MINIT MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT (ISMS)
KALI KEEMPAT UNIVERSITI PUTRA MALAYSIA

Tarikh : 27 November 2015
Masa : 10.30 Pagi
Tempat : Bilik Mesyuarat Utama, Fakulti Perubatan dan Sains Kesihatan
Kehadiran : Lampiran A

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	PENDAHULUAN **Kata Alu-aluan** Pengerusi: (a) mengalu-alu kehadiran ahli mesyuarat ke MKSP ISMS, Kali Keempat; (b) memaklumkan bahawa mesyuarat ISMS tahun hadapan akan digabungkan dalam satu MKPS merangkumi tiga (3) sitem iaitu Sistem Pengurusan Kualiti, Sistem Pengurusan Keselamatan Maklumat dan Sistem Pengurusan Alam Sekitar; dan (c) merakamkan ucapan takziah dan sedekahkan Al-Fatihah kepada Allahyarham Mohamad Ghazali bin Haji Ali, Mantan Pengarah Pusat Islam yang telah kembali ke rahmatullah pada pagi tadi.	 **Makluman** **Makluman**
4.1	**PENGESAHAN MINIT MESYUARAT** Minit MKSP ISMS kali ketiga yang telah diadakan pada 1 Disember 2014 disahkan dengan pindaan pada Minit 3.3.1 berkaitan tarikh Audit Pemantauan oleh SIRIM yang dilaksanakan pada 24 dan 5 September 2013 kepada 24 dan 25 September 2013.	 **Makluman**
4.2	**TINDAKAN SUSULAN DARIPADA MESYUARAT LEPAS** Mesyuarat dimaklumkan berkenaan tindakan susulan yang telah dilaksana daripada mesyuarat yang lepas sebagaimana **Lampiran 1**. Mesyuarat mengambil perhatian berhubung penggunaan skop baharu yang telah berkuat kuasa pada 7 Disember 2015 yang memberi kesan pindaan terhadap objektif keselamatan maklumat secara keseluruhan.	 **Makluman Semua Tindakan TWP ISMS**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
4.3	**PERUBAHAN ISU DALAMAN DAN ISU LUARAN** Mesyuarat mengambil maklum pembentangan perubahan isu dalaman dan luaran yang berkaitan ISMS seperti berikut: (a) perubahan isu dalaman dan luaran adalah meliputi pelaksanaan 2012 hingga 2015; dan (b) tumpuan skop 2015 yang telah dipinda dengan mengambil kira kepentingan universiti dalam aspek dalaman dan luaran. Jadual perbandingan pelaksanaan 2012-2014 dan pelaksanaan 2015 adalah seperti **Lampiran 2**. Mesyuarat mencadangkan, pada masa hadapan Pelaksanaan ISMS diperluaskan dengan mengambil kira skop berkaitan MOOC, precom. <u>Kesimpulan:</u> Berdasarkan keperluan Standard MS ISO/IEC 27001:2013 serta matlamat pelan strategik universiti, maka hala tuju pelaksanaan ISMS universiti berada di landasan yang betul dengan memberi tumpuan kepada pengurusan keselamatan maklumat untuk pelajar, pengajaran; penyelidikan; dan perkhidmatan korporat. Walau bagaimanapun, sebagai kesinambungan pelaksanaan ISMS yang menggunakan standard baharu, maka pada tahun 2015, skop tertumpu kepada proses pendaftaran pelajar baharu.	**Makluman** **Tindakan : Pusat Jaminan Kualiti**
4.4	**MAKLUM BALAS PRESTASI KESELAMATAN MAKLUMAT** **4.4.1 Ketakakuran dan Tindakan Pembetulan** Mesyuarat meneliti dan mengambil perhatian: (a) ketakakuran dan tindakan pembetulan yang telah direkodkan; (b) dua (2) ketakakuran yang direkodkan adalah seperti **Lampiran 3** dan hendaklah diambil tindakan mengikut tarikh yang ditetapkan; dan (c) ketakakuran yang kedua berkaitan proses perkhidmatan yang tidak memenuhi elemen penilaian risiko melibatkan bangunan menempatkan pusat data utama, tindakan pembetulan perlu diteliti semula kerana Pembanguan Pusat Data baharu melalui peruntukan Rancangan Ke-11 belum mendapat kelulusan.	**Makluman** **Makluman dan tindakan PTJ yang bertanggungjawab seperti pada Lampiran 3** **Tindakan : Pengarah, Pusat Pembangunan Maklumat dan Komunikasi**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	Kesimpulan: Setelah menerima dan meneliti laporan yang telah dibentangkan, didapati bahawa ketakakuran telah dikenalpasti dan tindakan dilihat secara menyeluruh serta direkodkan bagi memenuhi keperluan penambahbaikan berterusan ISMS. Kesemua ketakakuran hendaklah dilaksana secara berkesan supaya dapat meningkatkan prestasi penyampaian perkhidmatan kepada pelanggan dan pemegang taruh.	
	4.4.2 Pemantauan dan Pengukuran **4.4.2.1 <u>Objektif ISMS</u>** Mesyuarat mengambil maklum berkaitan Laporan Pencapaian Objektif ISMS 2015 dan sebanyak dua (2) daripada lima (5) objektif tersebut telah diukur dan tiga (3) daripadanya hanya akan diukur pencapaian pada Sesi Kemasukan 2016/2017. Jadual laporan pencapaian adalah pada **Lampiran 4**.	**Makluman**
	4.2.2.2 <u>Pelaksanaan Kawalan di Pelan Pemulihan Risiko</u> Mesyuarat mengambil maklum perkara berikut: (a) pelaksanaan kawalan di pelan pemulihan risiko telah dilaksana oleh Pusat Pembangunan Maklumat dan Komunikasi dengan kerjasama Peneraju Proses Pendaftaran Pelajar Baharu; (b) keseluruhan aset yang telah dinilai berdasarkan kerahsiaan, integriti dan ketersediaan (CIA) adalah sebanyak 566 aset berasaskan tiga (3) kategori nilai risiko (*risk value*) iaitu *low*, *medium* dan *high*; dan (c) laporan ringkas analisis penilaian risiko tahun 2015 adalah seperti **Lampiran 5**. <u>Kesimpulan:</u> Setelah meneliti laporan, objektif ISMS telah disesuaikan dengan keperluan standard baharu serta memenuhi sasaran dan sebahagiannya akan diukur pada Sesi Kemasukan 2016/2017. Manakala pelaksanaan kawalan bagi pemulihan risiko telah dikenalpasti dan diukur keberkesanannya berdasarkan keperluan.	**Makluman** **Makluman** **Makluman**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
4.5	**PENEMUAN AUDIT**	
	4.5.1 <u>Audit Pemantauan Semakan 2 (SIRIM)</u> Mesyuarat mengambil maklum pembentangan penemuan Audit Pemantauan Semakan 2 ISMS oleh SIRIM yang telah dilaksana pada 29 dan 30 Januari 2015 sebagaimana berikut:	
	(a) seramai empat (4) orang juruaudit telah terlibat bagi mengaudit skop Operasi Pusat Data yang meliputi Aplikasi Laman Sesawang UPM, Sistem Pengurusan Kewangan, Pengurusan Sumber Manusia dan Sistem Maklumat Pelajar;	**Makluman**
	(b) hasil audit terdapat lapan (8) ketakakuran minor telah ditemui dan 10 peluang penambahbaikan telah dicadangkan;	**Makluman**
	(c) bukti penutupan ketakakuran dan tiga (3) cadangan peluang penambahbaikan telah dikemuka kepada SIRIM pada 30 April 2015, dan pihak SIRIM telah mengesahkan penutupan tersebut;	**Makluman**
	(d) cadangan peluang penambahbaikan akan disemak oleh SIRIM pada Audit Pensijilan Semula; dan	**Tindakan : Pusat Pembangunan Maklumat Dan Komunikasi**
	(e) syor keseluruhan pihak yang terlibat dengan skop ISMS terkini hendaklah melihat semua ketakakuran yang berlaku dan memastikan ianya tidak berulang semasa Audit Pensijilan Semula. Pejabat Pembangunan Maklumat dan Komunikasi hendaklah mengambil tindakan pada setiap peluang penambahbaikan yang telah dikemukakan oleh SIRIM. Begitu juga pihak yang terlibat dengan skop terkini ISMS hendaklah meneliti dan melaksana peluang penambahbaikan yang dikemuka oleh SIRIM bagi yang berkaitan dengan skop semasa; dan	**Tindakan : Peneraju Proses Skop Baharu dan Pusat Pembangunan Maklumat dan Komunikasi**
	(f) laporan penemuan adalah pada **Lampiran 6**.	**Makluman**
	4.5.2 <u>Audit Dalaman</u> Mesyuarat mengambil maklum pembentangan penemuan Audit Dalaman UPM yang dilaksana pada 18 dan 19 November 2015 sebagaimana berikut:	**Makluman**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	(a) Audit Dalaman dilaksana bagi menentukan sama ada UPM melaksanakan pengurusan keselamatan maklumat berdasarkan keperluan Standard MS ISO/IEC 27001:2013 dengan efektif selaras dengan Peraturan Keselamatan ICT UPM serta objektif dan sasaran ISMS UPM, dan bersedia untuk menghadapi Audit Pensijilan Semula oleh Badan Pensijilan;	**Makluman**
	(b) Audit Dalaman dijalankan mengikut skop ISMS UPM yang hanya melibatkan proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra dalam Sistem Maklumat Pelajar (SMP), Pengoperasian Pusat Data bagi proses Pendaftaran Pelajar Baharu Prasiswazah dan Pengoperasian Pusat Pemulihan Bencana bagi proses Pendaftaran Pelajar Baharu Prasiswazah;	**Makluman**
	(c) 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;	
	(d) hasil audit terdapat tiga (3) ketakakuran dan 14 cadangan peluang penambahbaikan;	
	(e) semua ketakakuran telah dikenalpasti pembetulan, punca penyebab, tindakan pembetulan serta tarikh tindakan yang patut diambil dan antara cadangan peluang penambaikan yang perlu diambil tindakan adalah pindaan ayat pada skop; dan	**Tindakan: PTJ yang telah menerima ketakakuran dan cadangan peluang penambahbaikan**
	(f) keseluruhan laporan adalah pada **Lampiran 7**.	**Makluman**
	<u>Kesimpulan:</u> Audit Pemantauan dan Audit Dalaman telah dilaksana mengikut perancangan dan penemuan telah diambil tindakan. Secara keseluruhan, UPM telah melaksana ISMS dengan baik dan peluang penambahbaikan yang dicadangkan hendaklah diberi perhatian bagi menambahbaik pelaksanaan ISMS di UPM. Ketakakuran yang dikeluarkan oleh Pasukan Audit, hendaklah sentiasa dipantau supaya tidak berulang.	
4.6	**MAKLUM BALAS PEMEGANG TARUH** Mesyuarat mengambil maklum Laporan keberkesanan 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 sebagaimana berikut:	

