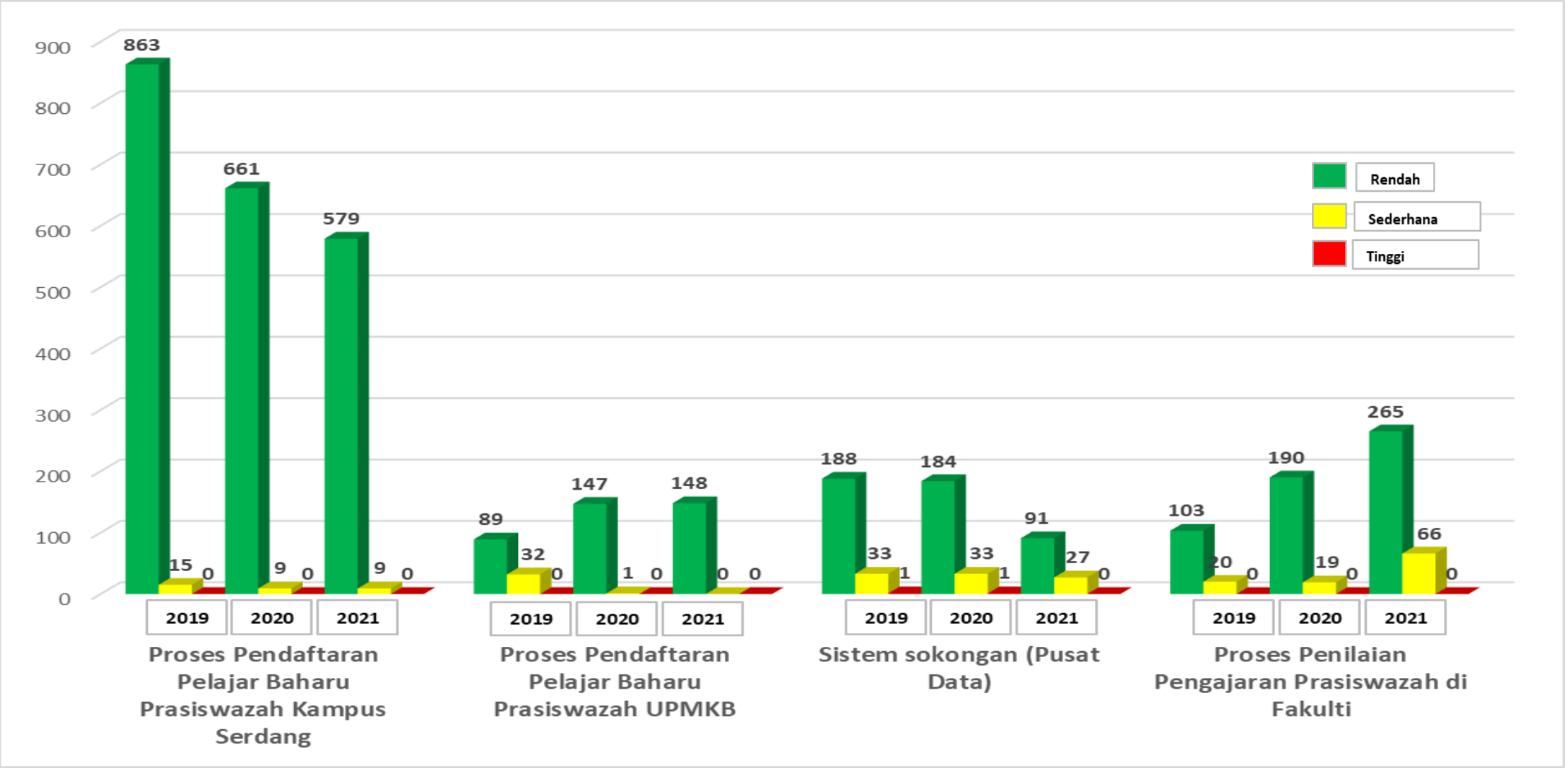
PELAN PEMULIHAN RISIKO SISTEM PENGURUSAN KESELAMATAN MAKLUMAT SEMAKAN MAC 2021

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)*** *T4.1 - Software malfunctions*	*A.12.3.1 - Information backup* Pendaftaran boleh dilakuan manual dengan merujuk senarai nama pelajar dan surat tawaran.	Tiada	Tiada
	Senarai Pendaftaran (Low) *T3.3 - Carelessness/ negligence in handling information and operating the IT system*	*8.1 - Operational planning and control* Cetakan semula dengan merujuk rekod dalam komputer.	Tiada	Tiada
Sistem sokongan (Pusat Data)	**DC Standby Genset *(Medium)*** *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 : Garis Panduan Penyelenggaraan Berkala (PPPA)	*A.15.2.1 - Monitoring and review of supplier services* Perkhidmatan penyelenggaraan Genset oleh PPPA	Apr 2020 - Apr 2022
