



UNIVERSITI PUTRA MALAYSIA
AGRICULTURE • INNOVATION • LIFE

Taklimat Persediaan Menghadapi Audit Pemantauan Semakan 2, Sistem Pengurusan Keselamatan Maklumat (ISMS) MS ISO/IEC 27001:2013

28 September 2017 | 3.00 petang



Objektif Audit

- 1. Untuk menilai pematuhan berterusan Sistem Pengurusan Keselamatan Maklumat UPM berdasarkan keperluan standard;**
- 2. Untuk menilai keupayaan berterusan Sistem Pengurusan Keselamatan Maklumat untuk memastikan pelanggan mematuhi keperluan berkanun, peraturan dan kontrak yang berkaitan, jika berkenaan;**
- 3. Untuk menilai sama ada operasi Sistem Pengurusan Keselamatan Maklumat menyumbang kepada pencapaian matlamat organisasi dan hasil yang diharapkan;**

- 4. Untuk mengenal pasti ruang penambahbaikan Sistem Pengurusan Keselamatan Maklumat;**
- 5. Untuk menilai perubahan yang telah dibuat kepada Sistem Pengurusan Keselamatan Maklumat;**
- 6. Untuk mengesahkan pelaksanaan tindakan pembetulan yang berkesan hasil daripada penemuan audit terdahulu.**

Tarikh Audit

**6 September 2017
(di Kampus Bintulu)**



&

**2 – 3 Oktober 2017
(di Kampus Serdang)**

Skop Pensijilan

Main Site:

Sistem Pengurusan Keselamatan Maklumat bagi Proses Pendaftaran Pelajar Baharu Prasiswazah Semasa Minggu Perkasa Putra

Site 2:

Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi Proses Pendaftaran Pelajar Baharu Prasiswazah

Site 3:

Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi Proses Pendaftaran Pelajar Baharu Praasiswazah

Site 4:

Sistem Pengurusan Keselamatan Maklumat bagi Proses Pendaftaran Pelajar Baharu Prasiswazah Semasa Minggu Perkasa Putra di UPM Kampus Bintulu

NEW

Kriteria Audit

1 ISO/IEC 27001:2013

2 Dokumentasi ISMS

Pasukan Audit

1. Puan Sazlin Alias – Ketua Pasukan
(6 September, 2 & 3 Oktober 2017)
2. Cik Efizan Zamri (2 & 3 Oktober 2017)
3. Puan Hidayatini Sarmin (2 Oktober)

Metodologi Audit

1

Semakan dokumen dan rekod

2

Pemerhatian keatas proses dan aktiviti

3

Temubual auditi

Tempoh Semakan

**Kebiasaannya semakan akan
dibuat bermula dari
30 Oktober 2016
hingga kini
termasuk status ketakakuran dan
peluang penambahbaikan tahun
lepas**

Senarai PTJ Terlibat

1. Pusat Jaminan Kualiti (CQA)
2. Pusat Pembangunan maklumat dan Komunikasi
3. Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik
4. Bahagian Hal Ehwal Pelajar
5. Perpustakaan Sultan Abdul Samad
6. Pejabat Pendaftar
7. Pejabat Strategi Korporat dan Komunikasi
8. Pejabat Penasihat Undang-Undang

Ringkasan Pergerakan Juruaudit

JURUAUDIT	TARIKH AUDIT DAN PUSAT TANGGUNGJAWAB DIAUDIT	
	2/10/2017 (Hari Ke-2)	3/10/2017 (Hari Ke-3)
1. Sazlin Alias	1. Pusat Jaminan Kualiti (CQA) 2. Pusat Pembangunan Maklumat dan Komunikasi (iDEC) – Pasukan Penilaian Risiko	1. Perpustakaan Sultan Abdul Samad 2. Pejabat Pendaftar
2. Efizan Zamri	Pusat Pembangunan Maklumat dan Komunikasi (iDEC)	1. Pejabat Strategi Korporat dan Komunikasi 2. Pejabat Pensihat Undang-Undang
3. Hidayatini Sarmin	1. Bahagian Kemasukan dan Bahagian Urus Tadbir Akademik 2. Bahagian Hal Ehwal Pelajar	

