UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

1970-2020 UKM #menciptamasadepan

TAKLIMAT PELAKSANAAN ISMS UKM (SKOP BAHARU)

NORHISHAH ELIAS
Ketua Penolong Pendaftar Kanan
Pusat Jaminan Kualiti (Kualiti-UKM)

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Sesi 1

Pengenalan Kepada ISMS UKM

Kenapa Perlu ISMS?

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

2 

Pemantauan oleh KPM (melalui Surat Ketua Pengarah JPT bertarikh 5 Februari 2014)

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

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

Proses Pelaksanaan ISMS di UKM

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

1. Penentuan **Skop**
2. Laksanakan **Penilaian Risiko**
3. Kenalpasti **Risiko yang perlu dirawat**
4. Kenalpasti **Kawalan Keselamatan**
5. **Pelaksanaan ISMS**
6. **Pengukuran Keberkesanan**
7. **Audit Dalaman**
8. **Mesyuarat Semakan Pengurusan**
9. **Audit SIRIM**

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Kuatkuasa Pelaksanaan ISMS

1 Mei 2014

PENGENALAN

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Objektif Pelaksanaan ISMS

- Menyediakan satu pendekatan yang teratur dan sistematik dalam menilai risiko dan mengawal keselamatan maklumat universiti dari segi kerahsiaan, integriti dan kebolehsediaan
- Mengenal pasti ancaman dan risiko yang wujud di dalam persekitaran ICT serta meningkatkan tahap keselamatan ICT universiti
- Memberi jaminan dan meningkatkan keyakinan kepada pelanggan dan pihak berkepentingan mengenai tahap keselamatan maklumat universiti

KEPIMPINAN

KOMITMEN PENGURUSAN

- Profesor Dr. Mohd Juzaiddin Ab Aziz menjalankan Tugas CIO UKM dan Wakil Pengurusan ISMS UKM mulai Januari 2019
- Menyemak Dasar Keselamatan ICT UKM dari masa ke semasa dan mengikut keperluan.
- Memantau Objektif Pengukuran ISMS UKM yang dilaksanakan secara berkala dalam Mesyuarat JK Pelaksana ISMS dan dilaporkan dalam Mesyuarat JK Induk ISMS UKM dan MSP
- Melaksanakan program promosi interaktif bagi meningkatkan kefahaman keselamatan maklumat di kalangan Warga UKM melalui cadangan dalam Mesyuarat JK Induk ISMS UKM dan MSP.
- Memastikan perancangan kecukupan sumber dalam pelaksanaan ISMS UKM dan berusaha memenuhi keperluan pelanggan.

AUDIT BADAN PENSIJLAN

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Peringkat 1
- 17-18 November 2014

Peringkat 2
- 23-24 April 2015

Pen 1
- 18-19 April 2016

Pengawasan 2
- 25-28 April 2017

Pensijilan Semula
- 24-27 April 2018

Pengawasan 1
- 25-26 April & 29-30 April 2019

Pengawasan 2
- 29 Jun – 02 Julai 2020

29 Mei 2015
- Pengiktirafan Pensijlan (Kitaran 1)

29 Mei 2018
- Pengiktirafan Pensijlan (Kitaran 2)

Kitaran 1 – 29 Mei 2015 – 28 Mei 2018

Kitaran 2 – 29 Mei 2018 – 28 Mei 2021

Faedah ISMS kepada UKM

Pengiktirafan (AR 6534)

- 29 Mei 2015 – 28 Mei 2018 (Kitaran 1)
- Majlis Penyampaian – 7 Oktober 2015
- 29 Mei 2018 – 28 Mei 2021 (Kitaran 2)

TAJUK

Jaminan kepada pihak berkepentingan & pelanggan berhubung keselamatan maklumat yang berkaitan

Pendekatan yang lebih **sistematik** dalam menilai risiko keselamatan maklumat dan **penambahbaikan dalam sistem kualiti.**

Meningkatkan **kesedaran** dan **rasa tanggungjawab** berhubung keselamatan maklumat di kalangan pekerja

Meningkatkan **imej** organisasi

AUDIT DALAMAN ISMS UKM

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

2016
- 16 Januari – 16 Februari 2017

2017
- 24 Januari – 26 Februari 2018

2018
- 25 Januari – 22 Februari 2019

2019
- 16 Januari – 22 Februari 2020

Laporan Penemuan

2016	2017	2018	2019
NCR - 8	NCR - 3	NCR - 1	NCR - 0
OFI - 13	OFI - 17	OFI - 16	OFI - 12

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Sesi 2

Peluasan Dan Pelaksanaan Skop ISMS UKM Baharu

Penentuan Skop ISMS UKM Yang Baharu

Mengenalpasti/Menentukan Isu Dalaman dan Luaran dalam keselamatan maklumat:

1. Pelajar
2. Kakitangan
3. Kewangan
4. Penyelidikan

Mengenalpasti keperluan dan jangkaan pihak berkepentingan dalam keselamatan maklumat di UKM

1. Pelajar
2. Kakitangan
3. Pengurusan
4. Pensyarah/penyelidik
5. Agensi Pusat
6. NGO/Industri/Komuniti
7. Pihak Berkanun

Menentukan bisnes dan proses utama yang menjadi parameter dalam pelaksanaan ISMS UKM.

1. Proses utama dalam Pengurusan P&P
2. Proses utama dalam pengurusan sumber manusia
3. Proses utama pengurusan kewangan
4. Proses utama pengurusan penyelidikan

CARTA PERBATUAN PELUASAN SKOP ISMS UKM TAHUN 2019-2020

Aktiviti / Bulan	Tahun 2019			Tahun 2020										
	Okt	Nov	Dis	Jan	Feb	Mac	Apr	Mei	Jun	Jul	Ogs	Sep	Okt	Nov
Perbincangan bersama CIO dan Pasukan Taskforce														
Pemurnian kerangka kerja peluasan skop ISMS kepada Pasukan Kerja														
Perbincangan dengan pihak SIRIM QAS International Sdn Bhd														
Perbincangan bersama pemilik proses utama														
Lawatan penandarasan ke UMT														
Analisis Jurang (Kecukupan Dokumen)														
Penentuan Isu Dalaman dan Luaran, Pihak Berkepentingan serta skop pensijilan														
Pengemaskinian dokumen utama														
Pengemaskinian pelan pengurusan risiko														
Pengukuran dan 'security matrix'														
Pembentangan kepada Pasukan Taskforce dan JK Induk ISMS UKM														
Penambahbaikan dokumentasi														
Muat naik dokumen dalam SPD														
Program Jerayawara														
Pelaksanaan Skop Baharu														