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	(a) kumpulan sasaran adalah pemilik dan pelaksana proses yang terlibat iaitu 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 dalam Pusat Pembangunan Maklumat dan Komunikasi;	**Makluman**
	(b) tujuan kajian untuk mengetahui tahap pengetahuan, kefahaman dan penerimaan terhadap pelaksanaan ISMS yang melibatkan operasi dan perkhidmatan entiti yang berkaitan pelaksanaan ISMS;	**Makluman**
	(c) hasil 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;	**Makluman**
	(d) maklum balas pemegang taruh 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;	**Makluman**
	(e) secara khususnya, staf yang terlibat dengan proses dan perkhidmatan yang berkaitan perlu diberi pemahaman asas keselamatan data secara komprehensif;	**Makluman**
	(f) 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; dan	**Tindakan: Bahagian Hal Ehwal Pelajar/Kolej**
	(g) laporan keberkesanan 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 adalah seperti **Lampiran 8**.	**Makluman**
	Mesyuarat bersetuju agar kajian ini diteliti semula dengan mengambil kira jumlah responden serta penentuan skala.	**Tindakan: Pusat Pembangunan Maklumat dan Komunikasi**
	<u>Kesimpulan:</u> Kajian keberkesanan ISMS dalam kalangan Peneraju Proses yang terlibat semasa pendaftaran pelajar baharu serta pengoperasian Sistem Maklumat Pelajar (SMP) di Universiti Putra Malaysia telah dilaksana dan dianalisa.	

