MESYUARAT
KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT
MS ISO/IEC 27001:2013
KALI KEEMPAT

TARIKH : 27 NOVEMBER 2015 (JUMAAT)
MASA : 10.30 PAGI HINGGA 12.15 TENGAH HARI
TEMPAT : BILIK MESYUARAT UTAMA, ARAS 4, FAKULTI PERUBATAN DAN SAINS KESIHATAN, UNIVERSITI PUTRA MALAYSIA

MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT
MS ISO/IEC 27001:2013
KALI KEEMPAT (1/2015)

AGENDA	RUJUKAN/PEMBENTANG
KATA ALUAN PENGERUSI	Pengerusi
1.0 PENGESAHAN MINIT MESYUARAT Minit Mesyuarat MKSP Kali Ketiga (Bil 1/2014)	**[Kertas 1] -** Pengerusi
2.0 TINDAKAN SUSULAN MESYUARAT LEPAS Tindakan Susulan Mesyuarat MKSP ISMS Kali Ketiga	**[Kertas 2] -** Setiausaha
3.0 PERUBAHAN ISU DALAMAN DAN ISU LUARAN	**[Kertas 3]** – Wakil Pengurusan
4.0 MAKLUM BALAS PRESTASI KESELAMATAN MAKLUMAT 4.1 Ketakakuran dan Tindakan Pembetulan 4.2 Pemantauan dan Pengukuruan 4.2.1 Objektif ISMS 4.2.2 Pelaksanaan kawalan di Pelan Pemulihan Risiko	 **[Kertas 4]** – Wakil Pengurusan **[Kertas 5]** – Wakil Pengurusan **[Kertas 6]** – Wakil Pengurusan
5.0 PENEMUAN AUDIT 5.1 Audit Pemantauan 2 (SIRIM) 5.2 Audit Dalaman ISMS 2015	 **[Kertas 7]** – Penyelaras Audit **[Kertas 8]** – Ketua Juruaudit Audit Dalaman ISMS 2015
6.0 MAKLUM BALAS PEMEGANG TARUH	**[Kertas 9]** – Wakil Pengurusan
7.0 HASIL PENILAIAN RISIKO DAN STATUS PELAN PEMULIHAN RISIKO	**[Kertas 10] –** Wakil Pengurusan

MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT MS ISO/IEC 27001:2013 KALI KEEMPAT	
AGENDA	**RUJUKAN/PEMBENTANG**
8.0 PELUANG PENAMBAHBAIKAN	**[Kertas 11] –** Wakil Pengurusan
9.0 HAL-HAL LAIN **9.1 Audit Pensijilan Semula**	**[Secara lisan, tanpa kertas edaran] –** Penyelaras Audit
KESIMPULAN	Pengerusi

AGENDA 1.0

PENGESAHAN MINIT MESYUARAT

MINIT MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) UNIVERSITI PUTRA MALAYSIA KALI KETIGA (BIL. 1/2014)

MINIT MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
UNIVERSITI PUTRA MALAYSIA (UPM)
KALI KETIGA (BIL. 1/2014)

Tarikh	:	1 Disember 2014 (Isnin)
Masa	:	3.00 petang
Tempat	:	Dewan Senat, Bangunan Pentadbiran
Kehadiran	:	Lampiran A

PENDAHULUAN Kata Aluan Pengerusi

Pengerusi –

a) mengalu-alukan kehadiran ahli mesyuarat ke Mesyuarat Kajian Semula Pengurusan (MKSP) ISO/IEC 27001:2013 Universiti Putra Malaysia Kali Ketiga.

b) memaklumkan audit pemantauan oleh SIRIM akan diadakan pada 29 dan 30 Januari 2015.

MINIT 3.1 Pengesahan Minit Mesyuarat

Minit MKSP ISMS Kali Kedua [Bil 1/2013] disahkan tanpa sebarang pindaan.

MINIT 3.2 Tindakan Susulan Mesyuarat Lepas

Mesyuarat dimaklumkan berkenaan tindakan susulan yang telah dilaksanakan daripada mesyuarat yang lepas (Minit MKSP ISMS Kali Kedua [Bil. 1/2013]) sebagaimana berikut:

3.2.1 Daripada Minit 2.1.3.3 – Teknik, Produk atau Prosedur yang Boleh Digunakan Organisasi bagi Penambahbaikan Prestasi dan Efektif Sistem Pengurusan Keselamatan Maklumat

Mesyuarat mengambil maklum yang berikut:

a) PKP UPM telah diluluskan oleh Mesyuarat Jawatankuasa Pengurusan Universiti Ke-516 pada 28 Mei 2014. Jawatankuasa Pemandu PKP UPM telah ditubuh dan dipengerusikan oleh YBhg. Dato' Wan Azman Wan Omar (Pendaftar). Mesyuarat Pertama Jawatankuasa Pemandu PKP telah diadakan pada 15 Ogos 2014.Walau bagaimana PKP UPM masih belum disimulasikan secara intergrasikan melibatkan ERT, CCT dan DRT.

b) Pasukan Tindakan Kecemasan atau *Emergency Response Team* (ERT) telah diwujud/dilantik oleh Pejabat Keselamatan dan Kesihatan Pekerjaan (PKKP) berdasarkan Pelan Pengurusan Bencana /*Disaster Management Plan* (DMP – UPM) di setiap PTJ. Program latihan dikendalikan oleh PKKP dari semasa ke semasa.

(Makluman: Semua)

3.2.2 Daripada Minit 2.1.3.5 – Keputusan Keberkesanan Pengukuran

Mesyuarat mengambil maklum antara langkah yang telah diambil bagi memastikan pelaksanaan salinan *backup redundance* untuk pangkalan data sebagaimana berikut:

(1) Pembangunan infrastruktur *server* dan storan Pemulihan Bencana (DR) untuk aplikasi utama Universiti.
(2) Pembangunan storan khas untuk mengarkib semua pangkalan data Universiti (secara harian).
(3) Kesemua infrastruktur berkenaan diletakkan di Pusat Pemulihan Bencara (DRC).

(Makluman: Semua)

3.2.3 Daripada Minit 2.1.3.7 – Peluang Penambahbaikan

Mesyuarat mengambil maklum yang berikut:

a) Pihak iDEC telah membuat permohonan kepada PPPA untuk menduduki bangunan Institut Kajian Dasar Pertanian dan Makanan (IKDPM) yang bakal dikosongkan. Pihak PPPA telah mencadangkan bangunan tersebut untuk diduduki oleh iDEC selepas pihak IKDPM berpindah ke bangunan lama PBS (dahulunya GSM). Walau bagaimanapun, pengambilalihan lokasi yang terbabit masih belum berlaku kerana pihak PBS masih belum berpindah masuk ke bangunan baharu yang telah dibina.

b) Fasa pertama pembangunan UPM-ID telah selesai pada penghujung tahun 2013. Pada tahun 2014 proses pelaksanaan bermula dengan staf UPM mendaftar UPM-ID yang melibatkan pertukaran kata laluan mengikut polisi, pengesahan emel kedua dan mengesetkan soalan keselamatan. Penggunaan UPM-ID akan dikuatkuasakan sepenuhnya pada Januari 2015 melibatkan sistem emel Putra, Putra (Lotus Notes), eISO, SPLN dan eLPPT. Fasa kedua melibatkan pelaksanaan *Single Sign On* pada tahun 2016.

(Makluman: Semua)

3.2.4 Daripada Minit 2.3 – Maklum Balas Pihak yang Berkepentingan

Mesyuarat mengambil maklum bahawa –

a) kaji selidik kepuasan pelanggan iDEC bagi tahun 2014 dijalankan dalam empat (4) fasa. Kaji selidik kepuasan pelanggan untuk suku tahun pertama (Q1), kedua (Q2) dan ketiga (Q3) telah dilaksanakan sementara bagi suku tahun keempat (Q4) akan dijalankan pada bulan Januari 2015. Berikut adalah jumlah responden dan kaedah kaji selidik pada Q1 hingga Q3:

Q1: 454 orang (Kaedah: *online* dan edaran salinan keras).
Q2: 33 orang (Kaedah: *online* sahaja).
Q3: 333 orang (Kaedah: *online* dan edaran salinan keras); dan

b) kaji selidik kepuasan pelanggan bagi tempoh Q1 – Q3 tahun 2014 menunjukkan pencapaian 65.12% kepuasan pada skala 4 dan ke atas (daripada skala likert 5).

(Makluman: Semua)

3.2.5 Daripada Minit 2.4 – Teknik, Produk atau Prosedur yang Boleh Digunakan Organisasi bagi Penambahbaikan Prestasi dan Efektif Sistem Pengurusan Keselamatan Maklumat

Mesyuarat mengambil maklum bahawa fasa pertama penyatuan pengurusan ISMS dengan SPK dan EMS akan bermula semasa Bengkel Integrasi Dokumen ISO yang dijadualkan pada 17 dan 18 Disember 2014.

(Makluman: Semua)

3.2.6 Daripada Minit 2.6 – Kelemahan atau Ancaman yang Tidak Diambil Kira pada Penilaian Risiko yang Lepas

Mesyuarat mengambil maklum yang berikut:

a) Infrastruktur *server* aplikasi utama yang telah melebihi had penggunaan telah dinaiktaraf melibatkan aplikasi berikut:

(1) Aplikasi Sumber Manusia.
(2) Aplikasi Kewangan (*server* dan storan).
(3) Aplikasi SMP (storan).

b) Pasukan *Risk Assessment* telah melaksanakan semakan penilaian risiko seperti berikut:

(1) Semakan 0: Februari 2012 (Penilaian 1).
(2) Semakan 1: Mei 2013 (Kemas kini *step* 7).
(3) Semakan 2: Oktober 2013 (Kemas kini aset).
(4) Semakan 3: Mei 2014 (Perubahan *Standard*).

(Makluman: Semua)

3.2.7 Daripada Minit 2.7 – Keputusan Keberkesanan Pengukuran

Mesyuarat mengambil maklum yang berikut:

(a) Perbezaan pengukuran tahun 2013 dan 2014 dibincangkan pada Minit 3.5.

(Makluman: Semua)

(b) Pencapaian semasa akan diukur melalui pencapaian Objektif Keselamatan Maklumat baharu dalam pelaksanaan ISMS di bawah piawaian ISO/IEC 27001:2013 sebagaimana berikut:

(1) Memastikan penilaian risiko dan pelan pemulihan risiko dilaksanakan apabila berlaku perubahan kepada Dasar ISMS atau inventori yang termaktub dalam skop.
(2) Menjalankan ujian kesinambungan perkhidmatan ICT sekurang-kurangnya 1 kali setahun.
(3) Memastikan 80% staf telah diberi kesedaran mengenai ISMS dalam tempoh lima (5) tahun.
(4) Memastikan insiden keselamatan ICT tidak melebihi 10 kali pada setiap tahun.
(5) Memastikan gangguan kepada ketersediaan rangkaian (Internet dan Intranet) tidak melebihi 10% setiap tahun.
(6) Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam.
(7) Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden.

(Makluman: Semua)

3.2.8 Daripada Minit 2.9 – Peluang Penambahbaikan

Mesyuarat mengambil maklum yang berikut:

a) Penyatuan pengurusan ISMS dengan pengurusan SPK akan berkuatkuasa pada tahun 2015 di bawah Bahagian Pengurusan Kualiti, Pejabat Pendaftar, UPM.

b) Penempatan secara hibrid telah dibuat di lima (5) PTJ yang mempunyai sistem utama Universiti bagi memastikan kelancaran urusan melibatkan sistem. Maklumat penempatan hibrid adalah sebagaimana berikut:

PTJ	Sistem	Nama Pegawai
Bahagian Akademik	SMP	Pn. Nor Ruhil Amal Hashim
Sekolah Pengajian Siswazah	iGIMS	En. Azman Shah Mohd Shahar
Pejabat Pendaftar	Sistem Maklumat Sumber Manusia	Pn. Sofiyatul Salmi Ismail
Pejabat Bursar	Sistem Kewangan	Pn. Azlina Shafie
Pusat Kesihatan Universiti	eKLINIK	En. Hafiz Abd Jalil

(Makluman: Semua)

3.2.9 Daripada Minit 2.10 – Hal-hal Lain

Mesyuarat mengambil maklum bahawa Kaedah-Kaedah UPM (Teknologi Maklumat dan Komunikasi) telah mendapat kelulusan Lembaga Pengurusan Universiti dan telah digunapakai berkuatkuasa 1 Januari 2014. Dokumen ini serta Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK) telah digunapakai sebagai rujukan dalam pelaksanaan ISMS UPM.

(Makluman: Semua)

MINIT 3.3 Penemuan Audit

3.3.1 Audit Pemantauan oleh SIRIM

Mesyuarat mengambil maklum pembentangan penemuan Audit Pemantauan Sistem Pengurusan Keselamatan Maklumat (ISO/IEC 27001:2005) oleh SIRIM yang dilaksanakan pada 24 dan 5 September 2013 sebagaimana berikut:

a) Seramai dua (2) orang Juruaudit telah terlibat bagi mengaudit skop Operasi Pusat Data meliputi Aplikasi Laman Sesawang UPM, Sistem Pengurusan Kewangan, Pengurusan Sumber Manusia dan Sistem Maklumat Pelajar.

b) Hasil audit terdapat satu (1) ketakakuran telah ditemui dan lima (5) peluang penambahbaikan telah dicadangkan.

c) Bukti penutupan ketakakuran telah dikemukakan kepada SIRIM pada 6 Disember 2013 dan pihak SIRIM telah mengesahkan penutupan pada 16 Disember 2013. Cadangan penambahbaikan telah diambil tindakan dan akan disemak oleh

pihak SIRIM semasa Audit Pemantauan yang akan dijalankan pada Januari 2015.

(Makluman: Semua)

3.3.2 Audit Dalaman

Mesyuarat mengambil maklum pembentangan penemuan Audit Dalaman UPM yang dilaksanakan pada 11 dan 12 November 2014 sebagaimana berikut:

a) Audit Dalaman ini merupakan yang pertama diadakan setelah UPM beralih daripada Sistem Pengurusan Keselamatan Maklumat MS ISO/IEC 27001:2007 (ISO/IEC 27001:2005) kepada ISO/IEC 27001:2013.

b) Seramai 16 orang Juruaudit telah terlibat bagi mengaudit skop Pusat Data merangkumi perkakasan (*server* dan storan), Pelajar Prasiswazah (SMP), Sistem Maklumat Pelajar Siswazah (iGIMS), Sistem Sumber Manusia (HRM), Sistem Kewangan (KEW) dan Laman Web Utama Universiti (WEB).

c) Hasil audit terdapat 13 ketakakuran telah ditemui dan 14 peluang penambahbaikan telah dicadangkan.

d) Kesemua rekod ketakakuran telah diambil tindakan dengan 11 daripadanya telah ditutup dan dua (2) belum ditutup kerana memerlukan masa yang lebih lama untuk menentukan keberkesanan tindakan penutupan yang diambil. Tindakan ke atas semua cadangan penambahbaikan sedang diambil tindakan namun ada di antaranya memerlukan peruntukan kewangan untuk dilaksanakan.

(Tindakan: TWP ISMS)

Kesimpulan

Selepas menerima dan mengkaji semula laporan audit dalaman**,** mesyuarat memutuskan bahawa –

i. secara keseluruhannya UPM telah melaksanakan ISMS dengan baik; dan

ii. peluang penambahbaikan yang dicadangkan perlu diberi perhatian serius bagi menambahbaik lagi pelaksanaan ISMS ISO/IEC 27001:2013.