Sasaran Pelaksanaan

Pengurusan Kawalan Keselamatan Maklumat:

- "Pengurusan Maklumat Pelantikan Kakitangan Bukan Akademik, Pembayaran Gaji Kakitangan, Pengurusan Pendaftaran Kursus Pelajar Prasiswazah dan Pengurusan Pusat Data"

1.11.2020

- Tarikh Pelaksanaan

Evolusi Pelaksanaan ISMS UKM

Skop pelaksanaan sedia ada

Pengurusan pangkalan data Sistem Maklumat Universiti (SMU)

Kelulusan Mesyuarat Majlis Tenologi Maklumat Bil . 2/2013	Kuat kuasa pelaksanaan pada 1 Mei 2014	Pusat Teknologi Maklumat sebagai PTj Utama

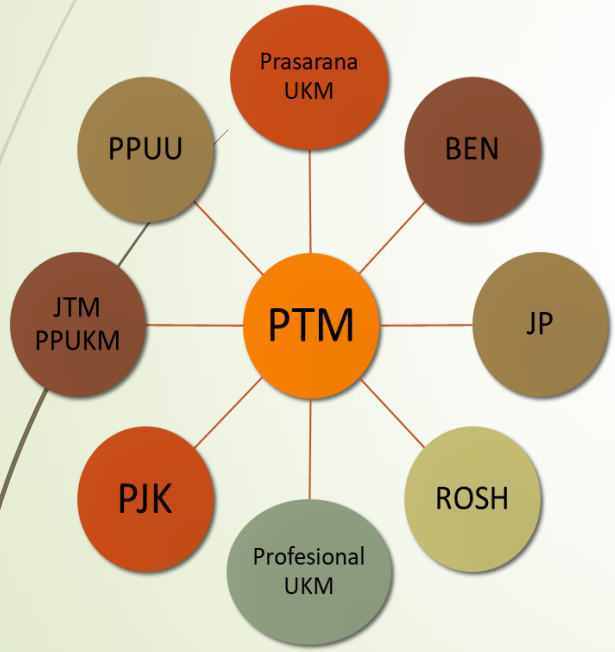
Skop pelaksanaan baharu

Pengurusan Kawalan Keselamatan Maklumat bagi proses: Pengurusan Maklumat Pelantikan Kakitangan Bukan Akademik, Bayaran Gaji Kakitangan , Pengurusan Pendaftaran Kursus Pelajar Pra Siswazah dan Pengurusan Pusat Data

Kelulusan Mesyuarat JK Pemandu ICT UKM Bil. 2/2019	Kuat kuasa pelaksanaan pada 1 Nov 2020	Penglibatan 4 PTj Utama: Jabatan Pendaftar Jabatan Bendahari Akademik UKM PTM UKM

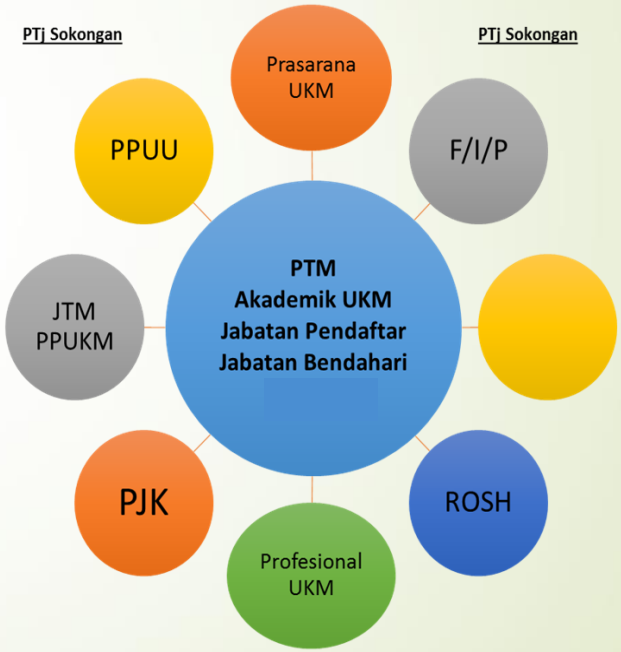
Penglibatan PTj Utama dan PTj Sokongan

- Pelaksanaan Skop ISMS Sedia ada



Penglibatan PTj Utama dan PTj Sokongan

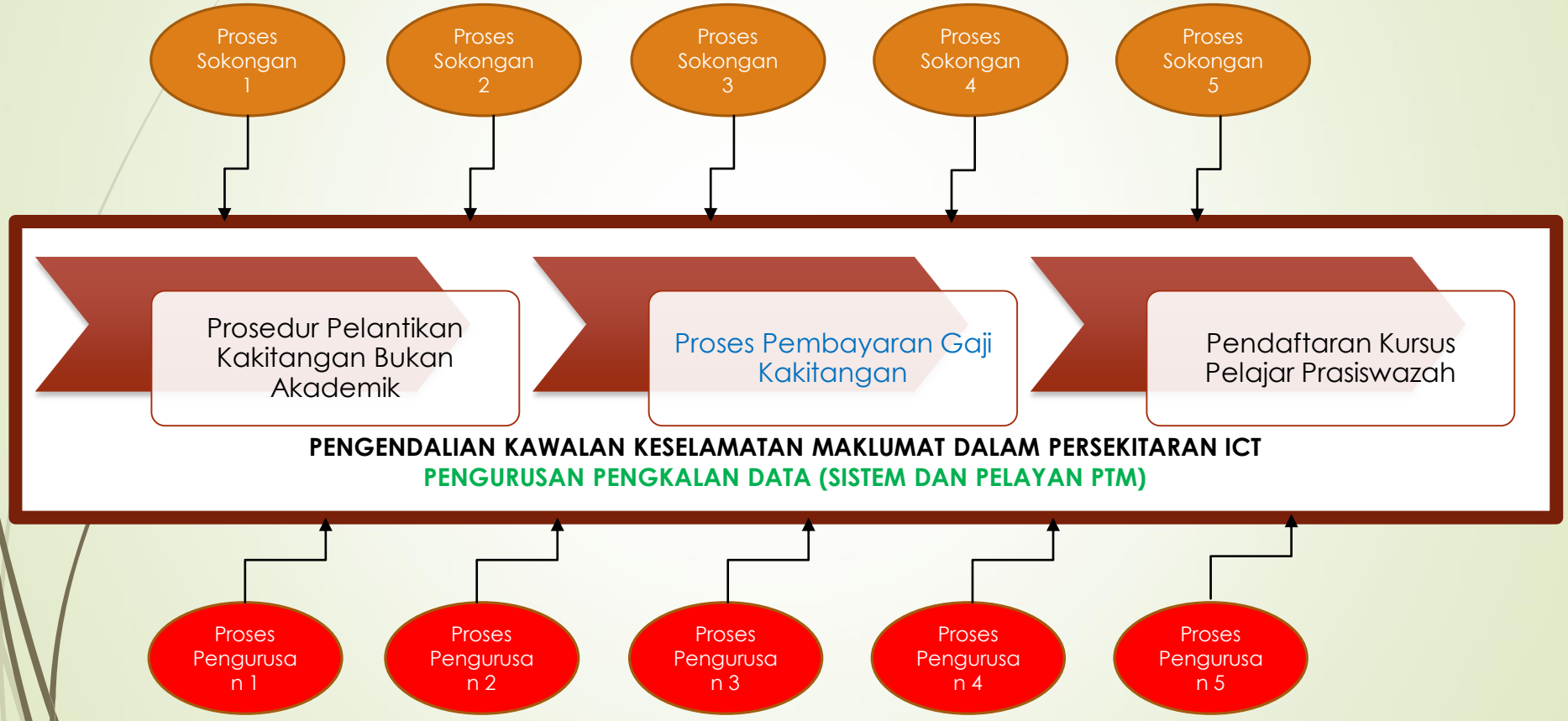
- Cadangan Penstrukturan Pelaksanaan Skop ISMS