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	Bagi menambah baik hasil kajian serta mendapat maklum balas pemegang taruh dan melihat keberkesanan proses pendaftaran pelajar dari segi aspek ISMS, kajian akan dilaksana pada Sesi Kemasukan 2016/2017 terhadap ibubapa atau penjaga dan pelajar baharu semasa hari pendaftaran.	
4.7	**HASIL PENILAIAN RISIKO DAN STATUS PELAN PEMULIHAN RISIKO** Mesyuarat mengambil maklum berkaitan hasil penilaian risiko dan status pelan pemulihan risiko seperti berikut: (a) penilaian risiko telah dilaksanakan oleh Pusat Pembangunan Maklumat dan Komunikasi dengan kerjasama Pentadbir Proses Universiti yang terlibat sejak tahun 2015; (b) penilaian risiko dilaksana menggunakan Sistem Aplikasi Malaysia Risk Assessment Methodology (MyRAM) yang telah dibangunkan oleh pihak Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU); (c) keperluan penilaian risiko dalam pelaksanaan ISMS adalah berdasarkan standard MS ISO/IEC 27001:2013; (d) output penilaian risiko bagi aset yang berjumlah 566 adalah: i) aset yang berisiko tinggi sebanyak 12 (1%) , ii) aset beridiko sederhana 260 (22.9%) dan iii) aset berisiko rendah adalah 865 (76.1%); (e) Laporan ringkas hasil penilaian risiko tahun 2014 adalah sebagaimana pada **Lampiran 9**. Mesyuarat bersetuju agar: (a) meneliti semula pelan pemulihan berkaitan pembayaran yuran pendaftaran secara tunai yang mana pelan pemulihan sifar adalah terlalu drastik untuk diturunkan memandangkan masih terdapat ibubapa yang masih membayar secara tunai dengan mengambil kira pelbagai sebab yang dianggap munasabah; dan (f) melihat semula cadangan lokasi pusat data jika peruntukan Rancagan Malaysia Ke-11 tidak meluluskan bajet bagi lokasi pusat data baharu.	**Makluman** **Makluman** **Makluman** **Makluman** **Makluman** **Tindakan: Pejabat Bursar** **Tindakan: Pejabat Pembangunan Maklumat dan Komunikasi**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	Kesimpulan: Setelah menerima dan meneliti laporan yang dibentangkan, didapati Penilaian Risiko dan Status Pelan Pemulihan Risiko telah dilaksana secara berkala di mana yang terkini pada Ogos 2015 dan telah memenuhi keperluan ISMS. Pasukan Penilaian Risiko hendaklah sentiasa melaksana penilaian secara berterusan bagi memastikan kualiti keselamatan maklumat sentiasa di tahap maksimum.	
4.8	**PELUANG PENAMBAHBAIKAN** Mesyuarat mengambil maklum tiga (3) peluang penambahbaikan yang telah dikenalpasti dalam pelaksanaan Sistem Pengurusan Keselamatan Maklumat ISO/IEC 27001:2013 sebagaimana pada **Lampiran 10**. Kesimpulan: Setelah menerima dan mengkaji semula laporan, diputuskan bahawa UPM telah mengenalpasti dan merancang tindakan untuk menambahbaik dan meningkatkan prestasi penyampaian perkhidmatan serta tahap kepuasan pemegang taruh. Hasil Peluang Penambahbaikan akan dibincang pada MKSP akan datang.	**Tindakan : Pejabat Bursar, Bahagian Kemasukan, Bahagian Hal Ehwal Pelajar dan Pusat Pembangunan Maklumat dan Komunikasi**
4.9	**HAL-HAL LAIN** **Audit Pensijilan Semula** Mesyuarat mengambil maklum dan bersetuju berkaitan Audit Pensijilan Semula ISMS oleh SIRIM seperti berikut: (a) UPM akan menghadapi Audit Pensijilan Semula pada 8 hingga 10 Disember 2015; (b) seramai tiga (3) orang Juruaudit akan hadir dan diketuai oleh Cik Efizan Zamri; (c) UPM masih belum menerima jadual audit oleh pihak SIRIM; (d) Pusat Tanggungjawab yang terlibat iaitu Bahagian Hal Ehwal Pelajar, Kolej, Pejabat Bursar, Perpustakaan Sultan Abdul Samad, Bahagian Keselamatan, Pejabat Strategi Korporat dan Komunikasi, Pusat Pembangunan Maklumat dan Komunikasi, Bahagian Kemasukan dan Tadbir Urus Akademik, Pusat Jaminan Kualiti dan Pejabat Penasihat Undang-Undang; dan	**Makluman** **Makluman** **Makluman** **Makluman**

MINIT	AGENDA / CATATAN	TINDAKAN/ MAKLUMAN
	(e) Cuti rehat dibekukan dan PTJ hendaklah bersedia menghadapi audit tersebut.	**Tindakan : PTJ yang berkaitan**
	KESIMPULAN KESELURUHAN Mesyuarat bersetuju: (a) secara keseluruhannya, didapati bahawa skop ISMS yang dipinda adalah bersesuaian dengan fokus utama Universiti dalam melindungi maklumat dengan mengambil kira isu dalaman dan luaran serta akan diperluaskan dari semasa ke semasa mengikut keperluan hala tuju ISMS Universiti; (b) UPM berupaya mengekalkan pensijilan ISMS yang kini dilaksanakan di bawah skop baharu MS ISO/IEC 27001:2013; dan (c) Pensijilan ISMS di UPM akan menjamin keselamatan maklumat yang merangkumi aspek kerahsiaan, integriti, dan ketersediaan sejajar dengan objektif keselamatan ICT sektor awam.	**Makluman**
	PENANGGUHAN Mesyuarat tamat pada jam 12.05 tengah hari dengan ucapan terima kasih daripada Pengerusi.	

LAMPIRAN A

SENARAI KEHADIRAN
MESYUARAT KAJIAN SEMULA PENGURUSAN (MKSP)
SISTEM PENGURUSAN KESELAMATAN MAKLUMAT

Tarikh : 27 November 2015 (Jumaat)
Masa : 10.30 Pagi
Tempat : Bilik Mesyuarat Utama, Fakulti Perubatan dan Sains Kesihatan

Hadir

1. YBhg. Profesor Dato' Dr. Mohd. Fauzi Hj. Ramlan **– Pengerusi**
2. YBhg. Profesor Dr. M. Iqbal Saripan – Wakil Pengurusan
3. Encik Mohd. Faizal Daud – Timbalan Wakil Pengurusan ISMS
4. YBhg. Profesor Datuk Dr. Mad Nasir Shamsudin
5. YBhg. Profesor Dato' Dr. Mohd. Azmi Mohd. Lila
6. Ybhg. Wan Azman Wan Omar
7. Encik Zulkiflee Othman
8. YBhg. Profesor Dr. Mohamed Zakaria bin Hussin
9. YBhg. Profesor Dr. Mohd. Hair bin Bejo
10. YBhg. Profesor Dr. Zulkornain bin Yusop
11. YBhg. Profesor Dr. Ab. Rahim bin Bakar
12. YBhg. Profesor Dr. Zainal Abidin bin Talib
13. YBhg. Profesor Dr. Hasanah binti Mohd. Ghazali
14. YBhg. Profesor Dr. Zaid bin Ahmad
15. Profesor Madya Dr. Abu Bakar bin Md. Sultan
16. Profesor Madya Dr. Ramdzani bin Abdullah
17. Profesor Madya Dr. Nur Ashikin Psyquay Abdullah
18. Profesor Madya Dr. Fatimah binti Sidi
19. YBhg. Profesor Dr. Khozirah binti Shaari
20. Tuan Haji Anuar bin Haji Ahmad
21. Dr. Khairulmazmi bin Ahmad
22. Dr. Abdul Razak bin Abdul Rahman
23. Dr. Paiman bin Bawon
24. Profesor Madya Dr. Haji Jamaludin bin Haji Ahmad
25. Dr. Mohd Ibrani Shahrimin Adan Assim