MINIT 3.4 Maklum Balas Pemegang Taruh

Mesyuarat mengambil maklum Laporan Kaji Selidik Persepsi Pemegang Taruh terhadap Pelaksanaan ISMS di UPM yang dilaksanakan pada 19-21 November 2014 sebagaimana berikut:

a) Kumpulan sasaran adalah pihak Pemilik Proses Sistem Aplikasi Utama Universiti iaitu Pejabat Perancangan Strategik dan Korporat, Pejabat Pendaftar, Pejabat Bursar, Bahagian Akademik dan Sekolah Pengajian Siswazah.

b) Maklum balas dilihat dari tiga (3) sudut iaitu –
   i. tahap kefahaman keperluan keselamatan data/maklumat selepas pelaksanaan ISMS;
   ii. tahap keyakinan pada perkhidmatan Pusat Data dalam mengurus *server* aplikasi selepas pelaksanaan ISMS; dan
   iii. tahap keyakinan pada perkhidmatan aplikasi yang diurus selepas pelaksanaan ISMS.

c) Hasil kaji selidik mendapati –
   i. majoriti pemegang taruh mempunyai pemahaman yang tinggi terhadap kerahsiaan data, integriti data dan ketersediaan data;
   ii. secara keseluruhannya pemegang taruh lebih yakin terhadap perkhidmatan Pusat Data dalam mengurus *server* aplikasi dari aspek kerahsiaan, integriti dan ketersediaan perkhidmatan; dan
   iii. secara keseluruhannya pemegang taruh lebih berkeyakinan terhadap perkhidmatan aplikasi yang diurus oleh pihak iDEC dari aspek kerahsiaan, integriti dan ketersediaan perkhidmatan.

(Makluman: Semua)

<u>Kesimpulan</u>

Hasil daripada kaji selidik persepsi pemegang taruh yang dilaksanakan berkenaan pelaksanaan ISMS terhadap keselamatan data Sistem Aplikasi Utama Universiti adalah sebagaimana berikut:

i. Pusat Pembangunan Maklumat dan Komunikasi selaku Jawatankuasa Pelaksana Sistem Pengurusan Keselamatan Maklumat perlu menambah usaha mewar-warkan kepada pengguna berkenaan objektif pelaksanaan ISMS bagi meningkatkan kefahaman dan keyakinan pengguna.

ii. Pihak pemegang taruh secara majoriti telah memahami kepentingan pelaksanaan ISMS terhadap sistem aplikasi utama Universiti.

iii. Tahap kepercayaan pemegang taruh terhadap perkhidmatan Pusat Data lebih tinggi selepas pelaksanaan ISMS (meningkat daripada 60% kepada 80%).

iv. Pemegang taruh sebagai pemilik sistem aplikasi lebih berkeyakinan terhadap keselamatan data/maklumat aplikasi yang digunakan oleh pelanggan masing-masing, sekaligus meningkatkan tahap perkhidmatan mereka.

MINIT 3.5 Prestasi Proses dan Kepatuhan Produk/Perkhidmatan

Mesyuarat mengambil maklum yang berikut:

a) Laporan prestasi proses diukur berdasarkan pencapaian objektif keselamatan maklumat pada tahun 2013 dan 2014. Terdapat perbezaan objektif keselamatan maklumat berikutan penggunaan piawaian MS ISO/IEC 27001:2007 pada tahun 2013 dan piawaian ISO/IEC 27001:2013 bagi tahun 2014 yang hanya akan dibuat pengukuran dalam tahun 2015.

b) Objektif baharu ISMS adalah sebagaimana berikut:

   i. Memastikan 80% staf telah diberi kesedaran pelaksanaan mengenai ISMS dalam tempoh 5 tahun.
   ii. Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam.
   iii. Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden.

c) Pencapaian objektif keselamatan yang diukur dipaparkan pada **Lampiran 1**.

(Tindakan: TWP ISMS)

Kesimpulan

Setelah menerima dan meneliti laporan yang dibentangkan, UPM mendapati bebahawa Objektif ISMS telah disesuaikan dengan keperluan piawaian baharu iaitu ISO/IEC 27001:2013.

MINIT 3.6 Ketakakuran dan Tindakan Pembetulan

Mesyuarat mengambil maklum terdapat dua (2) ketakakuran telah dikenalpasti di dalam pelaksanaan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2013. Punca ketakakuran dan tindakan pembetulan yang berkesan telah dikenalpasti sebagaimana pada **Lampiran 2**.

(Makluman: Semua)

Kesimpulan

Setelah menerima dan meneliti laporan yang dibentangkan, UPM mendapati bahawa ketakakuran dan tindakan pembetulan direkodkan dan dilaksanakan secara berterusan ke atas Sistem Pengurusan Keselamatan Maklumat untuk meningkatkan prestasi penyampaian perkhidmatan kepada pelanggan dan pemegang taruh.

MINIT 3.7 **Perubahan yang Memberi Kesan kepada Sistem Pengurusan Keselamatan Maklumat**

Mesyuarat mengambil maklum yang berikut:

a) Beberapa perubahan yang memberi kesan kepada ISMS telah dilaksanakan bagi menambahbaik perkhidmatan ICT di UPM.

b) Tindakan yang telah diambil antara lain adalah sebagaimana berikut:

   i. Penaiktarafan infrastruktur Pusat Data.

   ii. Penaiktarafan server Sistem Aplikasi Utama Universiti.

   iii. Mengadakan server Pemulihan Bencana Universiti.

   iv. Mengadakan storan Khas Mengarkib Data Universiti.

   v. Penaiktarafan Bilik Persediaan Server (Stagging).

c) Kesan tindakan yang telah diambil ke atas pelaksanaan Sistem Pengurusan Keselamatan Maklumat di UPM adalah sebagaimana pada **Lampiran 3**.

(Makluman: Semua)

Kesimpulan

Selepas menerima dan mengkaji semula laporan, mesyuarat memutuskan bahawa UPM telah melaksanakan perubahan yang memberi kesan kepada pelaksanaan ISMS secara berterusan untuk meningkatkan prestasi penyampaian perkhidmatan dan mencapai tahap kepuasan pemegang taruh.

MINIT 3.8 **Hasil Penilaian Risiko dan Status Pelan Pemulihan Risiko**

Mesyuarat mengambil maklum yang berikut:

a) Penilaian risiko telah dilaksanakan oleh Pusat Pembangunan Maklumat dan Komunikasi dengan kerjasama Pentadbir Proses Universiti yang terlibat sejak tahun 2012.

b) Penilaian risiko yang dilaksanakan menggunakan Sistem Aplikasi *Malaysia Risk Assessment Methodology* (MyRAM) yang telah dibangunkan oleh pihak Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU).

c) Laporan ringkas hasil penilaian risiko tahun 2014 adalah sebagaimana pada **Lampiran 4**.

(Makluman: Semua)

Kesimpulan

Setelah menerima dan meneliti laporan yang dibentangkan, UPM mendapati beberapa penurunan tahap risiko aset yang berkaitan daripada berstatus HIGH kepada MEDIUM oleh pihak *High Level Recommendation.* Walau bagaimanapun, terdapat penambahan aset yang berisiko iaitu perkakasan Sistem Aplikasi Pelajar (Siswazah) berikutan pindaan skop ISMS dalam tahun 2014. Penilaian terhadap risiko sentiasa dilaksanakan secara berterusan bagi memastikan jaminan kualiti keselamatan maklumat sentiasa ditahap maksimum.

MINIT 3.9 **Peluang Penambahbaikan**

Mesyuarat mengambil maklum lima (5) peluang penambahbaikan yang telah dikenalpasti di dalam pelaksanaan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2013 sebagaimana pada **Lampiran 5**.

(Tindakan: TWP ISMS)

Kesimpulan:

Selepas menerima dan mengkaji semula laporan, mesyuarat memutuskan bahawa UPM telah merancang tindakan untuk menambahbaik dan meningkatkan prestasi penyampaian perkhidmatan serta tahap kepuasan pemegang taruh.

MINIT 3.10 Hal-hal Lain

(1) Audit Pemantauan Sistem Pengurusan Keselamatan Maklumat (ISMS) oleh Pihak SIRIM

Mesyuarat mengambil maklum bahawa Audit Pemantauan ISMS oleh pihak SIRIM akan dijalankan pada 29 dan 30 Januari 2015.

(Makluman: Semua)

KESIMPULAN KESELURUHAN

Mesyuarat selepas menerima dan mengkaji semula semua laporan mendapati bahawa polisi Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia (UPM) adalah sesuai untuk menjamin kesinambungan urusan ICT di UPM dengan meminimumkan kesan insiden keselamatan ICT. Pelaksanaan ISMS bagi tempoh Oktober 2013 hingga September 2014 adalah mencukupi dan berkesan. Walau bagaimanapun, tindakan pembetulan dan cadangan penambahbaikan telah dikenalpasti dan dipersetujui sebagai tindakan penambahbaikan berterusan kepada Sistem Pengurusan Keselamatan Maklumat UPM.

Secara keseluruhannya mendapati bahawa Universiti Putra Malaysia (UPM) berupaya mengekalkan pensijilan Sistem Pengurusan Keselamatan Maklumat (ISMS) yang kini dilaksanakan di bawah piawaian baharu ISO/IEC 27001:2013.

Pensijilan ISMS di UPM akan menjamin keselamatan maklumat yang merangkumi aspek kerahsiaan, integriti, dan ketersediaan sejajar dengan objektif keselamatan ICT sektor awam.

PENANGGUHAN MESYUARAT

Mesyuarat ditangguhkan pada jam 4.30 petang dengan ucapan terima kasih kepada ahli yang hadir.

Lampiran A

SENARAI KEHADIRAN

TAJUK: **MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) UNIVERSITI PUTRA MALAYSIA KALI KETIGA [BIL. 1/2014]**

TARIKH: **1 DISEMBER 2014**

TEMPAT: **DEWAN SENAT, BANGUNAN PENTADBIRAN, UPM**

Hadir		
1.	YBhg. Prof. Datuk Dr. Mohd Fauzi Haji Ramlan	Naib Canselor – Pengerusi
2.	YBhg.Prof. Datuk Dr. Mad Nasir Shamsudin	Timbalan Naib Canselor (Akademik dan Antarabangsa)
3.	YBhg. Prof. Dr. –Ing. Ir. Renuganth Varatharajoo	Timbalan Naib Canselor (Jaringan Industri dan Masyarakat)
4.	Dato' Wan Azman Wan Omar	Pendaftar
5.	Encik Zulkiflee Othman	Bursar
6.	Encik Amir Hussain Md. Ishak	Ketua Pustakawan
7.	YBhg. Prof. Datin Paduka Dr. Aini Ideris	Pengarah, Pejabat Perancangan Strategik dan Korporat
8.	Prof. Madya Dr. Ramdzani Abdullah	Pengerusi, Jemaah Dekan UPM
9.	Dr. Mohd. Rafee Baharudin	Pengarah, Pejabat Pengurusan keselamatan dan Kesihatan Pekerjaan
10.	Prof. Dr. Abdul Shukor Juraimi	Dekan, Fakulti Pertanian
11.	Prof. Madya Dr. Fatimah Sidi	Pengarah, Pusat Pembangunan Maklumat dan Komunikasi
12.	Prof. Dr. Abdul Rahman Omar	Pengerusi, Jemaah Pengarah Institut
13.	Prof. Dr. Mohd Roslan Sulaiman	Pengerusi, Jemaah Pengetua
14.	Dr. Yahya Abu Ahmad	Ketua, Pusat Kesihatan Universiti

15.	Puan Siti Rozana Supian	Ketua Bahagian Pengurusan Sumber Manusia, Pejabat Pendaftar
16.	Puan Noorizai Hj. Mohamad Noor	Ketua Bahagian Pengurusan Kualiti, Pejabat Pendaftar
17.	Tuan Hj. Hashim Md. Shari	Ketua Pentadbiran Hal Ehwal Pelajar dan Alumni, Pejabat Timbalan Naib Canselor (Hal Ehwal Pelajar dan Alumni)
18.	Tuan Hj. Rosdi Wah	Ketua Pentadbiran Akademik dan Antarabangsa, Pejabat Timbalan Naib Canselor (Akademik dan Antarabangsa)
19.	Encik Rosmi Othman	Timbalan Pengarah (Pengurusan Strategik & Sokongan Pengguna), Pusat Pembangunan Maklumat dan Komunikasi
20.	Encik Mohd Faizal Daud	Timbalan Pengarah (Perkhidmatan Infrastruktur ICT), Pusat Pembangunan Maklumat dan Komunikasi (iDEC) – Setiausaha

Tidak hadir (Dengan Kenyataan)		
1.	YBhg. Prof. Dr. Mohd Azmi Mohd Lila	Timbalan Naib Canselor (Penyelidikan dan Inovasi)
2.	YBhg. Prof. Dato' Dr. Mohammad Shatar Sabran	Timbalan Naib Canselor (Hal Ehwal Pelajar dan Alumni)
3.	Prof. Madya Dr. Rozanah Abdul Rahman	Penasihat Undang-Undang, Pejabat Penasihat Undang-undang
4.	Encik Ahmad Razie Abu Bakar	Pengarah Keselamatan, Bahagian Keselamatan Universiti

Turut Hadir		
1.	Puan Salinah Junid	Pusat Pembangunan Maklumat dan Komunikasi
2.	Puan Hamidah Meseran	Pusat Pembangunan Maklumat dan Komunikasi

3.	Encik Krishnan Mariappan	Pusat Pembangunan Maklumat dan Komunikasi
4.	Encik Shahril Iskandar Amir	Pusat Pembangunan Maklumat dan Komunikasi
5.	Tuan Hj. Mohamad Farid Harun	Pusat Pembangunan Maklumat dan Komunikasi
6.	Encik Ahmad Faisal Abdul Ghafar	Pusat Pembangunan Maklumat dan Komunikasi
7.	Puan Nurul Fatihah Md Marham	Pusat Pembangunan Maklumat dan Komunikasi
8.	Pn. Noraihan Noordin	Bahagian Pengurusan Kualiti, Pejabat Pendaftar

LAMPIRAN

MINIT MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) UNIVERSITI PUTRA MALAYSIA KALI KETIGA (BIL. 1/2014)

Lampiran 1

PRESTASI PROSES DAN KEPATUHAN PRODUK/PERKHIDMATAN

BIL	OBJEKTIF KESELAMATAN MAKLUMAT 2014	SASARAN	PENCAPAIAN	
			2013	2014
1	Memastikan penilaian risiko dan pelan pemulihan risiko dilaksanakan apabila berlaku perubahan kepada dasar ISMS atau inventori yang termaktub dalam skop.	Apabila berlaku perubahan	2 kali penilaian telah di laksanakan	Sekali penilaian telah dilaksanakan
2	Menjalankan ujian kesinambungan perkhidmatan ICT sekurang-kurangnya 1 kali setahun.	Sekali setahun	Dilaksanakan Nov 2013	Akan dilaksanakan 10 Disember 2014
3	Memastikan 80% staf telah diberi taklimat kesedaran/pelaksanaan mengenai ISMS dalam tempoh 5 tahun.	80% untuk 5 tahun	-	Merupakan Objektif Baharu ISMS selepas perubahan piawaian 2013 dan akan dinilai pada 2016
4	Memastikan insiden ICT tidak melebihi 10 kali pada setiap tahun.	< 10 Kali	4 insiden telah didaftar dan diambil tindakan sewajarnya: 1.http://eng.upm.edu.my/upmnksu/ 2.http://www.pic.upm.edu.my/ 3.http://www.pkkssaas.upm.edu.my/ 4. http://www.devel.upm.edu.my/	2 insiden yang didaftarkan dan telah diambil tindakan sewajarnya: 1.spjonline.upm.edu.my 2.recent.upm.edu.my
5	Memastikan gangguan kepada ketersediaan rangkaian (Internet dan Intranet) tidak melebihi 10% setiap tahun.	10%	Peratusan pencapain ketersediaan rangkaian untuk internet dan intranet adalah 97.15%	Peratus pencapaian ketersediaan rangkaian bagi tempoh Januari - September: Intranet - 100% Internet - 99.88%

6	Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam.	Pemulihan bekalan elektrik 24 jam	-	Merupakan Objektif Baharu ISMS selepas perubahan piawaian 2013 dan akan dinilai pada 2015 dengan bantuan maklumat daripada pihak PPPA
7	Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden.	Pemulihan data 48 jam	-	Setakat Oktober 2014 tiada insiden yang tidak dapat dipulihkan.