Prosedur Teras Yang Telah Dinamakan oleh PTj

PTj	Proses	Sistem Yang Terlibat	Pemilik Proses	Pembangun Sistem
Jabatan Pendaftar	Prosedur Pelantikan Kakitangan (UKM-SPKP-JP-PK01)	SMK	Bahagian Sumber Manusia	Bahagian Aplikasi Sumber Manusia & Penyelidikan
Jabatan Bendahari	**Proses Pembayaran Gaji Kakitangan (UKM-SPKP-BEN-PK11-GP02)**	SMK/uFast	Bahagian Bayaran (Unit Gaji)	Bahagian Aplikasi Sumber Manusia & Penyelidikan
Akademik-UKM	1. Pendaftaran Kursus (UKM/PJK/PPPS/P03/AK03) 2. Tambah, Gugur & Tarik Diri Kursus (UKM/PJK/PPPS/P03/AK04)	SMP	Unit Pendaftaran Kursus Prasiswazah	Bahagian Aplikasi Akademik
PTM	Pengurusan Pengkalan Data	Pengkalan Data Utama Sistem Maklumat UKM	Bahagian Sistem dan Pelayan	Bahagian Sistem dan Pelayan

GAMBARAN PELAKSANAAN MENGIKUT PROSES UTAMA DAN SOKONGAN ISMS UKM MELALUI PENSTRUKTURAN ISMS UKM



GAMBARAN PELAKSANAAN MENGIKUT PROSES UTAMA DAN SOKONGAN ISMS UKM MELALUI PENSTRUKTURAN ISMS UKM

Proses Utama

- Pelantikan Kakitangan Bukan Akademik
- Proses Pembayaran Gaji Kakitangan
- Pendaftaran Kursus Pelajar Prasiswazah
- Pengurusan Pengkalan Data (Sistem dan Pelayan)

Proses Sokongan

- Pengurusan latihan
- Pengurusan tatatertib
- Pengurusan keselamatan
- Penyelenggaraan

Proses Pengurusan

- Pengurusan risiko
- Analisis Data
- Maklumat Berdokumen
- BCM
- CA, Pengukuran & Penambahbaikan
- Audit Dalaman

JANGKAAN KEBERHASILAN

Meningkat keupayaan UKM dalam memberikan jaminan kawalan keselamaan yang berasaskan kepada keperluan/piawaian antarabangsa

Sebagai langkah memperluaskan lagi pengurusan keselamatan maklumat yang menyatukan proses pengoperasian dengan pengurusan data maklumat dalam skop yang dipilih.

Pengurusan keselamatan maklumat yang meyakinkan pihak berkepentingan

Menyebarluaskan lagi penglibatan Warga UKM dalam kesedaran dan pelaksanaan kawalan keselamatan maklumat

Pelaksanaan ISMS UKM berasaskan kepada aktiviti utama universiti

Harapan Pengurusan UKM

Adalah diharapkan agar peluasan skop ISMS ini nanti mencapai hasratnya seperti berikut:

1	2	3
• Memastikan kawalan keselamatan maklumat dalam pengurusan universiti dalam ekosistem yang terkawal dan terjamin	• Mengukuhkan lagi pelaksanaan ISMS efisien dan yang lebih luwes untuk dikembangkan pada masa akan datang	• Memupuk budaya kesedaran yang tinggi dalam kalangan Warga UKM terhadap tanggungjawab mengawal keselamatan maklumat universiti

Pelaksanaan dan Perancangan Aktiviti : (Lampiran)

1. Mengadakan perbincangan awal dengan PTj-PTj yang berkaitan.
2. Perbincangan dengan pihak SIRIM QAS International Sdn Bhd
3. Lawatan Penandaarasan ke UMT
4. Menjalankan analisis jurang terhadap pelaksanaan semasa dengan keperluan mengikut Standard ISO/IEC 27001: 2013.
5. Bengkel Interpretasi Standard bersama Perunding.
6. Mengemaskini keperluan dokumentasi yang diperlukan dalam pelaksanaan ISMS seperti dasar, polisi, peraturan, prosedur dan arahan kerja.
7. Menetapkan kawalan-kawalan keselamatan yang berkaitan sesuai dengan keperluan annex dalam Standard ISO/IEC 27001: 2013.
8. Menyediakan Pelan Pengurusan Risiko bagi pelaksanaan mengikut skop/proses teras yang dipilih.
9. Menyesuaikan pengoperasian seperti proses kerja, analisis data, latihan, kajian kepuasan pelanggan, simulasi dan audit dalaman mengikut pelaksanaan Skop ISMS yang baharu.
10. Menstruktur semula Jawatankuasa Induk ISMS dan Pelaksana ISMS UKM.
11. Mengadakan simulasi pelaksanaan untuk menilai tahap kefahaman dan kepatuhan kepada standard.
12. Menyediakan program-program jerayawara dan promosi kepada Warga PTj yang berkenaan khususnya dan Warga UKM secara am

Semakan Dokumentasi

Bengkel

- Semakan Dokumentasi-15 September, 23 September dan 5 Oktober (JK Dokumentasi dan PTj), 8 Oktober - Semakan bersama perunding (siri 1) dan 2 November - Semakan bersama perunding (Akhir)
- Semakan SoA – 18 Ogos dan (7 September bersama perunding.)
- Semakan RA – 3 September dan 29 September
- Semakan BCM – 22 Sept dan 15 Oktober
- Semakan security metrics – Awal November
- Program Jerayawara – 26-27 Oktober 2020

Status

- 90 % Dokumen (Manual dan PK Utama) telah dikemaskini
- Proses muat naik dokumen akan dilakukan oleh JK Dokumetasi ISMS UKM.
- Kuat kuasa dokumen pada 1 November 2020.