26. YBhg. Profesor Dr. Mohd. Roslan bin Sulaiman
27. Dr. Yahaya bin Abu Ahmad
28. Dr. Mohamad Amran bin Mohd. Salleh
29. Encik Mohd. Nazri bin Md. Yassin
30. Tuan Haji Rosdi bin Wah
31. Encik Anuar Shah bin Bali Mahomed
32. Tuan Haji Hashim bin Md. Shari
33. Encik Rosmi bin Othman
34. Tuan Haji Mokhtar bin Dahari
35. Encik Julbakar bin Tajudin
36. Tuan Haji Abdul Ghaffar bin Othman
37. Tuan Haji Suhaifi bin Sulaiman
38. Encik Mohd. Nazri bin Noh
39. Encik Mustafa bin Che Ali
40. Encik Mustaffa bin Haji Dollah
41. Encik Asbullah bin Mohd. Yusof
42. Puan Fairuz binti Muchtar
43. Puan Azarizam Ali
44. Encik Ab. Malek bin Simon
45. Encik Mohammad Azlan bin Ali Basah
46. Encik Mhd. Hussin bin Abd. Rahim
47. Encik Sudirman bin Asmadi
48. Tuan Haji Jamsari bin Tamsir
49. Encik Din bin Ayup
50. Encik Zamre bin Yaacob
51. Puan Sarah Salwah binti Adnan
52. Puan Noraihan Noordin
53. Puan Rozi Tamin
54. Encik Fahmi Azar bin Mistar
55. Puan Mazitah Ahmad
56. Puan Noorizai Mohamad Noor **- Setiausaha**

Tidak hadir dengan Kenyataan

1. YBhg. Profesor Dr.–Ing. Ir. Renuganth Varatharajoo
2. YBhg. Profesor Dato' Dr. Mohammad Shatar bin Sabran
3. Profesor Madya Dr. Rozanah binti Ab. Rahman
4. YBhg. Profesor Datin Paduka Dr. Aini binti Ideris
5. YBhg. Profesor Dr. Abdul Shukor bin Juraimi
6. Profesor Madya Ir. Dr. Azmi bin Dato' Yahya
7. Profesor Madya Dr. Abdul Mua'ti @ Zamri bin Ahmad
8. Profesor Madya Lar. Dr. Osman bin Mohd. Tahir
9. YBhg. Profesor Dr. Abdul Jalil bin Nordin
10. YBhg. Profesor Datin Paduka Dr. Khatijah binti Yusoff
11. YBhg. Profesor Dr. Bujang Kim Huat
12. YBhg. Profesor Dr. Abdul Rahman bin Omar
13. YBhg. Prof. Dr. Nor Azah Yusof
14. Y.M. Profesor Dr. Tengku Aizan binti Tengku Abdul Hamid
15. YBhg. Profesor Dato' Dr. Kamel Ariffin bin Mohd. Atan
16. Profesor Madya Dr. Shaufique Fahmi Ahmad Sidique
17. YBhg. Profesor Dato' Dr. Mohd. Yazid bin Abd. Manap
18. YBhg. Profesor Dr. Turiman bin Suandi
19. YBhg. Profesor Dr. Zulkifli bin Idrus
20. YBhg. Profesor Dr. Mohd. Khanif bin Yusop
21. YBhg. Profesor Dr. Shamala a/p K. Subramaniam
22. Profesor Madya Dr. Hawa Ze Jaafar
23. YBhg. Profesor Dr. Paridah binti Md. Tahir
24. YBhg. Profesor Dr. Mahiran binti Basri
25. YBhg. Profesor Dr. Aida Suraya binti Haji Md. Yunus
26. Profesor Madya Dr. Mohd. Bakri bin Haji Ishak
27. Profesor Madya Dr. Abdul Rasid bin Jamian
28. Dr. Razali bin Othman
29. Profesor Madya Dr. Zulhamri bin Abdullah
30. Dr. Fathinul Fikri Ahmad Saad
31. YBhg. Profesor Dr. Latifah binti A. Latiff
32. YBhg. Profesor Dr. Aziz bin Arshad
33. Profesor Madya Arshad Abd Samad

34. Profesor Madya Dr. Azizan bin Asmuni
35. Puan Chek Zan binti Kasah
36. Dr. Mohd. Rafee bin Baharudin
37. Supt. Md Zamri bin Mat Zanu
38. YBhg. Profesor Dr. Japar Sidik bin Bujang
39. YBhg. Profesor Madya Dr. Samsilah binti Roslan
40. Dr. Saidon bin Amri
41. Dr. Amini Amir bin Abdullah
42. Lt. Kolonel Othman bin Jailani
43. Profesor Madya Dr. Pakhriazad bin Hassan Zaki
44. Profesor Madya Dr. Farinazleen binti Mohamad Ghazali
45. Profesor Madya Dr. Mohamad Azani bin Haji Alias
46. Puan Iza Dura binti Abdul Manan
47. Profesor Madya Dr. Faieza binti Abdul Aziz
48. Dr. Omrah bin Hassan @ Hussin
49. Profesor Madya Dr. Zulkiflle bin Leman
50. Profesor Madya Dr. Arifin bin Abdu
51. Puan Zainora binti Abdul Talib
52. Puan Kamariah binti Mohd. Saidin
53. Dr. Hanafiah bin Ayub
54. Puan Nor Adida binti Ab. Khalid
55. Puan Rohani bt. Abdul Latiff
56. Puan Siti Rozana binti Supian
57. Puan Rosmala binti Abd. Rahim
58. Encik Ahmad Nizam bin Abdullah
59. Tuan Haji Mohd. Nizan bin Jaafar
60. Puan Hasliza binti Zakaria
61. Encik Roslan bin Parjo
62. Encik Wan Mohd. Radzi bin Wan Ismail
63. Dr. Haji Latif bin Anwar
64. Encik Abd. Razak bin Ahmad
65. Encik Muhammad Adil bin Ahmad Tajuddin
66. Tuan Haji Amran bin Zakaria
67. Puan Zainaf binti Udin
68. Encik Shahriman bin Hashim