	Bangunan iDEC Beta *(Medium)* *T1.19 - Flash flood*	*6.1.1 - General* Permohonan Pusat Data Baru telah dikemukakan semula pada RMK12 Rolling Plan 2 Tahun 2022 pada 3 Feb 2021 ke KPT melalui PPPA	*A.11.1.4 - Protecting against external and environmental threats* 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)*** *T1.9 - Failure of the IT system*	*A.11.2.4 - Equipment maintenance* Prosedur Penyelenggaraan ICT: • GPKTMK Perkara 11.3 (e) : Penyelenggaraan Peralatan • UPM/OPR/IDEC/P003 : Prosedur Penyelenggaraan ICT Penyelenggaraan Berkala	Tiada	Tiada

PERBANDINGAN JUMLAH ASET YANG DI NILAI DAN ANCAMAN (2019 - 2021)



PERBANDINGAN JUMLAH ASET YANG DI NILAI DAN ANCAMAN (2019 - 2021)



PENILAIAN RISIKO ISMS UPM

Contoh Kawalan di Pelan Pemulihan Risiko Pusat Data UPM

Bangunan Pusat Data UPM berusia melebihi 50 tahun dan kedudukan di aras G.

PENILAIAN RISIKO ISMS UPM

Contoh Kawalan di Pelan Pemulihan Risiko Pusat Data UPM

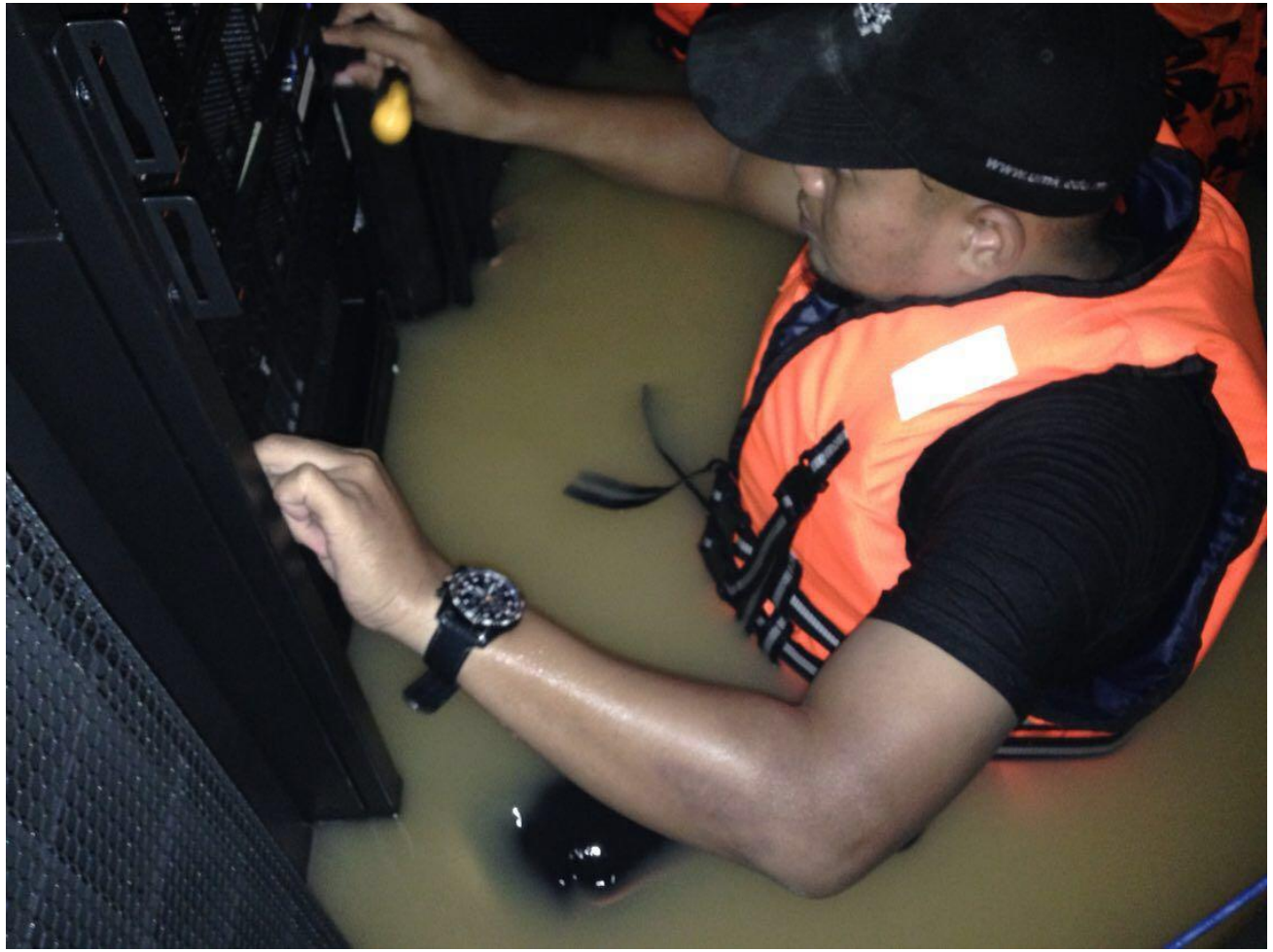
Bangunan Pusat Data UPM berusia melebihi 50 tahun dan kedudukan di aras G.