Jadual Audit

2 Oct. 2017 @ UPM Serdang		
Time	Activity to be audited	Responsibility
0930–1000	Opening Meeting. - Briefing on the Information Security Management System by organization's representative on any changes to the system since last audit - Briefing on audit details by SIRIM QAS International's representative	SIRIM's auditors and client's representatives
1000–1700	Follow-up previous audit findings Documented information inclusive of creating and updating and control of documented information. Covering A.5 and A.6 Context of the organization inclusive of understanding the organization and its context, understanding the needs and expectations of interested parties, determining the scope of the ISMS. Leadership inclusive of leadership and commitment, policy and organizational roles, responsibilities and authorities. Planning inclusive of actions to address security risk assessment, information security risk treatment and information security objectives and plans to achieve them. Performance evaluation inclusive of monitoring, measurement, analysis and evaluation, internal audit and management review. Improvement inclusive of nonconformity and corrective action and continual improvement.	Sazlin Pusat Jaminan Kualiti (CQA) CQA & TWP ISMS CQA & TWP ISMS Pusat Pembangunan Maklumat dan Komunikasi (iDEC) – Pasukan Penilaian Risiko CQA & TWP ISMS CQA & TWP ISMS

Temubual PKD
- Rujuk proses Kawalan Dokumen

Temubual WP & TWP ISMS
- Rujuk Manual ISMS

Temubual Pasukan Penilaian Risiko
- Rujuk Laporan MyRAM

Temubual TWP ISMS, KJAD ISMS, PAD & SU MKSP
- Rujuk Laporan MKSP ISO

...Jadual Audit

2 Oct. 2017 @ UPM Serdang		
Time	Activity to be audited	Responsibility
	Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Pusat Pembangunan Maklumat dan Komunikasi IDEC - Data centre operation - Site visit DR site - A.16 Information security incident management	 Efizan
	Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Bahagian Kemasukan & Bahagian Urus Tadbir Akademik Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Bahagian Hal Ehwal Pelajar	 Hidayatini
1700	Review of Day 2 Findings	SIRIM's auditors and client's representatives

Temubual Auditi di
IDEC
- Rujuk MyRAM,
SOA & dokumentasi
terlibat

Temubual Auditi di
B. Akademik &
BHEP
- Rujuk MyRAM,
SOA & dokumentasi
terlibat

...Jadual Audit

3 Oct. 2017 @ UPM Serdang	
Time	Activity to be audited
0930-1200	Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Perpustakaan
	Support inclusive of resources, competence, awareness and communication. A.7 Human resource security
	Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Pejabat Strategi Korporat & Komunikasi A.17 information security business continuity management
	Operation (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.). Verification on the effectiveness of control as per Statement of Applicability at Pejabat Penasihat Undang –undang A.18 compliance -
1400-1530	Continue audit on unfinished areas
1530-1630	Preparation of Report
1630	Closing Meeting. Presentation of Findings and Recommendation

Temubual Auditi di
Perpustakaan
- Rujuk MyRAM, SOA
& dokumentasi
terlibat

Temubual Auditi di
Pejabat Pendaftar
- Rujuk SOA &
dokumentasi terlibat

Temubual Auditi di
COSCOMM
- Rujuk Pelan Pengurusan
Kesinambungan
Perkhidmatan

Temubual Auditi di
PPUU
- Rujuk SOA

Persediaan PTJ Diaudit

Let's
Recap

PERNYATAAN DASAR

ISO/IEC 27001:2013

DASAR KESELAMATAN MAKLUMAT

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.

Dibuat oleh LPU pada 9/12/2014

Let's
Recap

Objektif ISMS Tahun 2017:

1. Memastikan pelajar prasiswazah yang mengemukakan tawaran yang sah dibenarkan mendaftar;
2. Memastikan pembayaran yuran pengajian adalah secara atas talian;
3. Memastikan proses pemulihan sistem aplikasi pendaftaran pelajar baharu dapat dilaksanakan;
4. Memastikan *Service Level Agreement* (SLA) 95.0 sokongan ICT Pusat Data (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester

...Persediaan PTJ Diaudit

Let's
Recap



ID dan Password
untuk login
MyRAM

The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) atau Penilaian Risiko Keselamatan Maklumat Sektor Awam adalah bertujuan untuk mengukur, menganalisis tahap risiko aset maklumat dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