Keperluan Tindakan

JK Dokumentasi

- Pengemaskinian Profil Kualiti (Isu Dalaman & Luaran, Pihak Berkepentingan)
- Pengemaskinian Dokumen Sokongan (Maklumat Perhubungan, Senarai Aset)
- Dasar kawalan keselamatan maklumat
- Objektif kawalan keselamatan maklumat
- Prosedur operasi

JK Risiko dan SoA

- Pengemaskinian SoA
- Pengemaskinian RA dan RTP
- Semakan semula metodologi RA

JK Analisis Data dan CA

- Semakan semula terhadap objektif ISMS
- Semakan semula terhadap Security Metrics

Keperluan Tindakan

JK BCP/PKP

- Semakan ke atas BCM
- Pelan perancangan pelaksanaan
- Governans dan tadbir urus JK BCM ISMS UKM

JK Latihan dan Publisiti

- Program Jerayawara
- Poster hebahan pelaksanan Skop Baharu ISMS UKM

PTj

- Pembentukan/Penstrukturan JK Kualiti PTj
- Penyediaan senarai aset
- Program taklimat kesedaran

JK Induk dan Pelaksana ISMS

- Penstrukturan semula JK Pelaksana
- Semakan terma rujukan JK Induk dan Pelaksana

Keperluan Dokumentasi

Senarai dokumen dan format seperti di lampiran

Tarikh Kuat Kuasa Dokumen 1.11.2020

Bengkel Penyediaan dan Semakan SoA

Bengkel

- 15 September, 23 September dan 5 Oktober (JK Dokumentasi dan PTj)
- 8 Oktober - Semakan bersama perunding (siri 1)
- 2 November - Semakan bersama perunding (Akhir)

Status

- 90 % Dokumen (Manual dan PK Utama) telah dikemaskini
- Pembangunan BCM (JP dan Akademik UKM) padq 15 Oktober 2020.
- Proses muat naik dokumen akan dilakukan oleh JK Dokumetasi ISMS UKM.

SOKONGAN

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

Dokumen ISMS

Atas Talian

- SPD UKM (SPK Sistem Pengurusan Keselamatan Maklumat (ISMS) UKM) http://spdukm.ukm.my/spk/isms/

Capaian

- Melalui Portal e-Warga menggunakan kod pengenalan dan kata laluan yang sama dengan log masuk dan keluar kerja.
- Had capaian ditentukan melalui Prosedur Kawalan Dokumen (PU01)

Format Dokumen

- PDF dan MS Word (doc/docx)

Tahap Kawalan

- Capaian, cetakan dan edaran

Manual (1)

Dokumen Utama (4)

Prosedur Kerja (4)

Dokumen Rujukan Silang

SPKP UKM

- Prosedur Utama
- PKU
- PK PTj

SPK PPPS

- Arahan Kerja (AK) – P02

Prosedur Kerja

Penilaian Risiko (UKM-ISMS-PK01)

- Metodologi sedia ada boleh dikekalkan.
- Menggunakan senarai asset yang diberikan oleh PTj baharu.
- UKM-ISMS-PK01-B001 (Borang Semakan Penilaian Risiko) – Last semakan pada 01/05/2014.
- UKM-ISMS-PK01-SS01(Senarai Semak Pelaksanaan Penilaian Risiko Dan SoA) – Last Semak 15/11/2014

Pengukuran Keberkesanan Kawalan (UKM-ISMS-PK02)

- Tiada cadangan pindaan.
- Pelaksanan boleh dikekalkan.

Kawalan Perubahan (UKM-ISMS-PK03)

- Semakan dan perlukan pindaan.
- Disesuaikan dengan pelaksanaan Skop yang baharu.

Pengurusan Keselamatan Insiden ICT (UKM-ISMS-PK04)

- Tiada cadangan pindaan.
- Pelaksanan boleh dikekalkan.

KEPERLUAN DOKUMEN UTAMA

1
- SoA

2
- RA & RTP

3
- BCM

4
- Pengukuran Kawalan (Security Metrics)

SoA (UKM-ISMS-SoA01)

Bengkel Penyediaan dan Semakan SoA

Bengkel 1 - Penyediaan

- 18 Ogos 2020 (Selasa)
- 9.00 pagi – 4.30 petang
- Pasukan Pemikir, Pemilik Proses dan Pembangun Sistem

Bengkel 2 - Pemurnian

- 7 September 2020
- 9.00 Pagi(Bersemuka)
- Perunding dan Pasukan Pemikir, Pemilik Proses dan Pembangun Sistem

Status

- 90 % Dokumen sokongan di dalam Annex telah disediakan
- Sedang dalam pengemaskinian akhir
- Terdapat beberapa kawalan tambahan yang dikenalpasti
- Pengecualian pada Annex 14 ((Pemerolehan, Pembangunan dan Penyelenggaraan Sistem).

Pengemaskinian SoA (UKM-ISMS-SoA01)