Tindakan Kawalan

1. Melaksana pemeriksaan bangunan selamat diduduki oleh Pejabat Pengurusan Keselamatan dan Kesihatan Pekerjaan (PPKKP)

2. Melaksana mitigasi mengelak banjir di kawasan persekitaran Pusat data oleh pihak Pejabat Pembangunan dan Pengurusan Aset (PPPA)

PENILAIAN RISIKO ISMS UPM



Contoh kesan banjir di salah sebuah Universiti Awam di pantai timur semasa banjir besar

PENEMUAN AUDIT SIRIM ISMS

CONTOH PENEMUAN AUDIT SIRIM ISMS UPM

Klausa 8.1 Perancangan dan kawalan operasi /A.12.1.2 Pengurusan perubahan

01

Pengurusan perubahan, terutama perubahan besar yang dilaksanakan di IDEC boleh diperkemaskan lagi agar jejak perubahan dapat dilakukan dengan mudah dan berkesan. Perancangan perubahan boleh diperjelaskan dan direkodkan dengan lebih teratur.

Klausa 8.2 Pentaksiran risiko keselamatan maklumat

02

Semakan pentaksiran risiko dan pelan penguraian risiko (RTP) telah dilaksanakan dan dikemas kini secara keseluruhan mengikut skop pensijilan. Namun, risiko-risiko berkaitan limitasi sistem, dan isu-isu pandemik terutamanya yang melibatkan kawalan penggunaan dan akses VPN boleh diambil kira bagi memastikan ianya dapat dikawal mengikut kawalan-kawalan sedia ada, ataupun memerlukan kawalan tambahan.

Klausa 8.1 Perancangan dan Kawalan Operasi/Annex A.11.2.8 Peralatan pengguna tanpa jagaan

03

PC pentadbir sistem Penilaian Pengajaran di Fakulti tidak mempunyai kawalan untuk komputer yang ditinggalkan tanpa jagaan.

Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.12.2.1 Kawalan daripada perisian hasad

04

PC pentadbir sistem Penilaian Pengajaran di Fakulti tidak mengemaskini definisi antivirus yang terkini dan imbasan tidak dilaksanakan pada sela masa yang sewajarnya.

CONTOH PENEMUAN AUDIT SIRIM ISMS UPM

Klausa 8.1 Perancangan dan kawalan operasi /A.12.1.2 Pengurusan perubahan

05

Kata laluan yang dimasukkan tidak mematuhi Garis Panduan Pengurusan Identiti.
-Kata laluan untuk kemasukan ke PC: Kombinasi kata laluan hanya mengandungi huruf sahaja
-Kata laluan untuk kemasukan Sistem Penilaian Pengajaran (Putrablast) : Kombinasi kata laluan hanya mengandungi huruf sahaja
-Kata laluan untuk kemasukan Sistem Maklumat Pelajar (SMP) : Kombinasi kata laluan tidak mempunyai simbol

Klausa 8.1 Pentaksiran risiko keselamatan maklumat/A.9.2.6 Penyingkiran atau pelarasan hak akses

06

Senarai hak akses pengguna terhadap VPN yang dikawal di firewall perlu dilihat semula organisasi agar risiko terhadap akses yang tidak sah dapat dikurangkan.