Lampiran 2

KETAKAKURAN DAN TINDAKAN PEMBETULAN

BIL	PROSES PERKHIDMATAN YANG TIDAK PATUH/CACAT	PUNCA PENYEBAB BERLAKU KETIDAKPATUHAN/KECACATAN	TINDAKAN PEMBETULAN	TARIKH TINDAKAN	TANGGUNG JAWAB	CATATAN
1	Tidak mengenalpasti Sistem Maklumat Pelajar Siswazah (iGIMS) sebagai salah satu Sistem aplikasi Utama Universiti	Fasiliti Sistem Maklumat Pelajar Siswazah kurang mantap dari aspek kemudahan pemulihan bencana	Memantapkan Sistem Maklumat Pelajar Siswazah dengan kemudahan *Server,* Storan dan Sistem *Backup* Data Pemulihan Bencana	Disember 2013	iDEC	Telah dilaksanakan
2	Tidak membuat kawalan ke atas elemen penilaian risiko, iaitu bangunan yang menempatkan Pusat Data Utama	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. Keluasan Pusat Data sekarang yang terhad (penuh) sudah tidak mampu menampung peningkatan	a. Menjalankan proses pemeriksaan bangunan layak diduduki b. Keperluan lokasi atau Bangunan Baru Pusat Data (Permohonan Pusat Data Baru telah dikemukakan dalam RMK Ke-11) c. Keperluan Pusat Data yang lebih besar (Permohonan Pusat Data Baru telah dikemukakan dalam RMK Ke-11).	a. Mac 2015 Perkara b. & c. Bergantung kepada kelulusan bajet RMK Ke-11.	iDEC	Permohonan peruntukan telah dikemukakan

		pertambahan *Server* universti yang perlu diurus dimasa hadapan.				

Lampiran 3

PERUBAHAN YANG MEMBERI KESAN KEPADA SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

BIL	PERUBAHAN YANG MEMBERI KESAN	KESAN	STATUS	
			TELAH DILAKSANAKAN	SEDANG DILAKSANAKAN
1	**Penaiktarafan Infrastruktur Pusat Data dilaksanakan pada Januari 2013**	a) Menjamin kesinambungan perkhidmatan / operasi Pusat Data walaupun semasa berlaku kegagalan bekalan elektrik utama. b) Menjamin ketersediaan perkhidmatan aplikasi ICT Universiti kepada warga kampus. c) Meningkatkan kebolehpercayaan kepada perkhidmatan ICT Universiti. d) Menjayakan Matlamat 5, Pelan Strategik UPM 2014-2020: Mempertingkat Kualiti Tadbir Urus, menerusi Objektif Strategik 4: Meningkatkan Infrastruktur Perkhidmatan Teknologi Maklumat dan Komunikasi.	√	
	a) Penaiktarafan Generator Elektrik Tunggu Sedia (Genset) Pusat Data daripada kemampuan 200kVA kepada 400kVA, yang juga berdasarkan justifikasi berikut: i. Keperluan penggantian *Genset* yang telah berusia 20 tahun (selalu mengalami kerosakan); dan ii. Membolehkan sistem pendingin udara Pusat Data beroperasi pada masa kecemasan (kegagalan sistem elektrik utama)			
	b) Penaiktarafan UPS Pusat Data kepada reka bentuk ***Centralised UPS*** yang berkeupayaan tinggi dan mudah diselenggara.			
	c) Penaiktarafan ***Power Distribution System*** yang menyambungkan sistem elektrik ke setiap *server*, dengan reka bentuk sistem pemutus litar elektrik di setiap *rack* bagi memastikan gangguan elektrik sesebuah *server* tidak mengganggu operasi *server* lain.			

2	**Penaiktarafan *Server* Sistem Aplikasi Utama Universiti** Penaiktarafan kemudahan Infrastruktur *Server* Sistem Aplikasi Utama dan pelaksanaan: i) HRMS Fasa 1: JUN 2013; ii) HRMS Fasa 1: SEPTEMBER 2013; iii) Kewangan: JUN 2013; dan iv) WEB, SMP dan IGIMS: SEPTEMBER 2013.	Meningkatkan prestasi capaian / kecekapan / efisyen perkhidmatan ICT Universiti yang semakin berkembang dengan pertambahan fungsi serta pengguna.	√	
3	**Mengadakan *Server* Pemulihan Bencana Universiti pada Disember 2013** Membangunkan Kemudahan Infrastruktur *Server* Pemulihan Bencana untuk Sistem Aplikasi Utama Universiti di Pusat Data Bencana (DRC).	Menjamin kesinambungan perkhidmatan ICT Universiti khususnya sistem aplikasi utama ketika berlaku kegagalan *Server* Utama berfungsi atau bencana kepada Pusat Data Utama.	√	
4	**Mengadakan Storan Khas Mengarkib Data Universiti pada Disember 2013** Membangunkan Storan Khas (berkapasiti: 140TB) untuk mengarkib Pangkalan Data penting Universiti dengan selamat setiap hari.	a) Memastikan semua pangkalan data disimpan dengan lebih sistematik dan terurus serta selamat; b) Menjamin dan meningkatkan integriti pangkalan data Universiti; dan c) Memastikan ketersediaan data / maklumat aplikasi utama agar boleh dirujuk dengan cepat, sekiranya berlaku bencana kepada Pangkalan Data Utama.	√	

5	**Penaiktarafan Bilik Persedian Server (Stagging) pada Julai 2014** Penaiktarafan Bilik Persediaan *Server (Stagging Room)* Pusat Data Utama.	a) Memastikan perkakasan yang dibawa masuk ke Pusat Data dalam keadaan selamat dan teruji; b) Mengurangkan ancaman kepada *production server* ketika kerja-kerja konfigurasi *server* baharu dilaksanakan; dan c) Mengurangkan akses pihak pembekal ke dalam Pusat Data.	√	

Lampiran 4

LAPORAN RINGKAS HASIL PENILAIAN RISIKO ISMS TAHUN 2014

BIL	PERKARA	TINDAKAN KAWALAN	TAHAP RISIKO		PELAN PEMULIHAN RISIKO
			SEBELUM	SELEPAS	
1	Mengurangkan tahap risiko aset: a) Sistem Pengurusan Sumber Manusia (HRMS) b) Sistem Pengurusan Kewangan (KEW) c) Sistem Maklumat Pelajar Pra-Siswazah (SMP) d) Sistem Web Utama Universiti (WEB) e) Sistem Maklumat Pengajian Siswazah (IGIMS)	1. Penaiktarafan Infrastruktur *Server* & Storan Utama *(production)*. 2. Membangunkan Infrastruktur Server & Storan Pemulihan Bencana (DR)	H H H H H	M M M M M	a) Pelaksanaan pemantauan berjadual; dan b) Ujian Simulasi Pemulihan Bencana dijalankan setahun sekali.
2	Infrastruktur Pengurusan Pusat Data	Penaiktarafan Infrastruktur Pusat Data: a) Generator Elektrik b) *Uninteruption Power Suply (UPS)* c) *Power Distribution System* d) Bilik Persediaan *Server (Stagging Room)*	H	M	Pelaksanaan Pemantauan Berjadual oleh pihak PPPA serta menwujudkan Objektif ISMS khas memantau ketersedian sistem elektrik

3	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.	Penyediaan Pusat Data Kedua (*Disaster Recovery Center*) di lokasi iDEC Epsilon UPM MTDC.	H	H	Permohonan Bangunan serta Pusat Data Baharu dalam RM Ke-11

Lampiran 5

PELUANG PENAMBAHBAIKAN

BIL.	KETERANGAN OFI	PELAKSANAAN TINDAKAN	TARIKH TINDAKAN	CATATAN
1	Memastikan Pentadbir Sistem boleh mencapai sistem aplikasi dengan selamat	Membangunkan sistem capaian VPN	2015	Akan dicadangkan dalam tindakan di Plan Strategik IDEC 2015 yang akan di adakan pada 6 Disember 2014
2	Memantapkan pemantauan setiap capaian pengguna ke sistem aplikasi universiti di Pusat Data	Membangunkan sistem log berpusat server di Pusat Data	2015	Akan dicadangkan dalam tindakan di Plan Strategik IDEC 2015 yang akan di adakan pada 6 Disember 2014
3	Meningkatkan tahap keselamatan (mengurangkan risiko gangguan) setiap server aplikasi yang dicapai oleh pengguna	Membangunkan sistem pertahanan rangkaian di Pusat Data	2015	Akan dicadangkan dalam tindakan di Plan Strategik IDEC 2015 yang akan di adakan pada 6 Disember 2014
4	Memantapkan keberkesanan tugas dan tanggungjawab Pegawai Teknologi Maklumat	Penstrukturan Semula IDEC 2015 berkonsepkan perkhidmatan hibrid	2015	Dalam proses Penyediaan Kertas Cadangan Kepada Jawatankuasa Pengurusan Universiti (JPU) pada Disember 2014
5	Penyelarasan ISO berpusat di UPM	Pemusatan tanggungjawab Bahagian Pengurusan Kualiti	2015	Cadangan pelaksanaan bermula 2015

AGENDA 2.0

TINDAKAN SUSULAN MESYUARAT LEPAS

TINDAKAN SUSULAN
MINIT MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) ISO/IEC 27001:2013
UNIVERSITI PUTRA MALAYSIA
KALI KETIGA (BIL.1/2014)

BIL	MINIT	PERINCIAN TINDAKAN	TANGGUNGJAWAB/ TINDAKAN	STATUS PELAKSANAAN/ PENCAPAIAN
1.	3.3.2	Audit Dalaman d) Kesemua rekod ketakakuran telah diambil tindakan dengan 11 daripadanya telah ditutup dan dua (2) belum ditutup kerana memerlukan masa yang lebih lama untuk menentukan keberkesanan tindakan penutupan yang diambil. Tindakan ke atas semua cadangan penambahbaikan sedang diambil tindakan namun ada diantaranya memerlukan peruntukan kewangan untuk dilaksanakan.	TWP ISMS	Semua rekod ketakakuran dan peluang penambahbaikan telah diambil tindakan
2.	3.5	**Prestasi Proses dan Kepatuhan Produk/perkhidmatan** a) Laporan prestasi proses diukur berdasarkan pencapaian objektif keselamatan maklumat pada tahun 2013 dan 2014. Terdapat perbezaan objektif keselamatan maklumat berikutan penggunaan piawaian MS ISO/IEC 27001:2007 pada tahun 2013 dan piawaian ISO/IEC 27001:2013 bagi tahun 2014 yang hanya akan dibuat pengukuran dalam tahun 2015.	TWP ISMS	Laporan pencapaian Objektif Keselamatan Maklumat bagi tahun 2015 untuk tempoh Januari hingga Jun telah dianalisis seperti **Lampiran A**.

BIL	MINIT	PERINCIAN TINDAKAN	TANGGUNGJAWAB/ TINDAKAN	STATUS PELAKSANAAN/ PENCAPAIAN
				Kesemua enam (6) objektif telah dicapai kecuali objektif 3: Memastikan 80% staf telah diberi taklimat kesedaran dan pelaksanaan mengenai ISMS dalam tempoh 5 tahun. Sehingga November 2015, lebih kurang 10% staf telah menghadiri beberapa siri bengkel, latihan, taklimat. **Walau bagaimanapun, keseluruhan objektif telah dipinda mengikut skop baharu.**
3.	3.9	**Peluang Penambahbaikan** Mesyuarat mengambil maklum lima (5) peluang penambahbaikan yang telah dikenalpasti di dalam pelaksanaan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2013	TWP ISMS	Lima (5) peluang penambahbaikan yang dikenal pasti telah dilaksanakan seperti di **Lampiran B**.

LAPORAN PENCAPAIAN OBJEKTIF KESELAMATAN MAKLUMAT
JANUARI HINGGA JUN 2015

BIL	OBJEKTIF KESELAMATAN MAKLUMAT	SASARAN	PENCAPAIAN 2015
1.	Memastikan penilaian risiko dan pelan pemulihan risiko dilaksanakan apabila berlaku perubahan kepada dasar ISMS atau inventori yang termaktub dalam skop	Apabila berlaku perubahan	Sekali penilaian telah dilaksanakan : Ogos 2015
2.	Menjalankan ujian kesinambungan perkhidmatan ICT sekurang-kurangnya 1 kali setahun	Sekali setahun	DRP ICT telah dilaksanakan pada Oktober 2015
3.	Memastikan 80% staf telah diberi taklimat kesedaran/pelaksanaan mengenai ISMS dalam tempoh 5 tahun	80% untuk 5 tahun	Sehingga November 2015, lebih kurang 10% staf telah menghadiri siri bengkel, latihan dan taklimat
4.	Memastikan insiden ICT tidak melebihi 10 kali pada setiap tahun	< 10 Kali	2 insiden yang didaftarkan dan telah diambil tindakan sewajarnya: 1.www.inkubasi.upm.edu.my 2.www.smb.upm.edu.my
5.	Memastikan gangguan kepada ketersediaan rangkaian (Internet dan Intranet) tidak melebihi 10% setiap tahun	10%	Peratus pencapaian ketersediaan rangkaian bagi tempoh Januari - September 2015: Intranet - 100% Internet - 100%
6.	Memastikan gangguan bekalan kuasa di Pusat Data dipulihkan dalam tempoh 24 jam	99.75% (Tier II Standard)	100% (Kesemua kegagalan sumber bekalan elektrik utama diambil alih oleh Genset)
7.	Memastikan 100% data dipulihkan dalam tempoh 48 jam selepas insiden	100%	100% (Kesemua kegagalan infrastruktur utama akan diambil alih oleh infrastruktur pemulihan bencana di Pusat Pemulihan Bencana)

PELUANG PENAMBAHBAIKAN

BIL.	KETERANGAN OFI	TINDAKAN	PELAKSANAAN TINDAKAN	CATATAN
1.	Membangunkan sistem capaian VPN untuk membolehkan Pentadbir Sistem mencapai sistem aplikasi dengan selamat	Membangunkan sistem capaian VPN	Membangunkan sistem capaian VPN secara berfasa. Fasa pertama VPN SMP telah dilaksanakan	Selesai
2.	Memantapkan pemantauan setiap capaian pengguna ke sistem aplikasi universiti di Pusat Data	Membangunkan sistem log berpusat server di Pusat Data	Telah menggunapakai Garis Panduan Kawalan Capaian ke Sistem di Pusat Data	Selesai
3.	Meningkatkan tahap keselamatan (mengurangkan risiko gangguan) setiap server aplikasi yang dicapai oleh pengguna	Membangunkan sistem pertahanan rangkaian di Pusat Data	Telah melaksanakan sistem pertahanan IPS di parameter gateway Pusat Data (26 Mac 2015)	Selesai
4.	Memantapkan keberkesanan tugas dan tanggungjawab Pegawai Teknologi Maklumat	Penstrukturan Semula IDEC 2015 berkonsepkan perkhidmatan hibrid	Telah dilaksanakan bermula Januari 2015	Selesai
5.	Penyelarasan ISO berpusat di UPM	Pemusatan tanggungjawab Bahagian Pengurusan Kualiti	Telah dilaksanakan bermula Januari 2015	Selesai

AGENDA 3.0

PERUBAHAN ISU DALAMAN DAN ISU LUARAN

PERUBAHAN ISU DALAMAN DAN LUARAN YANG BERKAITAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)

PELAKSANAAN 2012-2014		PELAKSANAAN 2015	
DALAM	**LUAR**	**DALAM**	**LUAR**
Pembudayaan pengurusan keselamatan maklumat tertumpu kepada staf Pusat Pembangunan Komunikasi dan Maklumat (iDEC) khusus untuk perkhidmatan ICT yang melibatkan pengendalian data dan maklumat digital. Tanggungjawab dan proses keselamatan maklumat hanya tertumpu kepada proses perkhidmatan ICT	i. Arahan MAMPU untuk agensi melaksanakan ISMS sebelum tahun 2013. ii. Pembudayaan amalan keselamatan maklumat dalam kalangan agensi kerajaan masih tidak jelas.	**Pembudayaan** pengurusan keselamatan maklumat setiap warga Universiti Putra Malaysia i. Kurang kefahaman dalam kalangan staf ii. Ketidakjelasan tanggungjawab dan proses iii. Tahap kebolehpercayaan, integriti dan ketersediaan data iv. Kekangan sumber manusia dan kewangan v. Infrastruktur tidak menyokong proses	i. Perubahan Dasar Kerajaan ii. Perkembangan teknologi dan inovasi yang pantas iii. Ekonomi tidak menentu iv. Ancaman ekologi v. Ekspektasi pelanggan terlalu tinggi vi. Kriteria penarafan yang berubah vii. Gangguan media sosial iii. Masalah komunikasi
<u>Kesimpulan :</u> Pelaksanaan ISMS di UPM (2012-2014) lebih tertumpu kepada pengurusan data dan maklumat digital yang diurus oleh iDEC di Pusat Data Universiti.		<u>Kesimpulan:</u> Pelaksanaan ISMS di UPM (2015 dan seterusnya) di mana Universiti beriltizam ke arah pelaksanaan menyeluruh kepada proses utama universiti yang melibatkan pengajaran dan pembelajaran, penyelidikan dan perkhidmatan korporat universiti.	