69. Tuan Haji Mohd. Aris Fadzilah bin Hj. Abdullah
70. Encik Amiruddin bin Abdul Aziz
71. Puan Joliah binti Hussin
72. Puan Wan Rohani binti Wan Mohamed
73. Puan Wan Nahariah binti Wan Tahir
74. Puan Nor Baizura binti Zamri
75. Cik Aidawati binti Ramali
76. Puan Salmee Suhana binti Hashim
77. Encik Muhazam Mansor
78. Puan Suhana Md Chairi
79. Encik Mohamed Farid Harun
80. Encik Mohd Zul Mohd Yusoff
81. Encik Syemsul bin Bahrim
82. Dr. Suhyna Mohamad Sulaiman

Turut Hadir

1. Encik Mohd Aizat Azmi (Wakil Penasihat Undang-Undang)
2. Prof. Madya Dr. Halimi Mohd Saud (Wakil Dekan Fakulti Pertanian)
3. Encik Mohd Radzi Mahidin (Wakil Dekan Fakulti Bioteknologi dan Sains Biomolekul)
4. Encik Nasrudin Yahya (Wakil Pengarah Pusat Pengimejan Diagnostik Nuklear)
5. Encik Mohd Naim Mohd Ishak
   (Wakil Pengarah Pejabat Pengurusan Keselamatan dan Kesihatan)
6. Encik Mustafa Kamal Tahir (Wakil Pengarah Pejabat Strategi Korporat dan Komunikasi)
7. Puan Zainor Mazwin Zainal (Wakil Pengetua Kolej Pendeta Za'ba)
8. Encik Mohd Azis Abdullah (Wakil Ketua Audit Dalam)
9. Dr. Fauziah Adnan
10. Wan Zaharuddin Wan Abdullah (Wakil Ketua Pusat Sukan)
11. Puan Mastura binti Abd. Rahim (Wakil TWP Pejabat Bursar)
12. Encik Muzaffar Shah Kassim (Wakil TWP Perpustakaan Sultan Abdul Samad)
13. Puan Dianna Watty Ibrahim (Wakil TWP Penerbit)
14. Encik Nur Anwar Hilmi (Wakil TWP Penerbit)
15. Encik Mohd Khairi Hasan (Wakit TWP Fakulti Perubatan dan Sains Kesihatan)
16. Puan Nor Azlida Aminudin (Wakil TWP Institut Penyelidikan Matematik)
17. Encik Norman Azlan Osman (Wakil Peneraju Latihan)
18. Encik Mat Razi Abdullah
19. Puan Nurul Fatihah Md Marham
20. Encik Krishnan Mariappan
21. Matron Maznah Mohamad (Wakil Peneraju PKU ISMS)

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

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>

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	

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	

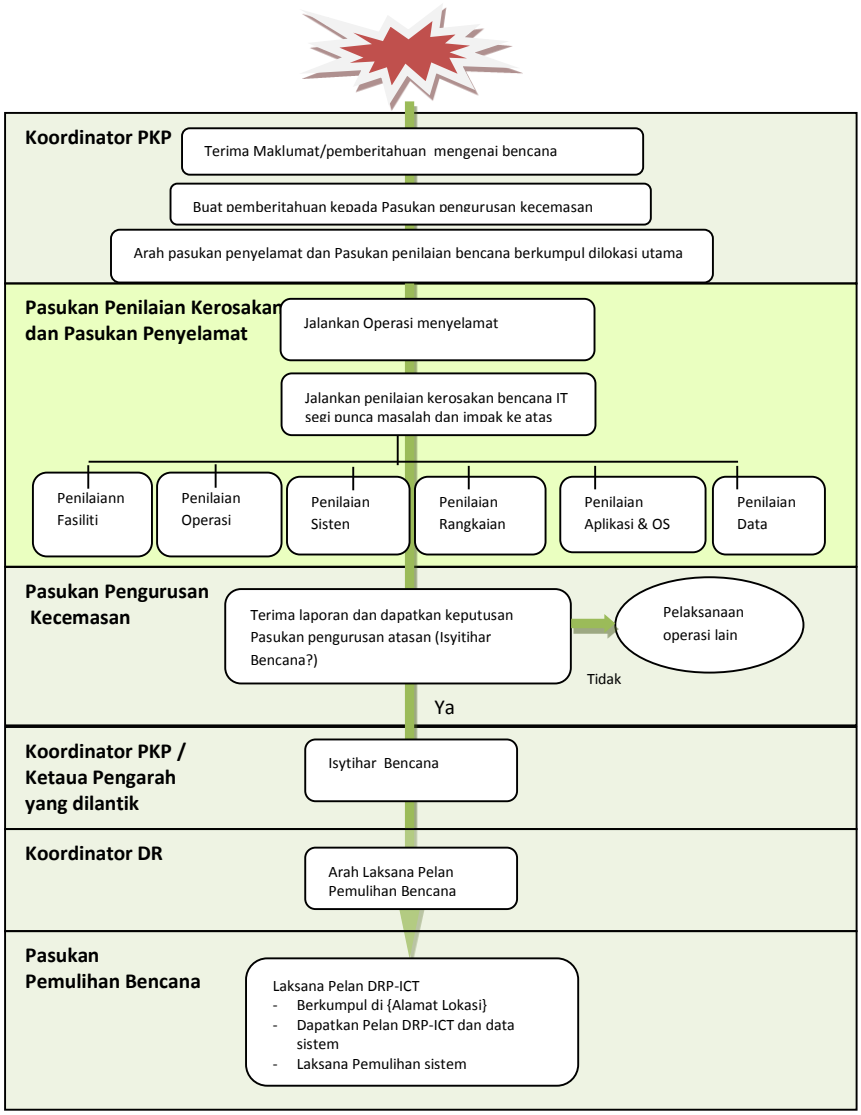
6. HASIL PENEMUAN SIMULASI DRP ICT 23 OKTOBER 2015