Klausa 8.1 Perancangan dan Kawalan Operasi/ A.12.4.4 Penyegerakan jam

07

Waktu pada sistem door access di pusat data dan bilik NOC perlu dilihat semula oleh organisasi supaya disegerakkan mengikut satu sumber rujukan masa yang tepat

Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.12.1.1 Prosedur operasi yang didokumenkan

08

Kawalan perubahan semasa pembangunan sistem/aplikasi dan selepas tamat tempoh 'warranty' dilaksanakan mengikut prosedur yang ditetapkan. Namun, kaedah kawalan perubahan bagi sistem/aplikasi yang berada dalam tempoh 'warranty' perlu diperjelaskan lagi agar sebarang perubahan yang dibuat dapat dilaksanakan dengan lebih baik.

CONTOH PENEMUAN AUDIT SIRIM ISMS UPM

Klausa 6.1.3 Penguraian Risiko Keselamatan Maklumat	09	Apabila merancang dan menentukan risiko, organisasi boleh menyemak kembali kawalan-kawalan yang di pilih. Di lihat bagi cadangan kawalan rawatan (treatment plan) ia merupakan kawalan-kawalan sedia ada. Ianya bukan kawalan- kawalan baru atau kawalan tambahan yang perlu di wujudkan bagi mengurangkan risiko.
Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex 9.4.3 Sistem Pengurusan Kata Laluan	10	Akses kata laluan ke pelayan (server) bagi Sistem Maklumat Pelajar (SMP) seperti server DRSMPDB, DRSMPAAP dan DRPWEB, tidak dapat menunjukkan bahawa kesemua pelayan patuh kepada GPKTMK (Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi). Walau bagaimanapun kerana kekangan sistem organisasi sudah bercadang melaksanakan UPM ID bagi menurunkan risiko kepada kawalan ke atas pengurusan kata laluan ini. Perlaksanaan ke atas kawalan ini masih dalam perancangan.
Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.11.2.2 Utiliti Sokongan	11	Semasa lawatan ke Pusat Pemulihan Bencana Epsilon, terdapat sebuah bilik yang menempatkan bateri UPS adalah agak panas, terdapat beberapa penghawa dingin yang ditempatkan di situ ,walau bagaimanapun masih tidak dapat menampung suhu bilik tersebut. Organisasi boleh melihat kembali dari segi pengurusan kapasiti ianya adalah memastikan bateri tersebut boleh bertahan lebih lama juga dari mengelakkan terdedah dengan suhu bilik yang tidak sesuai.
Klausa 8.1 Kawalan Operasi/ Annex A.18.1.3 Perlindungan Rekod	12	Kawalan terhadap rekod kesihatan (Filem X-ray) bagi pelajar-pelajar perlu ditambah baik, didapati rekod kesihatan (Filem X-ray) disimpan di dalam almari yang tidak berkunci di dalam ward sementara.

CONTOH PENEMUAN AUDIT SIRIM ISMS UPM

Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.18.1.3 Perlindungan Rekod

13

Pelaksanaan semakan terhadap dokumen lengkap yang diperlukan di Klinik Satelit perlu ditambah baik. Semakan rekod seharusnya direkodkan oleh PTJ yang berkenaan bukannya kepada Pembantu Perubatan. Namun pengesahan rekod-rekod tersebut dibuat oleh Pembantu Perubatan.

Klausa 7.2 (d) Kompetensi

14

Latihan kepada Juruaudit Dalaman ISMS telah dilaksanakan pada 21 – 22 Feb. 2017. Kehadiran bagi peserta perlu selaras dengan Rekod kehadiran di dalam Sistem Pengurusan Latihan (SPL). Dengan itu, sijil hanya diberikan kepada peserta yang hadir penuh sahaja.

Klausa 9.1 Pemantauan, Pengukuran, Analisis dan Penilaian

15

Didapati, Objektif ISMS telah dikenalpasti bagi mengukur peratusan pembayaran yuran pengajian secara atas talian dengan sasaran 80%. Sasaran yang ditetapkan perlu mengambil kita peratusan yang dikenalpasti di dalam penilaian risiko iaitu 100%.