<table>
<tr><th colspan="2">PELAKSANAAN 2012-2014</th><th colspan="2">PELAKSANAAN 2015</th></tr>
<tr><th>DALAM</th><th>LUAR</th><th>DALAM</th><th>LUAR</th></tr>
<tr><td colspan="2">Skop 2012 hingga kini adalah;

Perkhidmatan operasi Pusat Data dan Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah yang terlibat dalam skop pensijilan ISMS merangkumi aktiviti berikut:

a. Pelaksanaan operasi Pusat Data;
b. Penyelenggaraan fasiliti Pusat Data;
c. Pemantauan operasi Pusat Data;
d. Penyenggaraan perkhidmatan operasi server di Pusat Data;
e. Pemantauan capaian sistem di Pusat Data;
f. Kawalan keselamatan di Pusat Data; dan
g. Tindakan kecemasan di Pusat Data.</td><td colspan="2">Walau bagaimanapun tumpuan kepada proses pengurusan pendaftaran pelajar baharu sebagai langkah awal untuk membudayakan amalan pengurusan keselamatan data kepada semua warga universiti.

Cadangan skop baharu adalah seperti berikut;

Pengurusan Maklumat:

1. Pelajar;
2. Pengajaran;
3. Penyelidikan; dan
4. Perkhidmatan korporat.</td></tr>
<tr><td colspan="4">TUMPUAN SKOP 2015

Skop pensijilan ISMS UPM adalah seperti berikut:
1. Sistem Pengurusan Keselamatan Maklumat hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Maklumat Pelajar
2. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah
3. Sistem Pengurusan Keselamatan Maklumat untuk Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah</td></tr>
</table>

AGENDA 4.0

MAKLUM BALAS PRESTASI KESELAMATAN MAKLUMAT

AGENDA 4.1 KETAKAKURAN DAN TINDAKAN PEMBETULAN

AGENDA 4.2 PEMANTAUAN DAN PENGUKURAN

4.2.1 OBJEKTIF ISMS

4.2.2 PELAKSANAAN KAWALAN DI PELAN PEMULIHAN RISIKO

KETAKAKURAN DAN TINDAKAN PEMBETULAN

BIL.	PROSES PERKHIDMATAN YANG TIDAK PATUH	PUNCA PENYEBAB BERLAKU KETAKAKURAN	TINDAKAN PEMBETULAN	TARIKH TINDAKAN	TANGGUNGJAWAB
1.	**Kawalan Akses ke Sistem Maklumat Pelajar (SMP) – Modul Kolej :-**				
	i. Perkongsian ID Pengguna	i. ID pengguna boleh melaksanakan *multiple* akses.	i. Memastikan setiap ID pengguna adalah *single* akses.	7 Disember 2015	Bahagian Kemasukan dan Pusat Pembangunan Maklumat dan Komunikasi
	ii. Penggunaan ID staf yang tamat perkhidmatan	ii. ID SMP belum menggunakan UPM-ID yang membolehkan mengesan staf yang berhenti secara dalam talian.	ii. Melaksanakan penggunaan UPM ID sebagai ID Pengguna SMP	Disember 2016	Bahagian Urus Tadbir Akademik dan Pusat Pembangunan Maklumat dan Komunikasi

BIL.	PROSES PERKHIDMATAN YANG TIDAK PATUH	PUNCA PENYEBAB BERLAKU KETAKAKURAN	TINDAKAN PEMBETULAN	TARIKH TINDAKAN	TANGGUNGJAWAB
	iii. Akses ke sistem oleh pelajar	iii. Penggunaan perkhidmatan pelajar tidak diurus secara teratur.	iii. Jika perkhidmatan pelajar masih diperlukan, ianya hendaklah diurus secara rasmi seperti berikut: a. Surat lantikan b. Aku janji Akauntabiliti c. ID khas untuk kegunaan semasa hari pendaftaran sahaja	iii. Kemasukan sesi 2016/2017	iii. Bahagian Kemasukan, Bahagian Hal Ehwal Pelajar dan Kolej
2.	Tidak memenuhi elemen penilaian risiko iaitu bangunan melibatkan pusat data utama	i. Kedudukan pusat data kini berada di aras bawah dan berisiko tinggi dan tidak memenuhi Garis Panduan Pembangunan Pusat Data oleh pihak *Uptime Institute.*	Pembangunan Pusat Data baharu melalui peruntukan Rancangan Malaysia Ke-11. Walau bagaimanapun peruntukan ruang pusat data (4000 kaki persegi, di tingkat 1) memerlukan pertimbangan universiti.	2016/2017	Pusat Pembangunan Maklumat dan Komunikasi

BIL.	PROSES PERKHIDMATAN YANG TIDAK PATUH	PUNCA PENYEBAB BERLAKU KETAKAKURAN	TINDAKAN PEMBETULAN	TARIKH TINDAKAN	TANGGUNGJAWAB
		ii. Keluasan pusat data yang terhad dan sudah tidak mampu menampung peningkatan keperluan *server* universiti			

LAPORAN PENCAPAIAN OBJEKTIF
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT 2015

BIL.	OBJEKTIF	PETUNJUK PRESTASI	PENCAPAIAN	CATATAN
1.	Memastikan semakan penilaian risiko dan pelan pemulihan risiko dilaksanakan	sekurang-kurangnya sekali setahun	Ogos 2015 telah melaksana semakan penilaian risiko	**Rujuk Lampiran A** (Ringkasan Laporan Penilaian Risiko) Pembentangan terperinci pada Agenda 7.0 (Kertas 10)
2.	Menjalankan ujian simulasi pelan pemulihan bencana ICT	sekurang-kurangnya 1 kali setahun;	23 Oktober 2015 telah jalankan ujian simulasi pelan pemulihan bencana ICT	**Rujuk Lampiran B** (Laporan Ujian Simulasi Pemulihan Bencana ICT)
3.	Memastikan sokongan ICT (rangkaian, sistem aplikasi dan pangkalan data) terhadap proses pendaftaran pelajar baharu bebas dari gangguan setiap semester;	95%	Akan diukur Sesi Kemasukan 2016/2017	Maklumat log aktiviti sokongan ICT daripada pihak Pembangunan Maklumat dan Komunikasi (iDEC) menunjukkan tiada gangguan sepanjang dua (2) hari pendaftaran
4.	Memastikan pelajar yang berdaftar adalah pelajar yang mendapat tawaran; dan	100%	Akan diukur Sesi Kemasukan 2016/2017	
5.	Memastikan borang permohonan kad pelajar yang diterima diisi dengan lengkap.	100%	Akan diukur Sesi Kemasukan 2016/2017	

ANALISIS PENILAIAN RISIKO 2015

	HARDWARE	SOFTWARE	PEOPLE	DATA & INFORMATION	SERVICE (SUPPORTING)	SERVICE (ACCESSIBILITY)	RISK COUNT
LOW	218	112	353	41	106	35	865
MEDIUM	130	0	50	16	23	41	260
HIGH	1	0	0	0	0	11	12
TOTAL	349	112	403	57	129	87	1137

PERKARA	JUMLAH	PERATUS
RISK	**1137**	**-**
HIGH RISK	**12**	**1%**
MEDIUM RISK	**260**	**22.9%**
LOW RISK	**865**	**76.1%**

Projek : Pengesahan Pendaftaran Pelajar Baharu (Kolej)

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	0	0	0
Software	34	0	0	34
People	51	0	0	51
Data & Information	0	0	0	0
Service (supporting)	51	0	0	51
Service (Accessibility)	34	0	0	34
Total	170	0	0	170

Projek : Pembayaran Yuran Pelajar Baharu Prasiswazah (Pejabat Bursar)

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	1	1	2
Software	0	0	0	0
People	0	29	0	29
Data & Information	0	2	0	2
Service (supporting)	0	1	0	1
Service (Accessibility)	0	0	0	0
Total	0	33	1	34

Projek : Kad Pelajar Baharu Prasiswazah (Keselamatan)

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	0	0	0
Software	4	0	0	4
People	18	0	0	18
Data & Information	1	0	0	1
Service (supporting)	1	0	0	1
Service (Accessibility)	1	0	0	1
Total	25	0	0	25

Projek : Pengesahan Laporan Pemeriksaan Kesihatan Pelajar Baharu Prasiswazah (PKU)

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	0	0	0
Software	0	0	0	0
People	228	0	0	228
Data & Information	0	0	0	0
Service (supporting)	8	0	0	8
Service (Accessibility)	0	0	0	0
Total	236	0	0	236

Projek : Sistem Aplikasi Kewangan

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	8	32	0	40
Software	0	0	0	0
People	6	3	0	9
Data & Information	0	0	0	0
Service (supporting)	0	0	0	0
Service (Accessibility)	0	0	0	0
Total	14	35	0	49

Projek: Sistem Aplikasi Maklumat Pelajar Prasiswazah

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	210	0	0	210
Software	0	0	0	0
People	15	0	0	15
Data & Information	0	0	0	0
Service (supporting)	0	0	0	0
Service (Accessibility)	0	0	0	0
Total	225	0	0	225

Projek : Sistem Sokongan (Pusat Data, Rangkaian, Keselamatan)

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	57	0	57
Software	74	0	0	74
People	23	12	0	35
Data & Information	40	7	0	47
Service (supporting)	46	22	0	68
Service (Accessibility)	0	41	11	52
Total	183	13	11	333

Projek : Sistem Pangkalan Data

Asset Group	Risk Value			Risk Count
	Low	Medium	High	
Hadrware	0	40	0	40
Software	0	0	0	0
People	12	6	0	18
Data & Information	0	7	0	7
Service (supporting)	0	0	0	0
Service (Accessibility)	0	0	0	0
Total	12	53	0	65

LAPORAN UJIAN SIMULASI PEMULIHAN BENCANA ICT

1. PENGENALAN

Perancangan dan Pengujian Pelan Pemulihan Bencana ICT (DRP ICT) adalah sangat penting dalam memastikan kelancaran kesinambungan perkhidmatan ICT di UPM. Pelan pemulihan bencana yang telah digubal perlu diuji bagi memastikan keberkesanan proses pemulihan yang telah dirancang.

Simulasi atau pengujian DRP ICT bertujuan memastikan Pengurusan Pemulihan Bencana dilaksanakan seperti yang termaktub dalam Pelan apabila berlaku gangguan atau bencana.

Ujian pemulihan bencana ini fokus kepada gangguan teknikal ICT iaitu gangguan elektrik di Pusat Data Universiti Putra Malaysia yang menyebabkan gangguan infrastruktur dan infostruktur ICT sistem aplikasi kritikal yang terlibat dalam skop ISMS seperti berikut:

a. SISTEM APLIKASI PELAJAR
    i. Sistem Maklumat pelajar (undergraduate)
    ii. Sistem iGIMS (postgraduate)
b. SISTEM APLIKASI SUMBER MANUSIA
c. SISTEM APLIKASI KEWANGAN
    i. SAS
    ii. FAMS
    iii. SAGA
d. SISTEM LAMAN WEB UTAMA UNIVERSITI.

Aktiviti Simulasi DRP ICT berlaku pada 31 JULAI 2015 dan 23 OKTOBER 2015 di Pusat Data iDEC Beta dan Pusat Data iDEC Epsilon Universiti Putra Malaysia.

2. OBJEKTIF

Objektif melaksana simulasi adalah untuk:

a) Melatih dan meningkatkan pengetahuan ahli-ahli pasukan DRP ICT
b) Melatih dan menguji keupayaan kesemua Pasukan DRP ICT dalam melaksanakan semua tugas-tugas yang ditetapkan dalam pelan DRP ICT di bawah keadaan gangguan elektrik (power failure);
c) Menambahbaik Pelan Pemulihan Bencana (DRP) ICT UPM
d) Melihat keberkesanan prosedur pemulihan Sistem Aplikasi yang terlibat dalam simulasi.

3. SKOP SIMULASI DAN PERSEKITARAN

Untuk Pengujian simulasi pemulihan bencana ini, hanya sistem aplikasi kritikal terpilih ditakrifkan oleh Pentadbir Sistem UPM yang akan dipulihkan di Tapak Pemulihan Bencana iaitu Pusat Data DR iDEC Epsilon.

Jadual 1 di bawah menerangkan spesifikasi teknikal Utiliti di Pusat Data DR iDEC Epsilon.

JADUAL 1: SPESIFIKASI TEKNIKAL UTILITI PUSAT DATA DR iDEC EPSILON

PUSAT DATA UTAMA	PUSAT PEMULIHAN BENCANA (DRC)
Lokasi : iDEC BETA	Lokasi : iDEC EPSILON
Infrastruktur Utama	
1. Main Server Room 2. Data Storage Infrastructure 3. Racking enclosure 4. Raised floor system 5. Networking infrastructure 6. Backup system infrastructure 7. Application system infrastructure	1. 4 x Server Rooms (Cirrus, Stratus, Cumulus & Nimbus) 2. 60 x 42U perforated racks (Dec 2012) 3. Data Storage Infrastructure 4. Raised floor system 5. Networking infrastructure 6. Application system infrastructure
Sistem Keselamatan dan Persekitaran	
1. 8 x E-jari Access Control System 2. 16 x CCTV Camera 3. Fire Suppression System (Argonite	1. FM200 Fire Suppression System 2. Environmental Monitoring with 8 x Temp/Humidity Sensors (Dec 2012)

PUSAT DATA UTAMA	PUSAT PEMULIHAN BENCANA (DRC)
System)	3. 26 x CCTV Camera 4. 9 x Biometric Access Reader
Sistem Elektrik dan Pendingin Udara	
1. Electrical power distribution system 300A 2. Emergency power system (Generator) 200kVA 3. 3 x DB-Aire Air Precision Cooling System	1. 400A Incoming Electrical Supply 2. 2 x 80kVA Centralised UPS 3. 300kVA Standby Genset 4. 3 x 74kW Precision Cooling Units 5. 6 x 33kW Precision Cooling Units
Datacenter management facilities	
1. Console Room 2. Staging Room 3. Crisis room 4. Staff workstation	1. Staging Room 2. Network Operation Room 3. Telco Room 4. Crisis Room 5. Guest Workstation Room

Skop simulasi pengujian DRP ICT ini adalah berdasarkan kepada kemampuan dan ketersediaan infrastruktur ICT server dan rangkaian yang disediakan khusus untuk memenuhi keperluan pemulihan bencana ke atas 4 sistem aplikasi yang kritikal sahaja yang termaktub dalam skop ISMS UPM.

4 Sistem kritikal tersebut adalah:

a) Sistem Aplikasi Pelajar
    a. Sistem Maklumat Pelajar (undergraduate)
    b. Sistem iGIMS (postgraduate)
b) Sistem Aplikasi Sumber Manusia
c) Sistem Aplikasi Kewangan
    a. SAS
    b. FAMS
    c. SAGA
d) Sistem laman Web Utama Universiti

Kesemua sistem aplikasi di atas terpilih disebabkan sistem aplikasi tersebut merupakan sistem aplikasi yang digunakan dalam Pengurusan Bisnes Operasi Utama Universiti.