PTJ PELUASAN SKOP	DOKUMEN/MAKLUMAT BAHARU	DOKUMEN/MAKLUMAT KEMASKINI
JABATAN PENDAFTAR	1. GP Kawalan Keselamatan Maklumat Mesyuarat (JP) 2. GP Kawalan Keselamatan Penerimaan Dokumen (JP) 3. UKM-ISMS-L02 : Daftar Aset PTj (JP/BEN/AKADEMIK) 4. UKM-SPKP-PKU08 : Pengurusan Aset Alih (PTJ) 5. KEW-PA.2 : Daftar Harta Modal (PTM/JP/BEN/AKADEMIK-UKM) 6. KEW-PA.3 : Daftar Inventori (PTM/JP/BEN/AKADEMIK-UKM) 7. Pelan Penggantian Peralatan dan perkakasan operasi di JP/BEN/AKADEMIK-UKM 8. UKM-ISMS-BCM03- Pengurusan Kesinambungan Perkhidmatan JP/BEN/AKADEMIK 9. Perjanjian Kerahsiaan (Non Disclosure Agreement) JP/BEN/AKADEMIK 10. Garis Panduan Pengurusan Salah Laku ICT UKM (dalam Pembangunan) 11. Tatacara BDR (Bekerja dari Rumah) *Work From Home* 12. Garis Panduan Penggunaan Peralatan Mudah Alih 13. Dokumen pengesahan pertukaran penjawatan atau penempatan pegawai oleh Urusetia Sistem/ Ketua PTJ/ Ketua 14. GP Aplikasi Mobile (termasuk VPN) 15. Senarai Capaian Server Develop dan Produk	1. UKM-ISMS-MS01-L01 : Senarai Maklumat Perhubungan 2. Dasar Keselamatan Teknologi Maklumat Dan Komunikasi ~~ICT~~ Maklumat 3. Tambahan proses pada NDA 4. Program yang disediakan: Kakitangan: Program Suai Tugas dan Orientasi kepada kakitangan baharu
JABATAN BENDAHARI	1. Buku log Bilik Pemprosesan Gaji bagi mengawal keluar masuk kakitangan yang memproses gaji.	1. UKM-ISMS-GP01 : Keselamatan Fizikal (review) 2. UKM-SPKP-BEN-PK11-GP02 Garis Panduan Pengurusan Gaji Kakitangan (perlu dikemaskini) 3. UKM-SPKP-BEN-PK11-GP02-MO03 Modul ABB – Sub Modul Daftar Gaji 4. Senarai pemegang token CIMB BizChannel beserta terma rujukan (dasar/ TOR – rujuk En. Qamas) 5. Kemaskini Protokol Kawalan Dalaman Jabatan Bendahari.
PUSAT PENGURUSAN AKADEMIK	1. Laporan Audit Trail Aktiviti Pendaftaran Awal, Gugur dan Tambah 2. GP untuk menangani insiden penggunaan id 3. Senarai atau Peraturan yang berkaitan (Akademik)	

RA (UKM-ISMS-RA01) & RTP (UKM-ISMS-RTP01)

RISK ASSESMENT REPORT (UKM-ISMS-RA01)

Bengkel dan Perbincangan

- Perbincangan pada 3 September 2020.
- Pengemaskinian RA – Bengkel pada 29 September 2020

Pindaan

- Pengemaskinian RA
- Senarai Aset yang akan digunakan daripada BEN, JP dan Akademik-UKM)
- Cara penulisan boleh ditentukan mengikut kesesuaian pelaksanaan.

Status Dokumen

- 90% telah dikemaskini.
- Penyelarasan akan dilaksanakan ke atas ketiga-tiga RA yang dibangunkan (JP, BEN dan Akademik UKM) Untuk menilai risiko yang generic.
- Semakan semula dan pemurnian akan dilaksanakan oleh JK Pengurusan Risiko dan SoA.

RISK TREATMENT PLAN(UKM-ISMS-RTP01)

Bengkel

- Perbincangan pada 3 September 2020.
- Pengemaskinian RTP – akan diadakan selepas RA dikemaskini.

Cadangan Pindaan

- Pengemaskinian RTP setelah RA dikenalpasti
- Cara penulisan boleh ditentukan mengikut kesesuaian pelaksanaan.

Status

- Masih dalam pembangunan.

BCM (UKM-ISMS-BCM01)

Pengurusan Kesinambungan Perkhidmatan PTM (UKM-ISMS-BCM01)

Cadangan Pindaan

- Pengemaskinian PKP bagi setiap Skop Pelaksanaan
- Sedia ada – PKP PTM dan PKP Kewangan (Perlu semakan) jika sesuai boleh diteruskan
- Baharu – PKP Jabatan Pendaftar dan PKP Akademik UKM
- Penyelarasan akan dibuat bersama ROSH-UKM

Status

- Perbincangan pada – 22 September 2020
- Bengkel Penyediaan BCM (JP dan Akademik UKM) pada 15 Oktober 2020.

Pengukuran Keberkesanan Kawalan (UKM-ISMS-PK02)

Pengukuran Keberkesanan Kawalan(UKM-ISMS-PK02)

Cadangan Pindaan

- Semakan semula terhadap objektif ISMS
- Semakan semula terhadap Security Metrics
- Mengekalkan kaedah dan metodologi di dalam pengukuran keberkesanan.

Status

- Perancangan perbincangan belum diadakan lagi.
- Perbincangan bersama JK Analisis Data dan CA akan ditentukan nanti..

Cadangan Objektif Kualiti ISMS

i. Memastikan data tersedia dan boleh dicapai pada bila-bila masa:
   - Capaian data adalah pada tahap yang baik (24x7)
   - Pemulihan capaian dalam tempoh maksimum 24 jam

ii. Memastikan semua capaian SMU kritikal perlu mempunyai ID yang sah dan disemak secara berkala setiap 6 bulan.

iii. Memastikan proses pendaftaran/tambah, gugur dan tarik diri kursus dilakukan dalam tempoh yang ditetapkan pada setiap semester berdasarkan Pekeliling Akademik untuk memastikan maklumat dapat direkod dengan tepat

iv. Memastikan lantikan kakitangan dilaksanakan adalah memenuhi syarat dan skim perkhidmatan yang ditetapkan oleh JPA untuk menjamin maklumat pelantikan yang mematuhi syarat.

v. Memastikan pembayaran gaji dilaksanakan mengikut proses dan kawalan yang ditetapkan untuk menjamin ketepatan dan keselamatan maklumat gaji kakitangan.

Audit Kualiti Dalaman ISMS UKM (UKM-SPKP-PU03)

Pelaksanaan Audit Kualiti Dalaman ISMS UKM

Cadangan pelaksanaan

- Pelaksanaan pada bulan Jan-Feb 2021.
- Melibatkan penilaian rekod ke atas skop baharu mulai 1.11.2020.
- Namun data bagi skop sedia ada (pengurusan pengkalan data) boleh dinilai mulai Mac 2020 sehingga tarikh pelaksanaan Audit.
- Masih mengekalkan Prosedur Audit Kualiti Dalaman (UKM-SPKP-PU03)

Keperluan Tindakan

- Pembentukan pasukan audit yang mencukupi.
- Menyemak keperluan dokumentasi Audit Kualiti Dalaman jika terdapat pindaan yang perlu dilakukan.
- Taklimat kepada pasukan audit yang terlibat.
- Penjadualan berdasakan kepada skop baharu.