Risiko terhadap perkhidmatan atas talian tidak dikenalpasti semasa penilaian risiko bagi Pejabat Bursar

Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.9.4.3 Sistem Pengurusan Kata Laluan

16

Panjang kata laluan bagi sistem e-IHRAMS perlu ditambah baik bagi memenuhi GPKTMK (Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi). Pengguna di Jabatan Pendaftar

CONTOH PENEMUAN AUDIT SIRIM ISMS UPM

Klausa 8.2 Pentaksiran Risiko Keselamatan Maklumat 17

Pelaksanaan pentaksiran risiko keselamatan maklumat telah dilakukan oleh organisasi seperti mana yang dirancang dan meliputi skop ISMS yang terlibat, namun begitu penambahbaikan boleh dilaksanakan seperti di bawah: 1) Bagi Penilaian Risiko (RA) untuk Proses Penilaian Pengajaran Prasiswazah di Fakulti, pengenalpastian aset untuk kategori 'Data and Information' sebagai contoh, 'Laporan terperinci pencapaian pengajaran pensyarah' yang dinilai seharusnya mengambil kira risiko/ancaman ke atas data yang berbentuk salinan keras (hardcopy) dan dinyatakan dengan jelas kawalan yang dilaksanakan. 2) Semakan ke atas Penilaian Risiko yang dilaksanakan seharusnya mengambil kira sebarang perubahan yang berlaku seterusnya pengemaskinian perlu dilaksanakan sewajarnya. Sebagai contoh, Laporan Penilaian Risiko bagi Proses Pendaftaran Pelajar Baharu UPM Kampus Bintulu yang mana terdapat perubahan ke atas ahli/peranan dalam pasukan ISMS Kampus Bintulu.

Klausa 9.2 Audit Dalaman 18

Proses audit dalaman dilakukan secara decentralize audit oleh setiap PTJ yang terlibat dalam tempoh yang telah dirancang dan perincian dapatan audit dalaman direkodkan dalam Portal Jaminan Kualiti. Walaubagaimanapun, bagi memastikan perincian bagi setiap penemuan, khususnya untuk keperluan kawalan pada Annex A, nombor kawalan yang terlibat seharusnya dinyatakan dengan lebh jelas menjurus kepada setiap penemuan. Selain daripada itu, analisa atau statistik bagi penemuan audit dalaman yang dibuat yang hanya berdasarkan klausa boleh diperluaskan lagi kepada penemuan bagi kawalan Annex A.

Klausa 8.1 Perancangan dan Kawalan Operasi/ A.7.2.2 Kesedaran, Pendidikan dan Latihan Tentang Keselamatan Maklumat 19

Program dan taklimat kesedaran berkenaan keselamatan maklumat ada dilaksanakan oleh organisasi, namun begitu boleh ditambahbaik lagi dengan memastikan elemen kawalan keselamatan (rujuk SOA/Annex A) dilaksanakan dengan lebih spesifik. Selain daripada itu, penilaian terhadap program yang dilaksanakan ini boleh dilakukan bagi melihat keberkesanannya.

Klausa 8.1 Perancangan dan Kawalan Operasi/ Annex A.8.2 Pengelasan Maklumat dan Pelabelan Maklumat 20

Garis panduan bagi pengelasan maklumat dan kaedah pengendalian maklumat telah dibangunkan oleh organisasi, namun begitu pelaksanaan ke atas pengendalian maklumat ini boleh dipertingkatkan lagi. Sebagai contoh, pengelasan dan pelabelan maklumat untuk Laporan Penilaian Pengajaran yang telah dicetak di Sekolah Perniagaan dan Ekonomi.

Tayangan Video Kepentingan Penjagaan Keselamatan Maklumat

ISMS

Data yang bermakna ialah
MAKLUMAT

Maklumat yang **CIA** ialah
Keputusan yang **TERBAIK**

Keputusan yang **TERBAIK**
Organisasi yang **CEMERLANG**

Terima Kasih

UniPutraMalaysia @uputramalaysia uniputramalaysia universitiputramalaysia

PERTANIAN • INOVASI • KEHIDUPAN

BERILMU BERBAKTI
WITH KNOWLEDGE WE SERVE