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

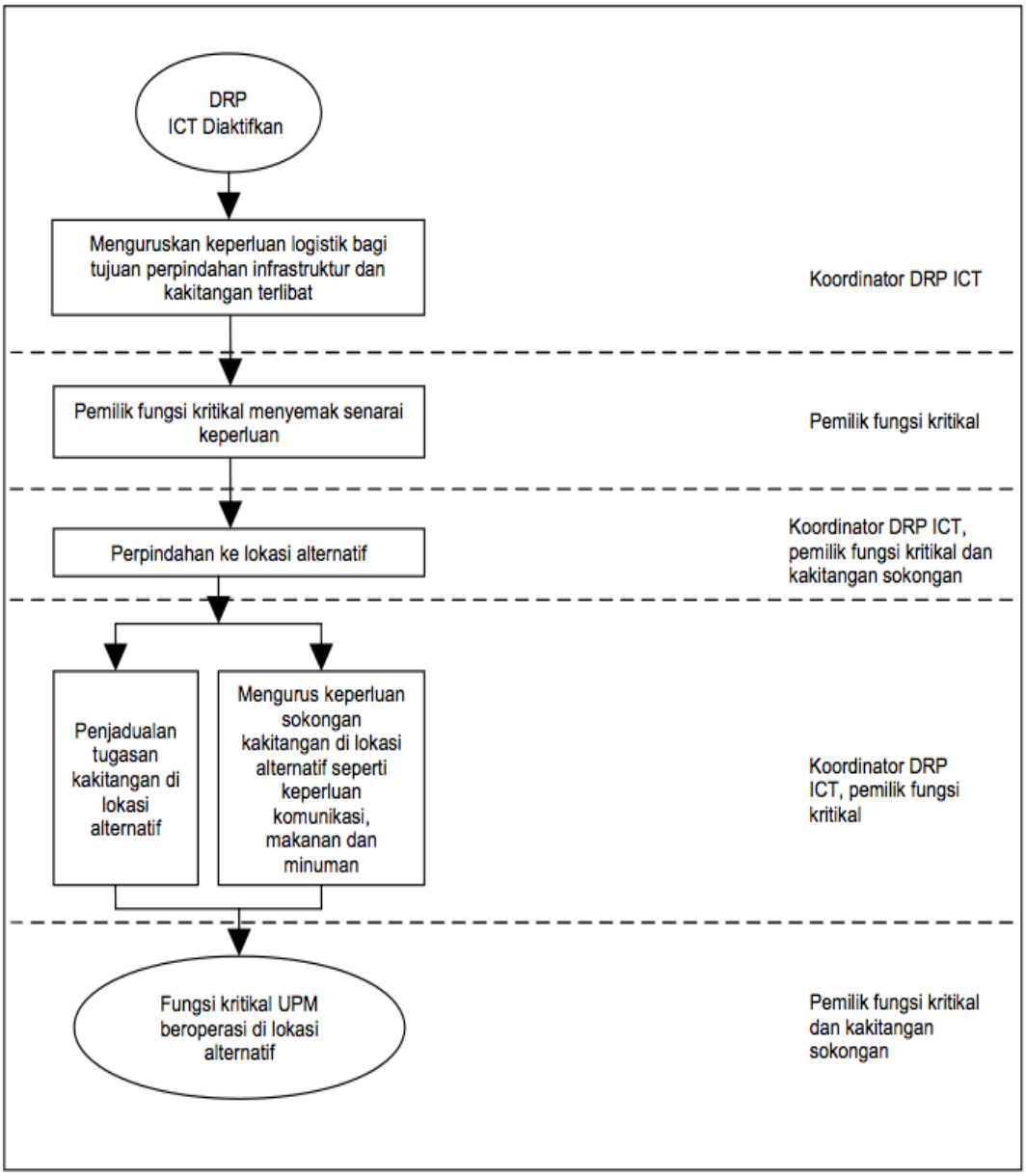
Penilaian gangguan dan penentuan tindakan yang boleh menentukan kepada pengaktifan Pelan DRP-ICT UPM

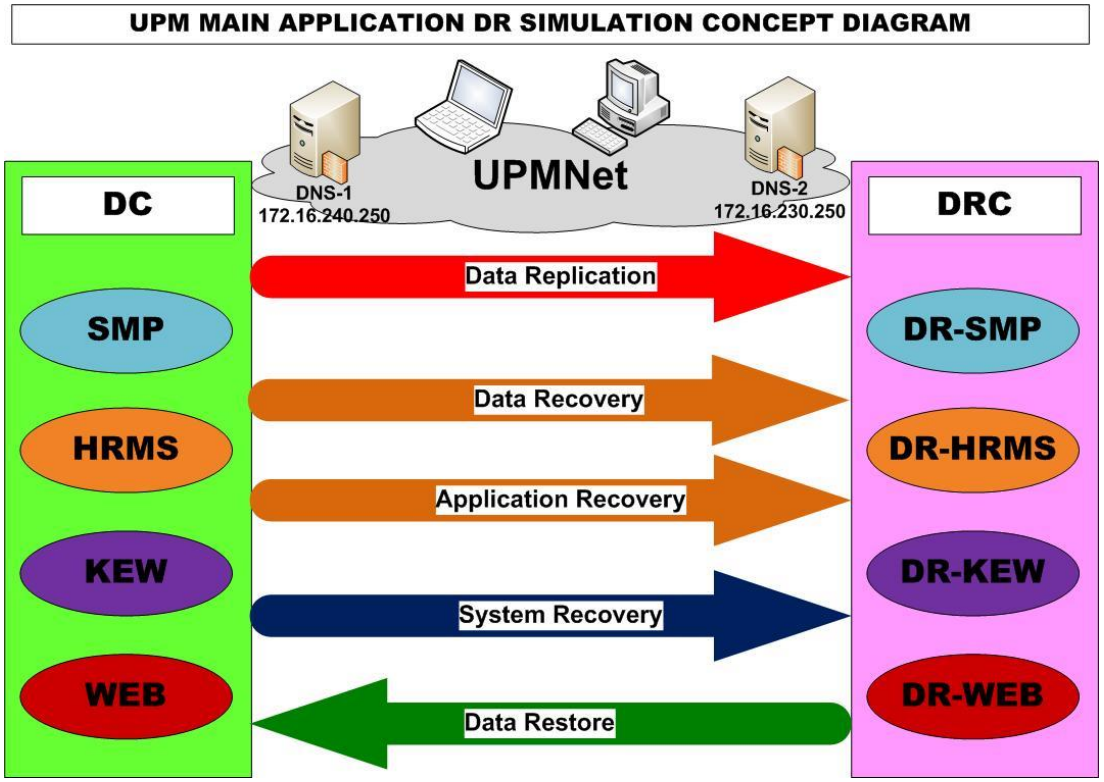
Semua ahli dalam pasukan pemulihan Bencana akan bersedia dengan Pelan DRP sistem aplikasi masing-masing.