4. STRATEGI SIMULASI PEMULIHAN BENCANA ICT

Aktiviti Pengujian Simulasi Pemulihan Bencana ICT.

BIL	FASA	LOKASI	AKTIVITI	MASA
1.	SEBELUM PERMULAAN BENCANA	Pusat Data Utama iDEC Beta	Team Seksyen Operasi melakukan ujian perubahan data ke atas semua sistem untuk dijadikan sample perubahan data KALI PERTAMA.	4.15 petang
2.	PERMULAAN BENCANA	Pusat Data Utama iDEC Beta	Gangguan kepada capaian Sistem Aplikasi i. Koordinator DRP akan membuat panggilan jemputan kepada Komander DRP dan Pentadbir Sistem untuk hadir ke loaksi utama Pusat Data Utama UPM. ii. Komander dan Semua Pentadbir Sistem hadir ke Pusat Data Utama untuk melihat dan menilai kerosakan.	4.30 petang
3.	PEMBERITAHUAN	Pusat Data Utama iDEC Beta	Sila Lihat **Lampiran 1** i. Semua Pentadbir Sistem memasuki Pusat Data Utama dan melihat serta melaporkan kerosakan atau gangguan yang dihadapi disebabkan bencana tersebut. ii. Komander DRP , Pentadbir Sistem dan Pentadbir Proses bersidang di bilik Collision Room untuk melaporkan laporan penilaian kerosakan masing-masing. iii. Komander DRP memohon kelulusan daripada Pengarah IDEC untuk mengistiharkan bencana.	5.00 petang

BIL	FASA	LOKASI	AKTIVITI	MASA
			iv. Komander DRP mendapatkan kelulusan untuk isytihar dan mengarahkan semua Pentadbir sistem untuk menggunapakai Disaster Recovery Plan seperti yang termaktub dalam Dokumen DRP ICT masing-masing.	
4.	PEMULIHAN	Pusat Data Utama iDEC Beta dan Pusat Data DR iDEC Epsilon	Sila lihat **Lampiran 2** i. Terdapat 2 kumpulan Pentadbir Sistem yang bertugas iaitu yang bertugas di Pusat Data Utama (iDEC Beta) dan satu kumpulan lagi bertugas di Pusat Data Pemulihan. ii. Semua ahli pentadbir Sistem melaksanakan proses pemulihan seperti yang termaktub dalam Dokumen DR masing-masing. iii. Team Seksyen Operasi melakukan ujian perubahan data ke atas semua sistem untuk dijadikan sample perubahan data KALI KEDUA.	5.30 hingga 7.30 petang
5.	PENGAKTIFAN DR	Pusat Data DR iDEC Epsilon	Semua Aplikasi Kritikal diaktifkan dan boleh capai oleh Pengguna i. Data dan HID DR diaktifkan ii. Sistem Operasi pelayan DR diaktifkan iii. Sistem aplikasi DR diaktifkan iv. Sistem DNS dan NAT DR diaktifkan	8.00 pagi
6.	PEMBENTUKAN SEMULA	Pusat Data Utama iDEC Beta	Sila lihat **Lampiran 3** 1. Data dan HID production di Pusat Data Utama diaktifkan beroperasi semula.	10:00 pagi sehingga semua aplikasi di Pusat Data

BIL	FASA	LOKASI	AKTIVITI	MASA
			2. Sistem Operasi pelayan production di Pusat Data Utama diaktifkan beroperasi semula 3. Sistem aplikasi production di Pusat Data Utama diaktifkan beroperasi semula 4. Sistem DNS dan NAT production diaktifkan di Pusat Data Utama beroperasi semula	Utama beroperasi seperti biasa

5. HASIL PENEMUAN SIMULASI DRP ICT 31 JULAI 2015

BIL	PENTADBIR SISTEM	KESIMPULAN	SYOR
1.	Pentadbiran Data	Terdapat 2 manual rollback yang berjaya :- a) Sistem Maklumat Pelajar b) Sistem Aplikasi Sumber Manusia	Akan melaksanakan kaedah auto rollback pada masa akan datang
2.	Sistem Aplikasi Pelajar	Berjaya dilaksanakan namum begitu *rollback* dibuat secara manual	Akan melaksanakan kaedah auto rollback pada masa akan datang.
3.	Sistem Sumber Manusia	Berjaya dilaksanakan	Akan melaksanakan kaedah auto rollback pada masa akan datang
4.	Sistem Kewangan	SISTEM SAGA Berjaya dilaksanakan pemulihan	
		SISTEM SAS Berjaya dilaksanakan pemulihan	
		SISTEM FAMS Berjaya dilaksanakan pemulihan	
5.	Sistem Laman Web Utama Universiti	Berjaya dilaksanakan pemulihan bencana termasuk roll back ke production	

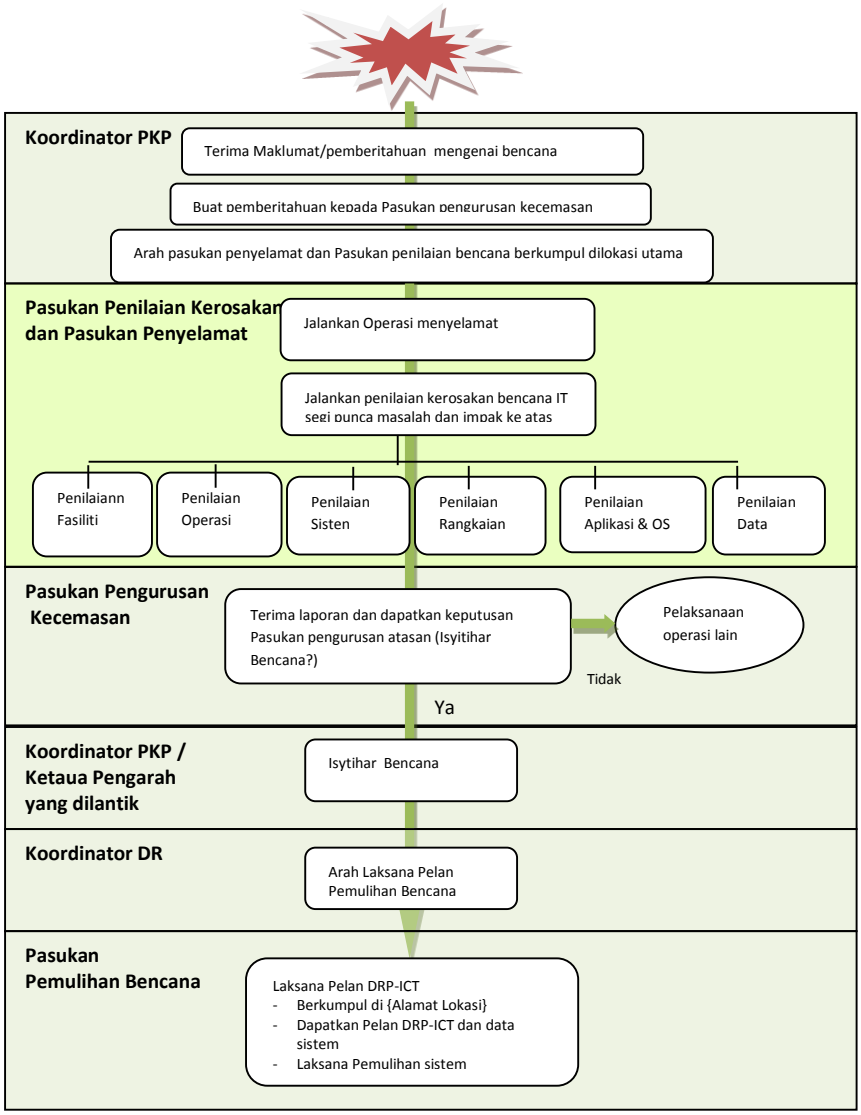
6. HASIL PENEMUAN SIMULASI DRP ICT 23 OKTOBER 2015

BIL	PENTADBIR SISTEM	KESIMPULAN	SYOR
1.	Pentadbiran Data	Terdapat 2 auto rollback yang berjaya :- a) Sistem Maklumat Pelajar b) Sistem Aplikasi Sumber Manusia	
2.	Sistem Aplikasi Pelajar	Simulasi sepenuhnya telah dijalankan dan Rollback secara auto Berjaya dilaksanakan	
3.	Sistem Sumber Manusia	Simulasi sepenuhnya telah dijalankan dan Rollback secara auto Berjaya dilaksanakan	

LAMPIRAN 1

FASA PEMBERITAHUAN

Rajah 1: Proses-proses Dalam Fasa Pengaktifan dan Pemberitahuan



Makluman Gangguan Elektrik kepada pasukan pemulihan bencana

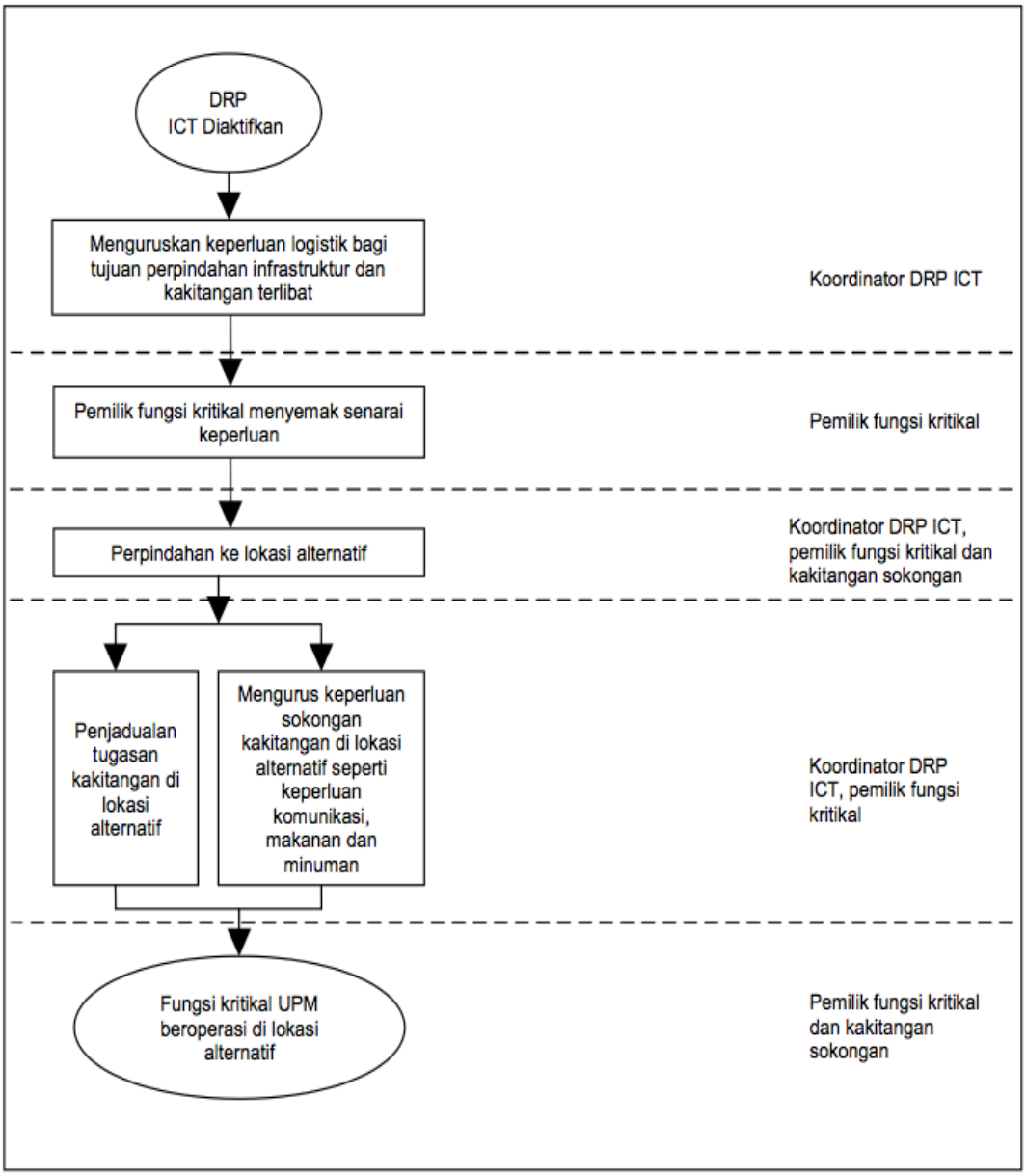
Penilaian gangguan dan penentuan tindakan yang boleh menentukan kepada pengaktifan Pelan DRP-ICT UPM

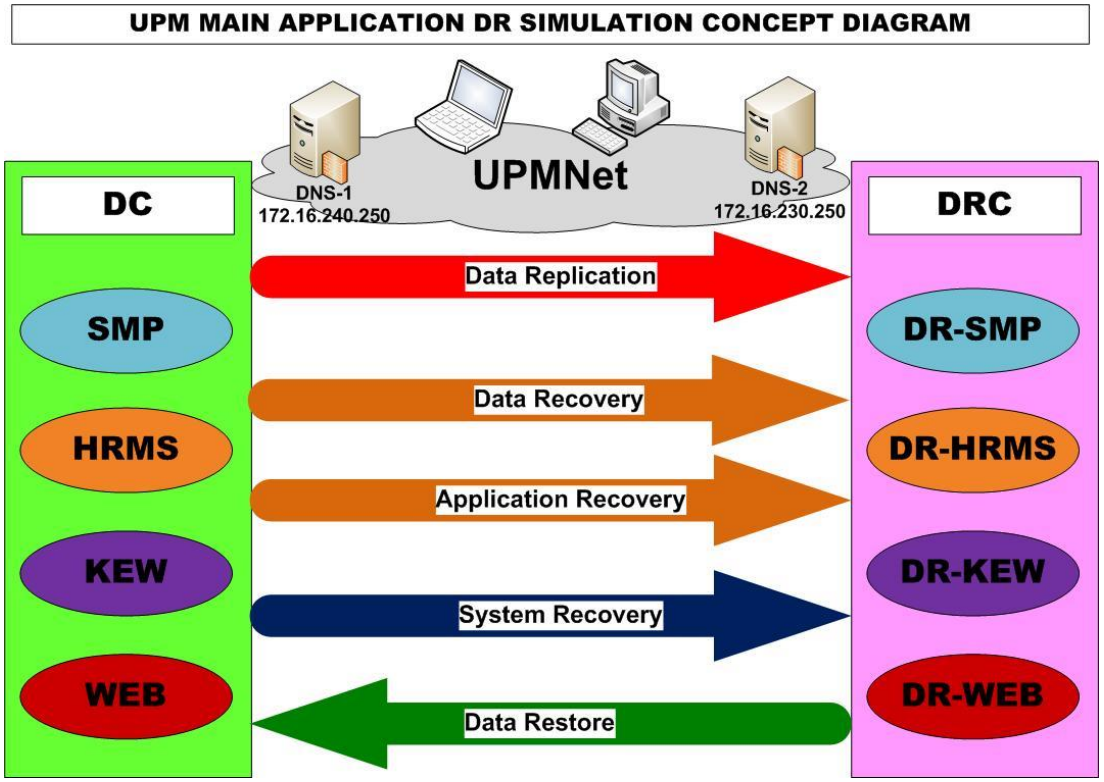
Semua ahli dalam pasukan pemulihan Bencana akan bersedia dengan Pelan DRP sistem aplikasi masing-masing.