MSP ISMS UKM
(UKM-SPKP-PU08)

Pelaksanaan MSP ISMS UKM

Cadangan pelaksanaan

- Pelaksanaan pada bulan Mac atau April 2021.
- Melibatkan pengumpulan data ke atas skop baharu mulai 1.11.2020.
- Namun data bagi skop sedia ada (pengurusan pengkalan data) boleh dinilai mulai Jan-Dis 2020
- Masih mengekalkan Prosedur Mesyuarat Semakan Pengurusan (UKM-SPKP-PU08).
- Agenda mesyuarat masih dikekalkan, namun semua laporan perlu mengambil kira pelaksanaan skop baharu (JP, BEN dan Akademik UKM)

Keperluan Tindakan

- Penyediaan format pelaporan.

Program Jerayawara

Pelaksanaan Program Jerayawara ISMS UKM

Cadangan pelaksanaan

- Diselaraskan oleh Jawatankuasa Latihan dan Publisiti ISMS
- Melibatkan Warga di PTj Baharu (JP, BEN dan Akademik UKM)
- Cadangan tarikh pelaksanaan pada 26 & 27 Oktober 2020.
- Penyediaan dan edaran poster pelaksanaan skop baharu (kuat kuasa 1 November 2020)

Keperluan Tindakan

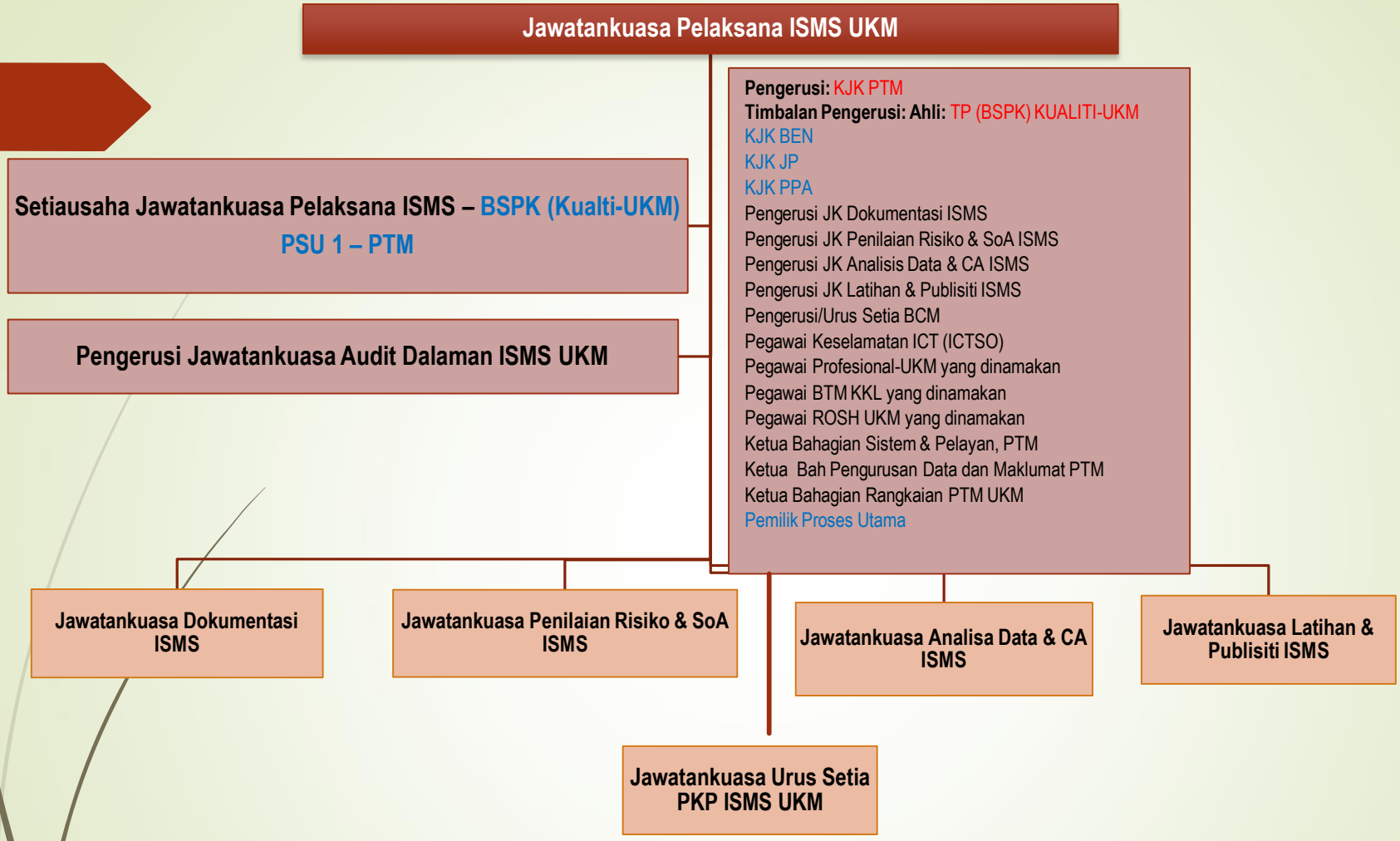
- Penyelarasan taklimat.
- Hebahan dan rekod pelaksanaan taklimat kesedaran.
- Edaran poster kesedaran kepada PTj yang terlibat.
- Pengenalan kepada Anugerah Khas Kawalan Keselamatan Maklumat.

Sistem Urus Tadbir JK ISMS UKM
Mulai 1 November 2020

Jawatankuasa Induk ISMS UKM

Wakil Pengurusan / Pengerusi: CIO
Timbalan Wakil Pengurusan:
Pengarah Kualiti-UKM
Ahli:
Pendaftar
Bendahari
Ketua Pustakawan
Timbalan Pendaftar PPA
Pengarah Eksekutif Strategi
Pengarah Profesional UKM
Pengarah Prasarana UKM
Pengarah CRIM
Pengarah ROSH-UKM
Timbalan Pengarah IT Kampus KL
Pakar Teknikal (Keselamatan Maklumat)
Pengerusi JK Pelaksana ISMS
Ketua Juruaudit Dalaman ISMS
Penasihat Undang-undang UKM
Pakar Risiko UKM
Pegawai Keselamatan ICT (ICTSO)

- Setiausaha Jawatankuasa Induk ISMS
- Jawatankuasa Audit Dalaman ISMS UKM
- Setiausaha Jawatankuasa Pelaksana ISMS
  - Jawatankuasa Dokumentasi ISMS
  - Jawatankuasa Penilaian Risiko & SoA ISMS
  - Jawatankuasa Urus Setia PKP ISMS UKM
  - Jawatankuasa Analisa Data & CA/PA ISMS
  - Jawatankuasa Latihan & Publisiti ISMS



- Pengerusi JK Kecil Pelaksana ISMS sedia ada dikekalkan sekurang-kurangnya untuk tempoh satu selepas pelaksanaan atau satu kitaran pensijilan.
- Penambahan AJK di dalam setiap JK dengan mengambil kira ahli daripada PTj baharu.
- Surat pelantikan kepada AJK baharu akan dikeluarkan.