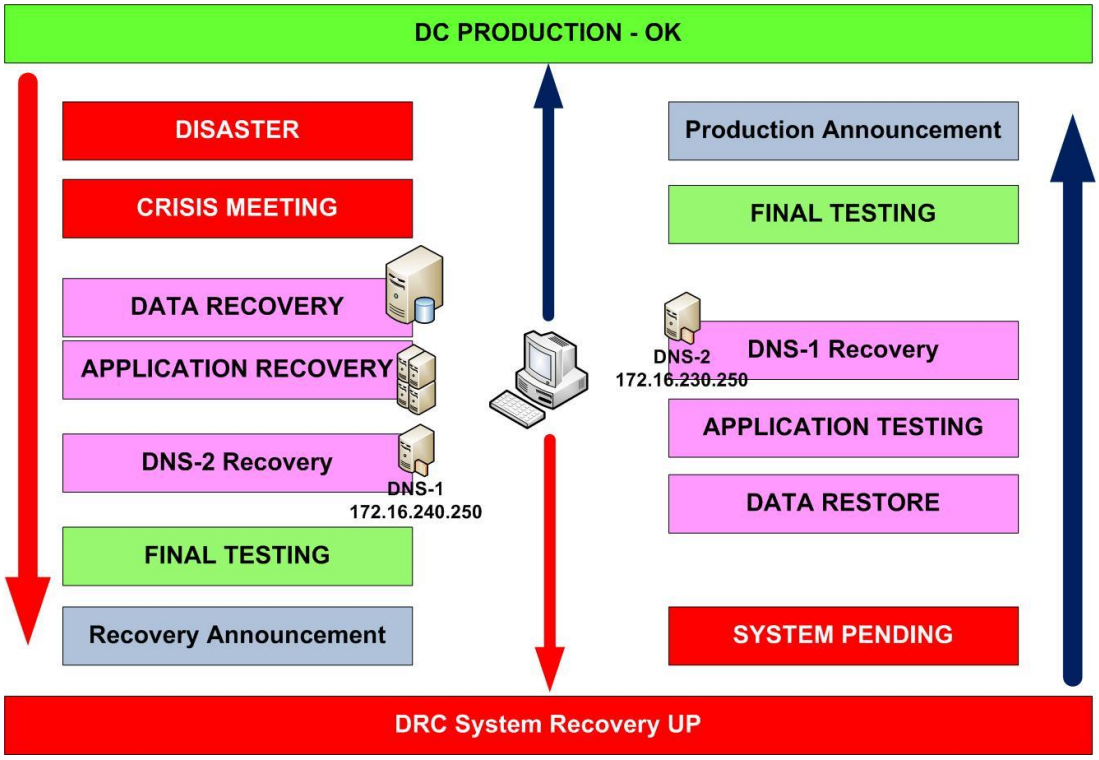
LAMPIRAN 2

FASA PEMULIHAN

Rajah 1: Proses-proses Dalam Fasa Pemulihan



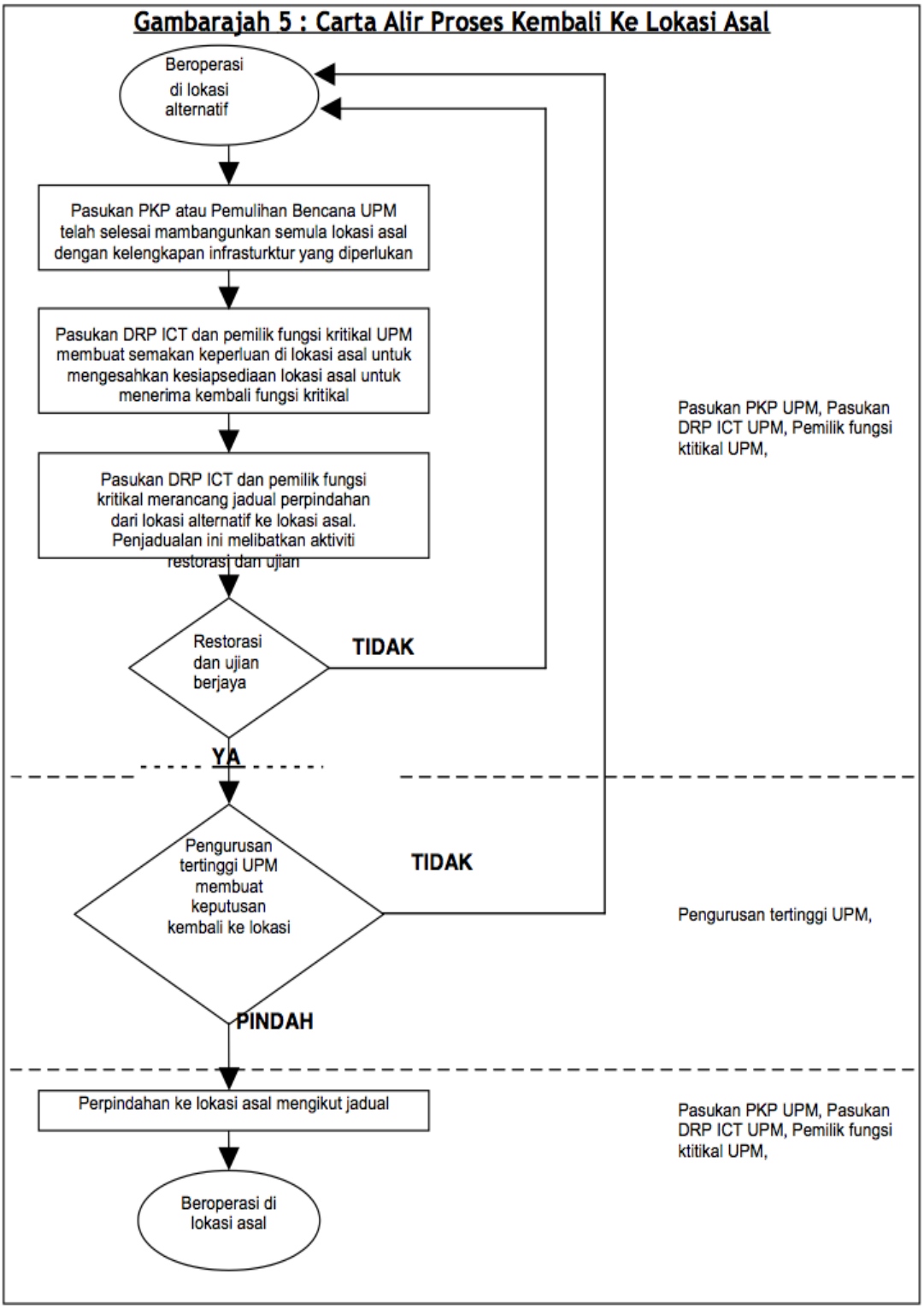

UPM MAIN APPLICATION DR SIMULATION CONCEPT DIAGRAM
UPMNet
DNS-1
172.16.240.250
DNS-2
172.16.230.250
DC
DRC
Data Replication
SMP
DR-SMP
Data Recovery
HRMS
DR-HRMS
Application Recovery
KEW
DR-KEW
System Recovery
WEB
DR-WEB
Data Restore