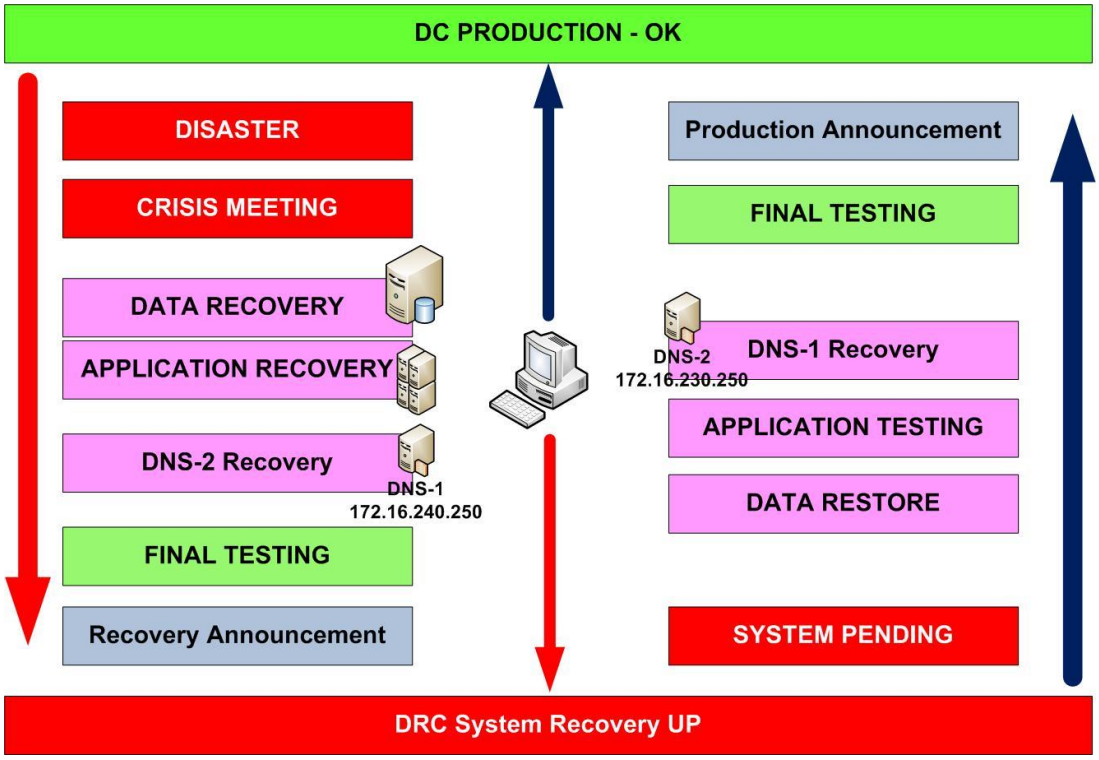
LAMPIRAN 2

FASA PEMULIHAN

Rajah 1: Proses-proses Dalam Fasa Pemulihan



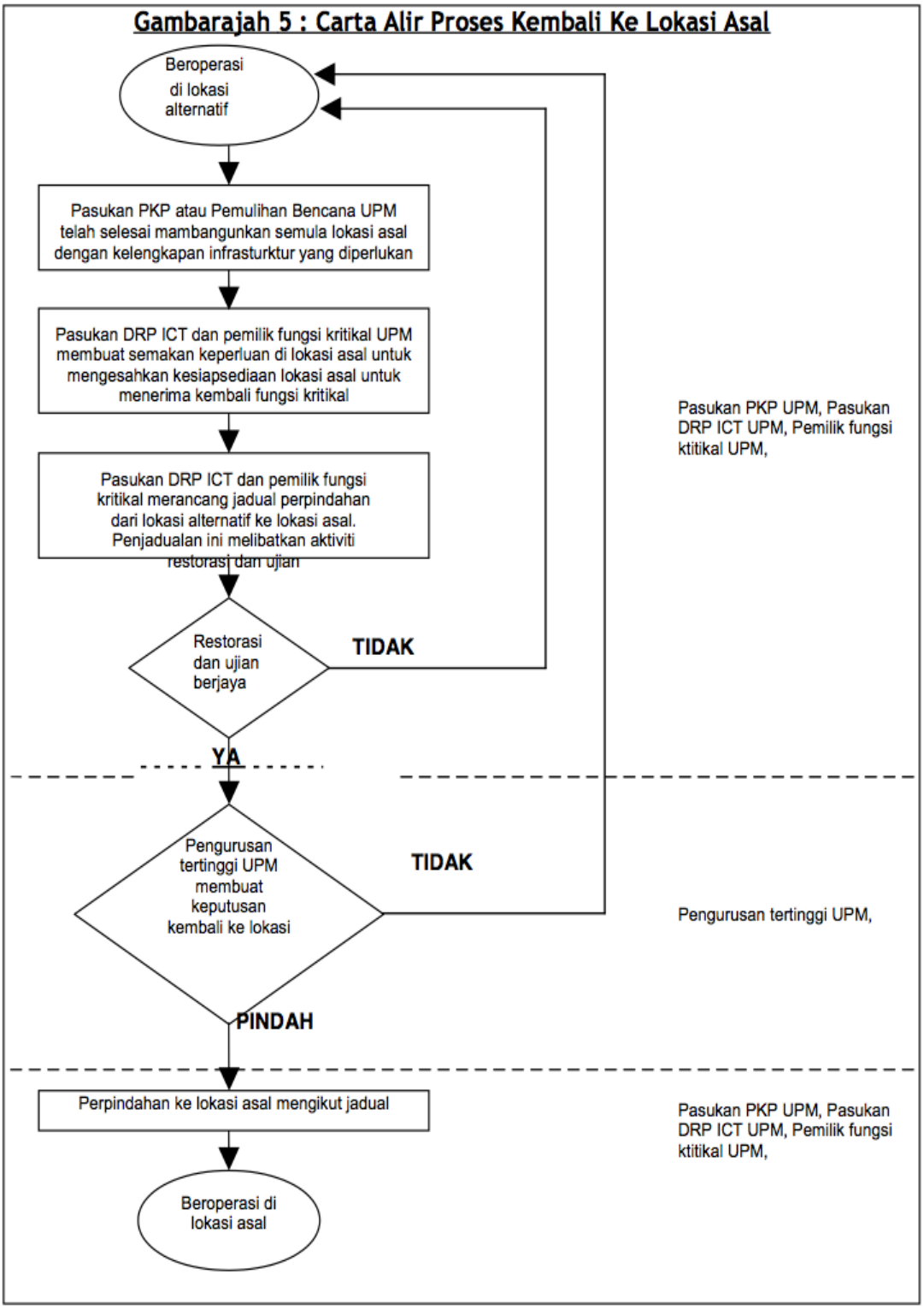

UPM MAIN APPLICATION DR SIMULATION CONCEPT DIAGRAM
UPMNet
DNS-1
172.16.240.250
DNS-2
172.16.230.250
DC
DRC
Data Replication
SMP
DR-SMP
Data Recovery
HRMS
DR-HRMS
Application Recovery
KEW
DR-KEW
System Recovery
WEB
DR-WEB
Data Restore


DC PRODUCTION - OK
DISASTER
CRISIS MEETING
DATA RECOVERY
APPLICATION RECOVERY
DNS-2 Recovery
DNS-1
172.16.240.250
FINAL TESTING
Recovery Announcement
Production Announcement
FINAL TESTING
DNS-2
172.16.230.250
DNS-1 Recovery
APPLICATION TESTING
DATA RESTORE
SYSTEM PENDING
DRC System Recovery UP

LAMPIRAN 3

FASA PEMBENTUKAN SEMULA

Rajah 1: Proses-proses Dalam Fasa Pembentukan Semula



PELAKSANAAN KAWALAN DI PELAN PEMULIHAN RISIKO

Statistik Aset Yang Dinilai Berasaskan Kerahsiaan, Integriti dan Ketersediaan (CIA)

	HARDWARE	SOFTWARE	PEOPLE	DATA & INFORMATION	SERVICE (SUPPORTING)	SERVICE (ACCESSBILITY)	ASSET COUNT
LOW	0	2	150	1	0	19	172
MEDIUM	47	19	51	42	95	0	254
HIGH	10	35	15	14	30	**36**	140
TOTAL	57	56	216	57	125	55	**566**

BIL.	ASET BERISIKO TINGGI	PELAN PEMULIHAN	STATUS PELAKSANAAN
1.	Lokasi Pusat Data di bangunan yang berumur lebih 50 tahun, kedudukan di aras bawah dan keluasan yang terhad untuk menampung keperluan server.	Pembangunan Pusat Data baharu melalui peruntukan Rancangan Malaysia Ke-11.	i. Permohonan cadangan Pusat Data baharu kepada Jawatankuasa Rancangan Malaysia Ke-11 Universiti pada Disember 2014. ii. Pembentangan cadangan di Bengkel Rancangan Malaysia Ke-11 Universiti pada Januari 2015. iii. Mendapat perakuan Pengurusan Universiti bagi mengenengahkan cadangan ke peringkat kementerian. iv. Pemurnian cadangan di Bengkel Pemurnian Racangan Malaysia Ke-11 UPM. v. Pembentangan cadangan kepada pihak EPU/MAMPU pada 18 Mei 2015. vi. Menunggu keputusan Rancangan Malaysia Ke-11.

AGENDA 5.0 - PENEMUAN AUDIT

AGENDA 5.1 AUDIT PEMANTAUAN 2 (SIRIM)

AGENDA 5.2 AUDIT DALAMAN ISMS 2015

PENEMUAN AUDIT PEMANTAUAN SEMAKAN 2
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT OLEH SIRIM

HASIL LAPORAN AUDIT PEMANTAUAN SEMAKAN 2
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (MS ISO/IEC 27001:2013)

1.0 TUJUAN

Kertas ini adalah bertujuan untuk memaklum kepada Ahli Mesyuarat Kajian Semula Pengurusan (MKSP) Universiti Putra Malaysia (UPM) berkaitan penemuan Audit Pemantauan Semakan 2, Sistem Pengurusan Keselamatan Maklumat oleh SIRIM.

2.0 PENGENALAN

Audit Pemantauan Semakan Kedua Sistem Pengurusan Keselamatan Maklumat oleh SIRIM telah dilaksana pada 29 hingga 30 Januari 2015. Sepanjang audit, seramai empat (4) orang Juruaudit telah terlibat bagi mengaudit skop seperti berikut:

a. Sistem pengurusan keselamatan maklumat bagi operasi Pusat Data UPM, merangkumi perkakasan (*server* dan storan) dan data/maklumat untuk aplikasi kritikal berikut:
    1. Laman Web Utama Universiti (www.upm.edu.my)
    2. Sistem Pengurusan Kewangan
    3. Sistem Pengurusan Sumber Manusia
    4. Sistem Maklumat Pelajar (SMP)
b. Sistem Pengurusan Keselamatan Maklumat untuk pengoperasian pusat data; dan
c. Sistem Pengurusan Keselamatan Maklumat untuk pengoperasian pusat pemulihan bencana.

3.0 LOKASI AUDIT

Lokasi audit adalah tertumpu kepada Pusat Pembangunan Maklumat dan Komunikasi.

4.0 PENEMUAN AUDIT

Hasil Audit Pemantauan Semakan 2, terdapat lapan (8) ketakakuran minor dan 10 peluang penambahbaikan. Ringkasan hasil laporan audit pensijilan semula boleh dirujuk seperti di bawah:-

4.1 ketakakuran;

4.2 peluang panambahbaikan; dan

4.1 KETAKAKURAN

BIL.	KETAKAKURAN	KLAUSA	BUKTI PENEMUAN *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
1.	AIS-1	7.5.3	Kawalan dokumen 1. Dokumen lapuk tidak dicop sebagai "DOKUMEN LUPUS". Sampel yang dilihat, Manual Sistem Pengurusan Keselamatan Maklumat, No. Semakan 04, No. Isu 01. 2. Dokumen Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi, No. Semakan 00, No. Isu 02. 3. Surat Aku Janji telah digantikan dengan Surat Aku Janji Pihak Luar tetapi tidak dicap batal.
2.	AIS-2	6.1.3	Merujuk kepada dokumen *Statement of Applicability (SoA)*, penggunaan dan justifikasi kawalan tidak dinyatakan mengikut keperluan klausa; 1. Penggunaan kawalan A.14.2 *Security in development and support process*. 2. Justifikasi bagi kawalan yang dikecualikan, iaitu A.6.2.2 dan A.14.2.5.
3.	AIS-3	9.1	Keperluan Garis Panduan Pengukuran Keberkesanan Kawalan ISMS, No. Semakan 01, No. Isu 01, bertarikh 9/11/2012. – Para 3.0 Skop dan 4.0 Pengukuran Keberkesanan Kawalan ISMS; 1. Tiada bukti pemilihan kawalan keselamatan dibuat berdasarkan penemuan penilaian risiko dan Risk Treatment Plan (RTP). 2. Pelaporan perbandingan pengukuran keberkesanan yang dibentangkan tidak mengikut format yang dinyatakan di dalam prosedur, iaitu dalam bentuk graf. 3. Pengukuran security metric yang kedua (kawalan A.16.1.1) perlu dilihat kembali agar kawalan dan objektif pengukuran berpadanan.

BIL.	KETAKAKURAN	KLAUSA	**BUKTI PENEMUAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
4.	EFI-1	6.1.3	Di dapati semakan terhadap laporan penguraian risiko (RTP) adalah tidak memenuhi keperluan kawalan standard. 1. Jangkamasa pelan penguraian risiko adalah sudah tamat. (Sample: Mula :Mac 2012- Dis 2012) 2. *Existing safeguard* adalah merujuk kawalan *treatment* yang sama. (sample: A.11.2.2 *Supporting utilities*).
5.	NR-1	8.1 / A 9.2.3	Audit mendapati *login* ID yang digunakan untuk capaian ke *network switches* dikongsi oleh beberapa orang pentadbir rangkaian. Tidak ada kekangan teknikal untuk mewujudkan *login* ID yang berasingan berdasarkan maklumat yang diperolehi semasa audit dijalankan. *Login* ID dengan *admin privilege* dikongsi untuk *capaian ke core switches* (core 24 dan core 23)
6.	NR-2	8.1 / A.9.3.1	Audit mendapati pengguna sistem masih boleh menggunakan kata laluan yang sama seperti yang diperuntukkan oleh pentadbir proses semasa *'login ID'* diwujudkan tanpa sebarang had. Tidak ada mekanisme untuk memastikan kata laluan ini ditukar semasa pengguna mencapai sistem pada kali pertama. Penukaran kata laluan semasa *'first time login'* tidak dilaksanakan mengikut keperluan garis panduan kata laluan UPM/IDEC untuk Sistem Maklumat Pelajar (SMP).
7.	SAZ-1	8.1 / A.9.4.1	*Login* ID ke aplikasi iGIMS di Sekolah Pengajian Siswasah tidak dikawal dan diselenggara dengan berkesan 1. *Login* ID tidak unik dan konsistent (ID: ex5tuff) 2. *Login* ID bagi pegawai yang bertukar tidak dikemaskini (KA0406 dan farah)

BIL.	KETAKAKURAN	KLAUSA	**BUKTI PENEMUAN** *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
8.	SAZ-2	8.1 / A.8.1.1	Aset- aset yang berkaiatan sistem iGIMS tidak dikenalpasti didalam Aset Register 1. Data & Information : Pengakalan Data iGIMS 2. People : Unit Pentadbiran Data (DB Administrator) dan Pentadbir sistem di Sekolah Pengajian Siswazah 3. Hardware : DR server (5 server VM, DRSGS dan DRSGSDB)

4.2 PELUANG PENAMBAHBAIKAN

BIL	KLAUSA	RINGKASAN PELUANG PENAMBAHBAIKAN *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
1.	4.2 (b)	Organisasi telah mengenal pasti pihak berkepentingan / pemegang taruh seperti mana yang dinyatakan di dalam dokumen Manual Sistem Pengurusan Keselamatan Maklumat. Walau bagaimanapun, keperluan bagi memenuhi kehendak pihak tersebut masih belum dinyatakan dengan jelas.
2.	4.3 (c)	***Determining the scope of the information security management system*** i) Organisasi boleh memperjelaskan lagi fungsi-fungsi sistem serta modul-modul yang terlibat bagi kesemua sistem kritikal di bawah skop pensijilan. ii) Audit mendapati bahawa organisasi masih belum menerangkan aktiviti-aktiviti yang melibatkan pihak ketiga (dalaman dan luaran).
3.	9.1	Merujuk kepada Manual Sistem Pengurusan Keselamatan Maklumat, organisasi telah menentukan beberapa objektif keselamatan dan *security metric* sebagai pengukuran terhadap pelaksanaan ISMS. Namun, kaedah pemantauan, pengukuran, analisa dan penilaiannya perlu diperjelaskan lagi.
4.	7.2(c)	***Competence*** Organisasi masih belum melaksana penilaian keberkesanan latihan bagi Bengkel Pemantapan Juruaudit Dalaman ISMS
5.	A.12.6.1	*Management of tehcnical/ vulnerabilities* Imbasan berkala bagi server/host telah dijalankan pada 12/6/2014 dan 22/12/2014 dengan menggunakan peralatan Acunetix. Walau bagaimanapun, perkara di bawah boleh dilihat kembali:- i. Definisi kategori bagi setiap penemuan iaitu *High, Medium* dan *Low*. ii. Justifikasi bagi penemuan yang tidak memerlukan tindakan selanjutnya dan tindakan yang telah diambil perlu direkodkan dengan lebih jelas.