...Persediaan PTJ Diaudit

Let's
Recap

Bil.	Kod Dokumen	Nama Dokumen
1.	Prosedur	
1.	UPM/ISMS/SOK/P001	
2.	UPM/ISMS/SOK/P002	
		PENILAIAN RISIKO ASET
		GARIS PANDUAN PENGENDALIAN MAKLUMAT
3.	UPM/ISMS/SOK/GP04/ENKRIPSI	GARIS PANDUAN ENKRIPSI FAIL
4.	UPM/ISMS/SOK/GP05/PERALATAN MUDAH ALIH	GARIS PANDUAN KESELAMATAN PERALATAN MUDAH ALIH
5.	UPM/ISMS/SOK/GP06/INSTALASI PERISIAN	GARIS PANDUAN KAWALAN INSTALASI PERISIAN
6.	UPM/ISMS/SOK/GP07/IDENTITI	GARIS PANDUAN PENGURUSAN IDENTITI
3.	Dokumen Rujukan	
1.	UPM/ISMS/SOK/SOA	STATEMENT OF APPLICABILITY

SOA
"STATEMENT OF APPLICABILITY"



**Rujuk SOA di
bawah tindakan
PTJ berkaitan**

Keperluan dan Kesediaan PTJ

1. Kenderaan

- **Untuk menjemput dan menghantar Juruaudit.**

2. Pengiring

- **Keutamaan pengiring adalah dikalangan Timbalan Wakil Pengurusan/Timbalan Penyelaras Audit/Timbalan Pegawai Kawalan Dokumen/Juruaudit Dalaman atau pegawai yang terlibat secara langsung dalam skop audit.**

3. Tempat (Bilik mesyuarat/ruang perbincangan)

- **Untuk semakan rekod, temubual dan perbincangan.**

4. Keperluan Komputer

- **Untuk paparan/rujukan Sistem Pengurusan ISO (e-ISO)**

Peranan Pengiring Juruaudit

- 1. Bertanggungjawab mewakili Pusat Tanggungjawab (PTJ) membantu Juruaudit SIRIM;**
- 2. Mengambil catatan penting terutama maklum balas Juruaudit secara teguran lisan untuk tindakan segera PTJ;**
- 3. Melaksanakan tugas Pegawai Pengiring sepanjang tempoh audit iaitu menyambut kedatangan dan menghantar Juruaudit ke lokasi yang ditetapkan:**

...Peranan Pengiring Juruaudit

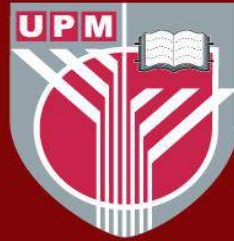
(A) Menyambut kedatangan Juruaudit di lokasi berikut:

Tarikh dan masa	Lokasi	PTJ yang terlibat
2/10/2017 (10.00 pagi)	Di Dewan Senat, Tingkat 1, Bangunan Canselori Putra (Selepas Mesyuarat Pembukaan Audit)	PTJ pertama diaudit pada sesi pagi
2/10/2017 (2.00 petang)	Di Bilik Lembaga, Tingkat 1, Bangunan Canselori Putra	PTJ pertama diaudit pada sesi petang
3/10/2017 (8.30 pagi)	Di Foyer Bangunan Canselori Putra dan bawa Juruaudit ke Bilik Lembaga Tingkat 1 untuk sarapan pagi	PTJ pertama diaudit pada sesi pagi

...Peranan Pengiring Juruaudit

(B) Menghantar Juruaudit ke lokasi seterusnya:

Tarikh dan masa	Lokasi	PTJ yang terlibat
2/10/2017 (1.00 petang)	Ke Bilik Lembaga Tingkat 1, Bangunan Canselori Putra untuk makan tengahari	PTJ diaudit pada sesi pagi
2/10/2017 (5.00 petang)	Ke Foyer Bangunan Canselori Putra	PTJ diaudit pada sesi petang
3/10/2017 (1.00 petang)	Ke Bilik Lembaga Tingkat 1, Bangunan Canselori Putra untuk makan tengahari	PTJ diaudit pada sesi pagi



UNIVERSITI PUTRA MALAYSIA
AGRICULTURE • INNOVATION • LIFE

Terima Kasih | *Thank You*