Pembentangan Kepada Pihak SIRIM QAS International Sdn Bhd

Tarikh & Masa

- 6 November 2020 (Jumaat)
- 11.00 Pagi
- MS Teams

Objektif

- Penerangan pelaksanaan skop baharu kepada pihak SIRIM QAS International Sdn Bhd.
- Permohonan pengecualian beserta justifikasi.

Sesi 3

Keperluan Standard MS ISO/IEC

ISO 27001 is
INFORMATION SECURITY
NOT
IT SECURITY

ISMS……

I – Information

S – Security

M – Management

S – System

What is Information Security?

"Information Security protects information from a wide range of threats in order to ensure business continuity, minimise business damage and maximise return on investment and business opportunities."

Komponen Asas

Confidentiality (Kerahsiaan)

Ensuring that information is accessible only to those authorised to have access.

Sesuatu maklumat aset itu tidak boleh dicapai atau didedahkan kepada individu, entiti atau proses tertentu

Integrity (Integriti)

Safeguarding the accuracy and completeness of information and processing methods.

Sesuatu aset itu dilindungi ketepatan dan kesempurnaannya

Availability (Ketersediaan)

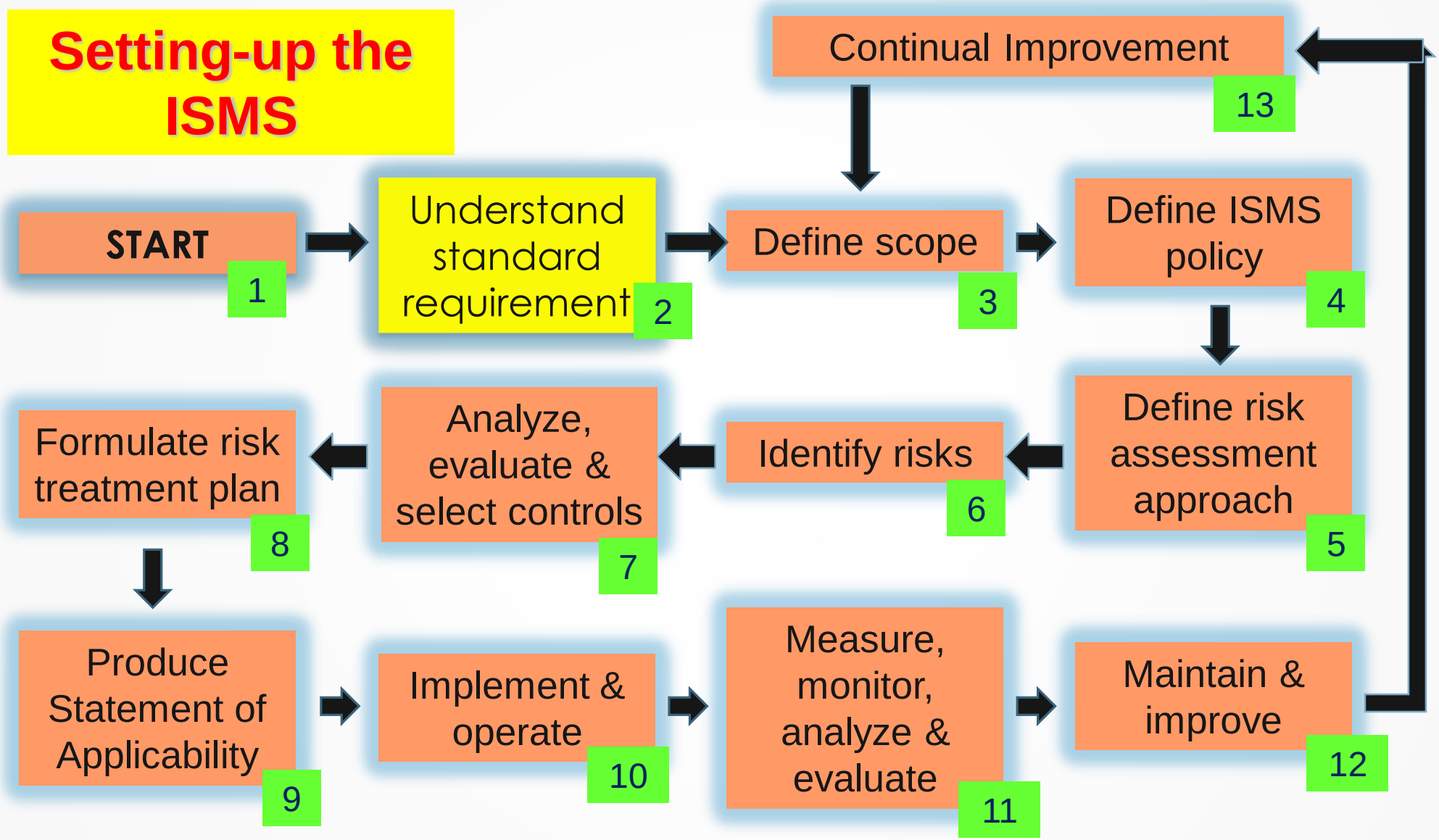
Ensuring that authorised users have access to information and associated assets when required.

Sesuatu aset itu boleh dicapai dan digunakan apabila diperlukan oleh entiti yang dibenarkan.

In some organisations, integrity and / or availability may be more important than confidentiality.