BIL	KLAUSA	RINGKASAN PELUANG PENAMBAHBAIKAN *Hendaklah dibaca bersama Laporan SIRIM yang boleh dirujuk pada e-ISO*
6.	A.11.2.1	***Equipment Siting and Protection*** Didapati bilik rangkaian yang menempatkan perkakasan rangkaian boleh ditambahbaik dari segi pengudaraan suhu bilik.
7.	A.12.1.3	***Capacity Management*** Pengurusan kapasiti untuk storan pendua boleh ditambahbaik bagi mengelakkan pendua gagal kerana storan penuh.
8.	A.13.2.4	***Confidentiality or non-disclosure agreements.*** Surat Akuan Pematuhan GPKTMK UPM tidak digunapakai secara konsisten untuk pihak ketiga. (pembekal).
9.	A.9.2.5	***Review of user access rights*** Pelaksanaan kawalan pengemaskinian login ID bagi capaian *servers* di dalam pusat data telah dilaksanakan pada tahun 2013. Walau bagaimanapun, pemantauan untuk memastikan kawalan terus dilaksanakan dengan berkesan perlu diberi perhatian memandangkan jangkamasa Januari 2015 untuk pelaksanaan tersebut hampir tamat.
10.	A.12.4.1 A.12.4.2 A.12.4.3	***Logging and monitoring*** Kawalan ***'centralised log server'*** masih di dalam perancangan. Pelaksanaan kawalan ***'logging and monitoring'*** untuk semua aset yang terlibat perlu dipantau bagi memastikan 'event logs' sentiasa direkod, disimpan dan disemak dengan baik.

5.0 STATUS KETAKAKURAN DAN PELUANG PENAMBAHBAIKAN

Semua bukti ketakakuran dan tiga (3) peluang penambahbaikan telah dimajukan kepada SIRIM dalam tempoh tiga (3) bulan dan pihak UPM telah memajukan dokumen kepada SIRIM pada 30 April 2015 dan telah ditutup. Bagi peluang penambahbaikan, pihak SIRIM akan melihat pada Audit Pensijilan Semula yang dijadualkan pada 8 dan 9 Disember 2015.

6.0 SYOR

Mesyuarat dimohon beri perhatian perkara berikut:-

i. pihak yang terlibat dengan skop ISMS terkini hendaklah melihat semua ketakakuran yang berlaku dan memastikan ianya tidak berulang semasa Audit Pensijilan Semula;
ii. Pejabat Pembangunan Maklumat dan Komunikasi hendaklah mengambil tindakan pada setiap peluang penambahbaikan yang telah dikemukakan oleh SIRIM; dan
iii. pihak yang terlibat dengan skop terkini ISMS hendaklah meneliti dan melaksana peluang penambahbaikan yang dikemuka oleh SIRIM bagi yang berkaitan dengan skop semasa.

LAPORAN AUDIT DALAMAN TAHUN 2015

UNIVERSITI PUTRA MALAYSIA
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
MS ISO/IEC 27001:2013

1. TARIKH AUDIT

Audit Dalaman Sistem Pengurusan Keselamatan Maklumat (ISMS) Universiti Putra Malaysia (UPM) 2015 telah dijalankan pada 18 dan 19 November 2015.

2. TUJUAN AUDIT

Audit Dalaman dijalankan untuk menentukan sama ada UPM:

i. melaksanakan pengurusan keselamatan maklumat berdasarkan keperluan Standard MS ISO/IEC 27001:2013 dengan efektif selaras dengan Peraturan Keselamatan ICT UPM serta objektif dan sasaran Sistem Pengurusan Keselamatan Maklumat UPM; dan

ii. bersedia untuk menghadapi Audit Pensijilan Semula oleh Badan Pensijilan.

3. KRITERIA AUDIT

Audit Dalaman dijalankan berdasarkan dokumen dan rujukan berikut:

i. Standard MS ISO/IEC 27001:2013
ii. Dokumentasi ISMS UPM
iii. Akta dan Peraturan berkaitan
iv. Rujukan lain yang dinyatakan dalam Manual Kualiti/Prosedur

4. KAEDAH AUDIT

Kaedah pelaksananaan Audit Dalaman merangkumi:

i. Lawatan tapak/tempat *(Site visit)*
ii. Pemerhatian
iii. Temubual
iv. Penilaian ke atas prosedur, rekod dan dokumen berkaitan
v. Pelaporan penemuan audit secara lisan dan bertulis.

5. SKOP AUDIT

Audit Dalaman dijalankan mengikut skop Sistem Pengurusan Keselamatan Maklumat UPM yang hanya melibatkan proses :

i. Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Maklumat Pelajar (SMP);

ii. Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah; dan

iii. Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah.

6. KUMPULAN AUDIT

Seramai 15 orang Juruaudit Dalaman ISMS UPM yang telah dibahagikan kepada tiga (3) kumpulan audit telah mengaudit proses dalam skop Sistem Pengurusan Keselamatan Maklumat UPM.

7. PROGRAM AUDIT DALAMAN

Program Audit Dalaman telah disediakan oleh Ketua Seksyen Audit Kualiti, Pusat Jaminan Kualiti UPM dan disahkan oleh Wakil Pengurusan UPM. Program Audit telah dimaklumkan kepada semua peneraju proses, pusat tanggunjawab dan Juruaudit Dalaman pada 30 Oktober 2015.

8. PENEMUAN AUDIT

Kekuatan

i. Tahap dokumentasi adalah baik dan memenuhi keperluan Standard MS ISO/IEC 27001:2013.
ii. Komitment Pengurusan UPM, Peneraju Proses dan Pusat Jaminan Kualiti adalah tinggi dalam menyelaraskan dan melaksanakan Sistem Pengurusan Keselamatan Maklumat.
iii. Semua objektif keselamatan yang ditetapkan telah diukur telah dan mencapai sasaran 100%.
iv. Dokumen ISMS mudah dicapai dan dirujuk oleh semua staf menerusi sistem e-ISO menggunakan id dan kata laluan (UPMID) masing-masing. Capaian laman sesawang sistem e-ISO boleh diakses di dalam dan di luar kampus.
v. *Risk assessment* dan *Risk treatment* telah dilaksanakan dengan baik dan memenuhi keperluan Standard MS ISO/IEC 27001:2013

vi. Pengoperasian Pusat Data adalah pada tahap selamat dan memenuhi keperluan Standard MS ISO/IEC 27001:2013
vii. Amalan keselamatan maklumat adalah baik walaupun kesedaran terhadap ISMS dalam kalangan staf pelaksana kurang memuaskan.

Kelemahan

i. Tahap kesedaran tentang Sistem Pengurusan Keselamatan Maklumat dalam kalangan pelaksana adalah kurang memuaskan.
ii. Kawalan terhadap pengopersian proses perlu dipertingkatkan.
iii. Penggunaan katalaluan perlu dikawal dengan lebih rapi.

Cadangan

i. Skop ISMS dalam Manual Sistem Pengurusan Keselamatan Maklumat diselarikan dengan Proses Perkhidmatan Skop ISMS UPM.
ii. Pernyataan Dasar ISMS dihebahkan kepada pihak dalaman dan pihak luaran untuk meningkatkan tahap kesedaran ISMS.
iii. Kaedah kawalan katalaluan pegawai yang akan bersara dari perkhidmatan perlu diperbaiki.
iv. *Mirror site* dibangunkan untuk Portal eISO bagi membolehkan capaian berterusan (24/7) dan memastikan maklumat sentiasa selamat dan terjamin.
v. Justifikasi Pengeculian Skop ISMS diperincikan dengan pelan perancangan yang jelas.
vi. Takwim disediakan bagi semakan semula Pelan Pemulihan Bencana ICT, Pelan Kesinambungan Perkhidmatan dan Aktiviti Jawatankuasa Penilaian Risiko ISMS.
vii. *Statement of Applicability* (SOA) yang dihasilkan dikenalpasti semula bagi memastikan meliputi keseluruhan skop ISMS.
viii. Taklimat persediaan untuk hari pendaftaran direkodkan.
ix. Senarai tugas staf disemak semula selaras dengan tanggungjawab keselamatan maklumat yang dilaksanakan.

9. BILANGAN KETAKAKURAN DAN PELUANG PENAMBAHBAIKAN

Ketakakuran

Jumlah Ketakakuran (NCR) – Tiga (3)
i. Satu (1) - Klausa 7.1 : *Resources*
ii. Satu (1) - Klausa 7.3 : *Awareness*

iii. Satu (1) - Klausa 8.1 : *Operational planning and control*

Peluang Penambahbaikan

Jumlah Cadangan Peluang Penambahbaikan (OFI) – 14

i. Dua (2) - Klausa 4.3 : *Determining the scope of the ISMS*
ii. Satu (1) - Klausa 5.2 (f) : *Policy*
iii. Satu (1) - Klausa 6.1.1 : *Planning*
iv. Satu (1) - Klausa 6.1.3 (d) : *Information security risk treatment*
v. Satu (1) - Klausa 7.3 : *Awareness*
vi. Satu (1) - Klausa 7.5.3 : *Control of documented information*
vii. Tujuh (7) - Klausa 8.1 : *Operational planning and control*

10. TARIKH TUTUP NCR

Semua ketakauran (NSR) hendaklah diambil tindakan dan ditutup dalam tempoh 21 hari bekerja atau pada tarikh yang telah dipersetujui oleh Juruaudit Dalaman UPM.

11. KESIMPULAN

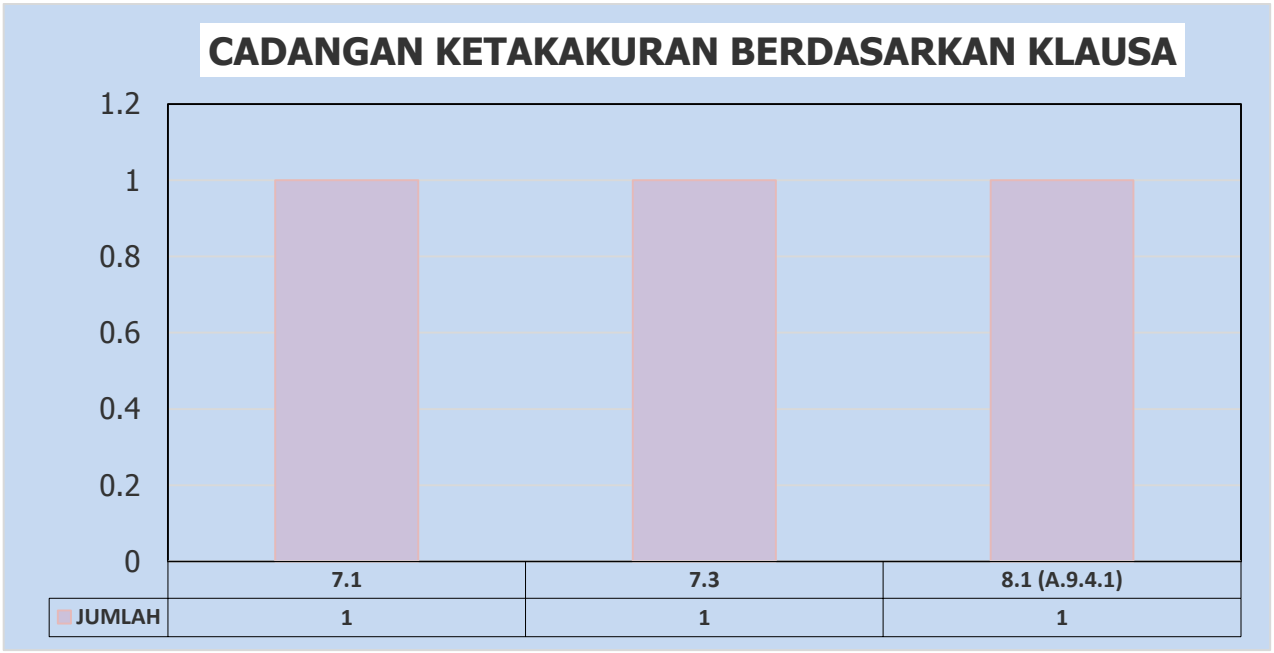
Hasil dari proses audit dalaman yang telah dijalankan, ketakakuran yang ditemui adalah menjurus kepada sumber, tahap kesedaran serta perancangan dan kawalan operasi.

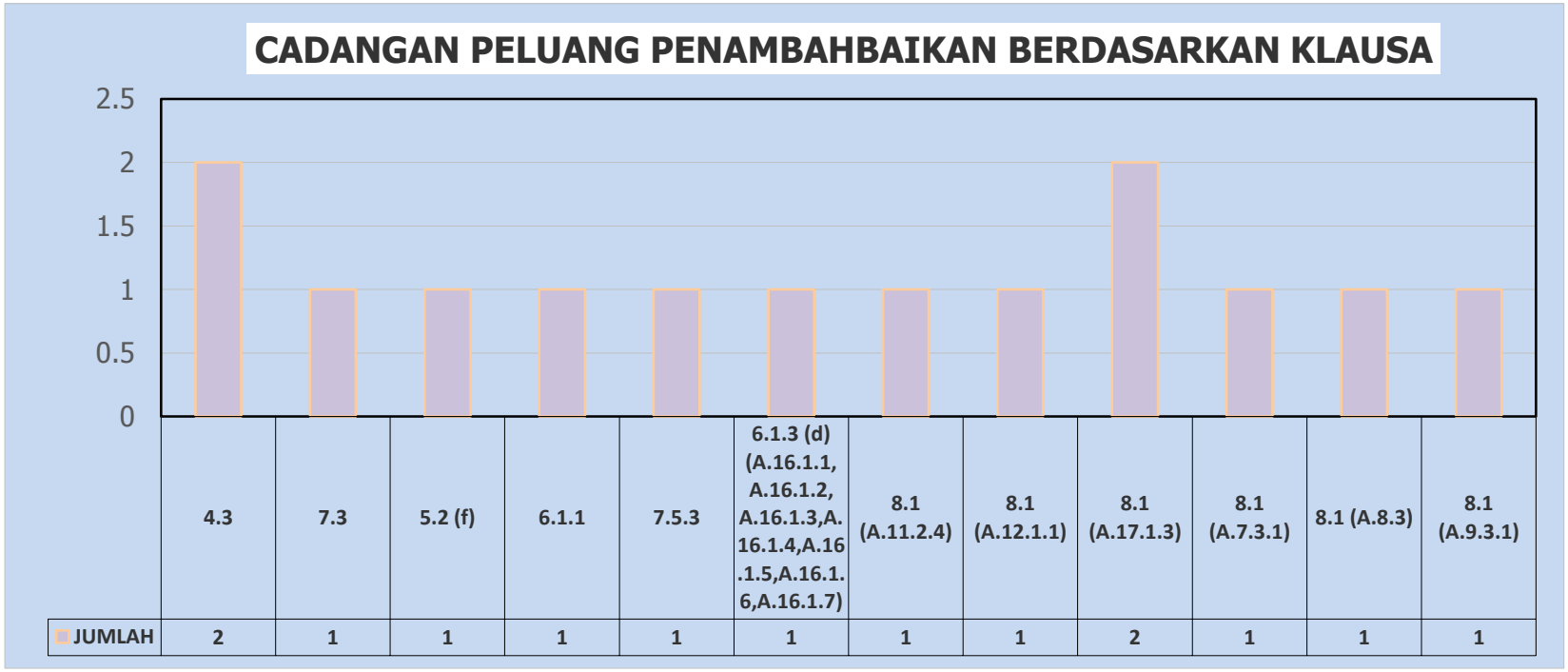
Dari segi perlaksanaan ISMS, Universiti Putra Malaysia adalah bersedia untuk diaudit oleh badan pensijilan tertakluk kepada tindakan pembetulan yang berkesan diambil terhadap ketakakuran yang ditemui dalam masa yang telah ditetapkan.

Pihak pengurusan Universiti Putra Malaysia perlu terus meningkatkan tahap kefahaman ISMS dalam kalangan semua staf UPM melalui latihan, komunikasi dalaman dan penyampaian maklumat mengenai ISMS kepada semua staf, pihak dalaman dan luaran yang ada kepentingan, pemilik risiko serta pembekal yang berkaitan.

Ketua Juruaudit dan semua Juruaudit Dalaman ISMS UPM ingin merakamkan ucapan setinggi-tinggi terima kasih atas kerjasama dan layanan baik yang diberikan oleh setiap peringkat staf Universiti Putra Malaysia sepanjang perlaksanaan audit dalaman ini.

Disediakan oleh
Krishnan Mariappan
Ketua Juruaudit Audit Dalaman ISMS
19 November 2015


CADANGAN KETAKAKURAN BERDASARKAN KLAUSA
1.2
1
0.8
0.6
0.4
0.2
0
7.1
7.3
8.1 (A.9.4.1)
JUMLAH
1
1
1



	4.3	7.3	5.2 (f)	6.1.1	7.5.3	6.1.3 (d) (A.16.1.1, A.16.1.2, A.16.1.3,A.16.1.4,A.16.1.5,A.16.1.6,A.16.1.7)	8.1 (A.11.2.4)	8.1 (A.12.1.1)	8.1 (A.17.1.3)	8.1 (A.7.3.1)	8.1 (A.8.3)	8.1 (A.9.3.1)
JUMLAH	2	1	1	1	1	1	1	1	2	1	1	1

AGENDA 6.0

MAKLUM BALAS PEMEGANG TARUH

LAPORAN KAJIAN KEBERKESANAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) DALAM KALANGAN PENERAJU PROSES YANG TERLIBAT SEMASA PENDAFTARAN PELAJAR BAHARU SERTA PENGOPERASIAN SISTEM MAKLUMAT PELAJAR (SMP) DI UNIVERSITI PUTRA MALAYSIA

1.0 TUJUAN

Kajian ini bertujuan untuk melihat keberkesanan Sistem Pengurusan Keselamatan Maklumat (ISMS) dalam kalangan Peneraju Proses yang terlibat semasa pendaftaran pelajar baharu serta pengoperasian Sistem Maklumat Pelajar (SMP) terhadap keselamatan data atau maklumat di Universiti Putra Malaysia.

2.0 LATAR BELAKANG

Kajian ini dilaksana kepada Peneraju Proses terhadap pelaksanaan ISMS di Universiti Putra Malaysia. Ia adalah untuk mengetahui tahap pengetahuan, kefahaman dan penerimaan terhadap pelaksanaan ISMS yang melibatkan operasi dan perkhidmatan entiti-entiti yang berkaitan. Persepsi mereka yang juga sebagai pemegang taruh ini dipengaruhi oleh perkaitan dan kepentingannya serta harapan mereka terhadap implementasi ISMS di Universiti Putra Malaysia.

Pelaksanan ISMS bagi skop yang baharu bukan sahaja melibatkan pihak Pusat Pembangunan Maklumat dan Komunikasi (iDEC) tetapi semua pihak yang terlibat dalam urusan pendaftaran kemasukan pelajar baharu, pengurusan keselamatan UPM dan juga pengurusan sumber manusia. Pelaksanaan pada peringkat awal jelas membuktikan pemegang taruh kurang faham dan kurang jelas berkenaan tujuan ISMS serta impak pelaksanaan. Pihak iDEC telah mengedarkan borang kajian yang memberikan perkhidmatan berkaitan pengurusan serta proses pendaftaran kemasukan pelajar baharu di Universiti Putra Malaysia. Kumpulan sasaran adalah pemilik dan pelaksana proses yang terlibat seperti Pejabat Strategi Korporat dan Komunikasi, Pejabat Pendaftar, Pejabat Bursar, Kolej-Kolej, Bahagian Kemasukan dan Tadbir Urus Akademik, Bahagian Hal Ehwal Pelajar, Bahagian Keselamatan Universiti dan juga seksyen-seksyen di dalam iDEC.

3.0 RINGKASAN MAKLUMAT BERKAITAN

Kajian yang dijalankan adalah berdasarkan soalan-soalan yang diajukan kepada pemegang taruh sasaran. Respon pemegang taruh adalah berdasarkan tahap kepuasan mereka mengikut skala 1 hingga 5 yang telah ditetapkan. Maklumat skala, soalan-soalan yang diajukan dan respon pemegang taruh yang berkaitan dapat dirujuk pada **Lampiran A**.

Ringkasan analisis bagi kaji selidik berkenaan adalah seperti jadual di bawah:-

Kategori Penilaian	Pencapaian (Peratus)	
	Skala 4 dan ke atas (%)	**Skala 3 dan ke bawah (%)**
1. Tahap keselamatan data atau maklumat **semasa** yang berada di bawah tanggungjawab responden	54.55%	45.45%
2. Tahap kefahaman keperluan keselamatan data atau maklumat **sebelum pelaksanaan ISMS**	27.30%	72.70%
3. Tahap kefahaman keperluan keselamatan data atau maklumat **selepas pelaksanaan ISMS**	63.64%	36.36%
4. Keyakinan anda terhadap tahap keselamatan data atau maklumat bagi proses yang berada di bawah tanggungjawab responden **sebelum pelaksanaan ISMS**	45.45%	54.55%
5. Keyakinan anda terhadap tahap keselamatan data atau maklumat bagi proses yang berada di bawah tanggungjawab responden **selepas pelaksanaan ISMS**	81.82%	18.18%

Daripada kajian terhadap keperluan keselamatan data atau maklumat **sebelum** dan **selepas** pelaksanaan ISMS, secara majoriti pemahaman pemegang taruh terhadap keperluan kerahsiaan data, integriti data dan ketersediaan data adalah di tahap yang baik. Maklum balas pemegang taruh juga menyatakan kurang pemahaman dalam kalangan warga UPM kerana kurang penganjuran kursus dan pendedahan setiap staf yang terlibat dalam proses berkaitan berkenaan tentang keselamatan data atau

maklumat. Secara khususnya, staf yang terlibat dengan proses dan perkhidmatan yang berkaitan perlu diberi pemahaman asas keselamatan data secara komprehensif.

Secara keseluruhan, Peneraju Proses lebih berkeyakinan terhadap tahap keselamatan data atau maklumat bagi proses yang berada di bawah tanggungjawab mereka dengan adanya pelaksanaan ISMS di UPM. Walau bagaimanapun, rata-rata berpendapat pihak berkaitan perlu lebih giat melaksanakan *roadshow* atau sesi taklimat berkenaan keselamatan maklumat kepada semua staf dan pelajar untuk meningkatkan kefahaman dan keyakinan pengguna terhadap pelaksanaan ISMS di UPM.

4.0 KESIMPULAN

Hasil kajian terhadap pelaksanaan ISMS bagi keselamatan data atau maklumat di Universiti Putra Malaysia adalah:

a. usaha memberi kesedaran kepada pengguna berkenaan objektif pelaksanaan ISMS bagi meningkatkan kefahaman dan keyakinan pengguna terutamanya apabila berlakunya perubahan terhadap skop ISMS sebelum ini;
b. pihak pemegang taruh secara majoriti telah memahami kepentingan pelaksanaan ISMS terhadap aspek keselamatan data dan maklumat;
c. tahap kepercayaan pemegang taruh terhadap aspek keselamatan data dan maklumat lebih tinggi selepas pelaksanaan ISMS; dan
d. pemegang taruh lebih berkeyakinan terhadap tahap keselamatan data atau maklumat yang digunakan.

5.0 CADANGAN

Pada Sesi Kemasukan 2016/2017 adalah dicadangkan agar kajian dibuat semua proses pendaftaran pelajar baharu dengan mengedarkan borang kajian kepada pihak yang berkepentingan dengan skop baharu seperti pelajar atau ibubapa.

LAMPIRAN A

ANALISIS KAJIAN KEBERKESANAN SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS) DALAM KALANGAN PENERAJU PROSES YANG TERLIBAT SEMASA PENDAFTARAN PELAJAR BAHARU SERTA PENGOPERASIAN SISTEM MAKLUMAT PELAJAR (SMP) DI UNIVERSITI PUTRA MALAYSIA

SKALA	1	2	3	4	5
JAWAPAN	Sangat Tidak Memuaskan	Tidak Memuaskan	Sederhana	Memuaskan	Sangat Memuaskan

Bil	Soalan	Maklumat Kajian		
		Skala	Kekerapan	Peratusan
1	Tahap keselamatan data atau maklumat di bawah tanggungjawab anda sekarang			
		1	0	0.00%
		2	0	0.00%
		3	5	45.45%
		4	3	27.27%
		5	3	27.27%
2	Tahap kefahaman keperluan keselamatan data atau maklumat *sebelum pelaksanaan* ISMS			
		1	0	0.00%
		2	4	36.36%
		3	4	36.36%
		4	2	18.18%
		5	1	9.09%
3	Tahap kefahaman keperluan keselamatan data atau maklumat *selepas pelaksanaan* ISMS			
		1	0	0.00%
		2	0	0.00%
		3	4	36.36%
		4	3	27.27%
		5	4	36.36%
4	Keyakinan anda terhadap tahap keselamatan data atau maklumat bagi proses yang berada di bawah tanggungjawab anda *sebelum pelaksanaan* ISMS daripada aspek berikut :- (* jawab jika berkaitan) i. Tahap keyakinan anda terhadap perkhidmatan Pusat Data dalam mengurus aplikasi server (Sila jawab jika proses anda melibatkan aplikasi) ii. Tahap keyakinan anda terhadap pengurusan maklumat semasa proses pendaftaran pelajar. (Sila jawab jika proses anda melibatkan pendaftaran)			

Bil	Soalan	Maklumat Kajian		
		Skala	Kekerapan	Peratusan
		1	0	0.00%
		2	0	0.00%
		3	6	54.55%
		4	2	18.18%
		5	3	27.27%
5	Keyakinan anda terhadap tahap keselamatan data atau maklumat bagi proses yang berada di bawah tanggungjawab anda *selepas pelaksanaan* ISMS daripada aspek berikut :- (* jawab jika berkaitan) i. Tahap keyakinan anda terhadap perkhidmatan Pusat Data dalam mengurus aplikasi server (Sila jawab jika proses anda melibatkan aplikasi) ii. Tahap keyakinan anda terhadap pengurusan maklumat semasa proses pendaftaran pelajar. (Sila jawab jika proses anda melibatkan pendaftaran			
		1	0	0.00%
		2	0	0.00%
		3	2	18.18%
		4	5	45.45%
		5	4	36.36%

AGENDA 7.0

HASIL PENILAIAN RISIKO DAN STATUS PELAN PEMULIHAN RISIKO

HASIL PENILAIAN RISIKO DAN STATUS PELAN PEMULIHAN RISIKO

Keperluan penilaian risiko dalam pelaksanaan ISMS adalah berdasarkan standard ISO/IEC 27001:2013, iaitu:

a) Klausa 6.1 : *Actions to address risk and opportunities*
b) Klausa 8.2 : *Information security risk assessment*
c) Klausa 8.3 : *Information security risk treatment*

BIL.	OUTPUT PENILAIAN RISIKO JUMLAH ASET : 566	PUNCA DOMINAN	PELAN PEMULIHAN	TANGGUNGJAWAB
1.	Aset berisiko tinggi = 12 (1%)	Lokasi Pusat Data di bangunan yang berumur lebih 50 tahun, kedudukan di aras bawah dan keluasan yang terhad untuk menampung keperluan server.	Pembangunan Pusat Data baharu melalui peruntukan Rancangan Malaysia Ke-11.	Pusat Pembangunan Maklumat dan Komunikasi
2.	Aset berisiko sederhana = 260 (22.9%)	i. Pembayaran yuran pendaftaran secara tunai (30%) adalah terdedah kepada risiko. ii. Pelaksanaan naik taraf elektrik Pusat Pemulihan Data sedang dilaksanakan. iii. Masih terdapat komputer lama	i. Sifar bayaran yuran pendaftaran secara tunai. ii. Naik taraf dijangka siap Disember 2015. iii. Kajian semula keperluan komputer kolej dengan	i. Pejabat Bursar ii. Pejabat Pembangunan dan Pengurusan Aset iii. Kolej dan Pusat Pembangunan

BIL.	OUTPUT PENILAIAN RISIKO JUMLAH ASET : 566	PUNCA DOMINAN	PELAN PEMULIHAN	TANGGUNGJAWAB
		(sistem pengoperasian (OS) yang telah luput) yang digunakan oleh pihak Kolej untuk tujuan pendaftaran pelajar yang berisiko dari aspek keselamatan .	mengambil kira penggantian komputer lama dengan sistem pengoperasian (OS) luput yang tidak selamat dalam aspek keselamatan.	Maklumat dan Komunikasi
	Aset berisiko rendah = 865 (76.1%)	i. Hampir semua proses pendaftaran pelajar baharu dilaksana berdasarkan arahan kerja yang wujud di dalam Sistem Pengurusan Kualiti. ii. Semakan awal pendaftaran pelajar oleh pihak kolej. iii. Kepelbagaian kaedah pembayaran yuran pengajian telah diwujudkan oleh Pejabat Bursar. iv. Penambahbaikan dengan mewujudkan bilik khas bagi penyimpanan x-ray oleh Pusat Kesihatan Universiti. v. Sumber maklumat pelajar yang ditawarkan kemasukan terus daripada sumber maklumat Bahagian Pengurusan	Tidak perlu pelan pemulihan	

BIL.	OUTPUT PENILAIAN RISIKO JUMLAH ASET : 566	PUNCA DOMINAN	PELAN PEMULIHAN	TANGGUNGJAWAB
		Kemasukan Pelajar (BPKP/UPU) ke Sistem Maklumat Pelajar (SMP). vi. Sumber maklumat untuk tujuan penghasilan kad pelajar diambil terus daripada Profil Pelajar SMP oleh Bahagian Keselamatan.		

AGENDA 8.0

PELUANG PENAMBAHBAIKAN

PELUANG PENAMBAHBAIKAN

BIL.	KETERANGAN PELUANG PENAMBAHBAIKAN	JUSTIFIKASI	TANGGUNGJAWAB
1.	Sifar bayaran yuran pendaftaran secara tunai.	Pembayaran secara tunai sentiasa terdedah kepada pelbagai risiko keselamatan.	Pejabat Bursar
2.	Melaksana pendaftaran pelajar baharu secara atas talian sebelum hari pendaftaran sebenar.	i. Pendaftaran awal membolehkan pihak UPM membuar anggaran pelajar yang menerima tawaran. ii. Dapat mempercepatkan proses pendaftaran sebenar.	Bahagian Kemasukan dan Bahagian Hal Ehwal Pelajar
3.	Menambah ciri pelaporan dalam sistem capaian pintu secara *biometric* di Pusat Data Utama.	Menukar sistem sistem capaian pintu daripada teknologi e-jari (2011) kepada teknologi terkini.	Pusat Pembangunan Maklumat dan Komunikasi