- Industry working group – 1993
- Code of Practice issued – 1993
- BS 7799 Part One published – February 1995
- BS 7799 Part Two published – February 1998
- BS 7799:1999: Part 1 and Part 2 – April 1999
- ISO 17799 (BS 7799-1) published 2000
- BS 7799-2 published 2002
- ISO 17799:2005
- ISO 27001:2005
- MS ISO 27001:2007
- ISO 27001:2013

ISO/IEC 27001:2013 – Information Security Management System (ISMS)



ISMS PDCA MODEL

ISO/IEC 27001:2013 – Information Security Management System (ISMS)

Understand Standard requirement

1

Major Clauses

Clause 1
Clause 2
Clause 3
Clause 4
Clause 5
Clause 6
Clause 7
Clause 8
Clause 9
Clause 10

2

SOA

Annex A

A.5
A.6
A.7
A.8
A.9
A.10
A.11
A.12
A.13

A.14
A.15
A.16
A.17
A.18

ISO/IEC 27001:2013 – Information Security Management System (ISMS)

Security Domains + more

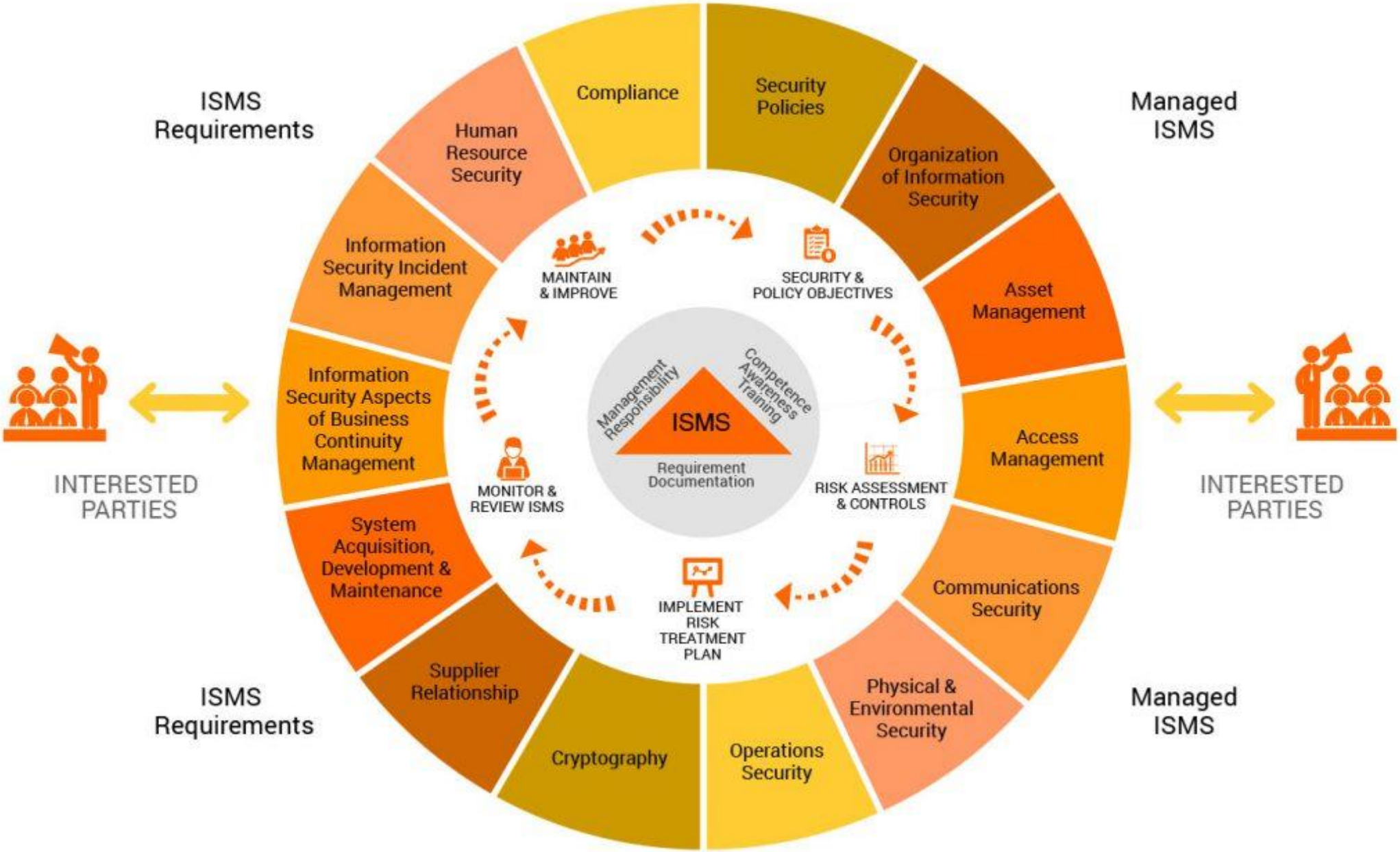
Security Domains – ISO 27001:2013 version
Annex A

1. Scope, Information Security Management System
2. Information Security Policies *(A.5)*
3. Organization of Information Security *(A.6)*
4. Human Resource Security *(A.7)*
5. **Asset Management (A.8)**
6. **Access Control (A.9)**
7. **Cryptography (A.10)**
8. Physical and Environmental Security *(A.11)*
9. **Operations Security (A.12)**
10. **Communications Security (A.13)**
11. System Acquisition, Development, and Maintenance *(A.14)*
12. Supplier Relationships *(A.15)*
13. **Information Security Incident Management (A.16)**
14. **Information Security Aspects of Business Continuity Management (A.17)**
15. Compliance *(A.18)*

Total 114 Controls

& risk assessment…

ISO/IEC 27001:2013 – Information Security Management System (ISMS)



STRUCTURE OF ISO 27001 2013 INFORMATION SECURITY MANAGEMENT STANDARD

UNIVERSITI KEBANGSAAN MALAYSIA
The National University of Malaysia

ISMS stands for Information Security Management System.

- **4. CONTEXT**
  - 4.1 Understand your organization's context
  - 4.2 Define the expectations of interested parties
  - 4.3 Clarify scope of infosec management system
  - 4.4 Develop an infosec management system
- **5. LEADERSHIP**
  - 5.1 Provide leadership and show that you support ISMS
  - 5.2 Establish an appropriate information security policy
  - 5.3 Assign ISMS roles, responsibilities, and authorities
- **6. PLANNING**
  - 6.1 Formulate actions to address risks and opportunities
    - 6.1.1 Consider risks and opportunities when you plan your ISMS
    - 6.1.2 Establish an information security risk assessment process
    - 6.1.3 Develop an information security risk treatment process
  - 6.2 Set ISMS objectives and make plans to achieve them
- **7. SUPPORT**
  - 7.1 Support ISMS by providing resources
  - 7.2 Support ISMS by promoting competence
  - 7.3 Support ISMS by making people aware of duties
  - 7.4 Support ISMS by controlling ISMS communications
  - 7.5 Support ISMS by managing related information
    - 7.5.1 Include information and documents that the ISMS needs
    - 7.5.2 Manage the creation and modification of ISMS documents
    - 7.5.3 Control your organization's ISMS documents and records

Sesi 4

Standard MS ISO/IEC

Sesi 5

Soal Jawab

SEKIAN
TERIMA KASIH