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



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	

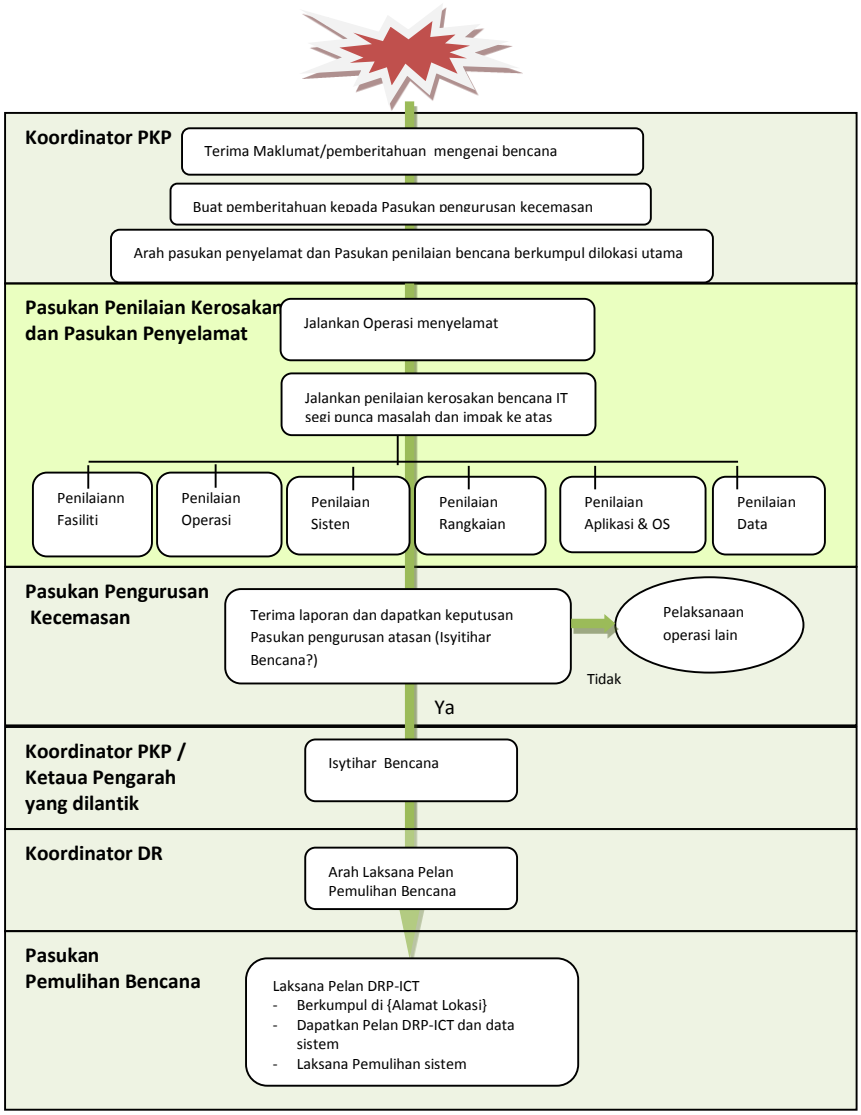
6. HASIL PENEMUAN SIMULASI DRP ICT 23 OKTOBER 2015

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

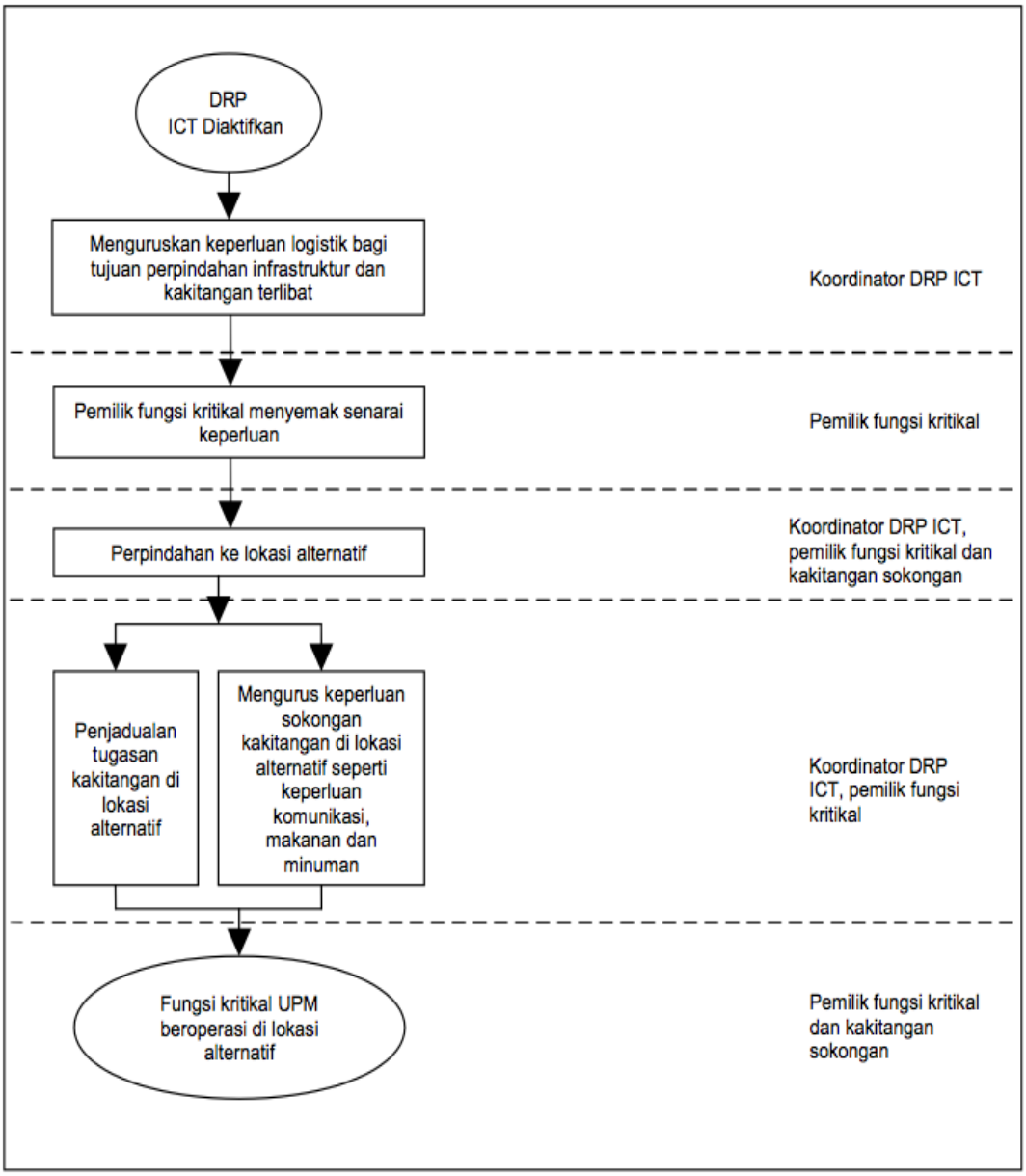
Penilaian gangguan dan penentuan tindakan yang boleh menentukan kepada pengaktifan Pelan DRP-ICT UPM

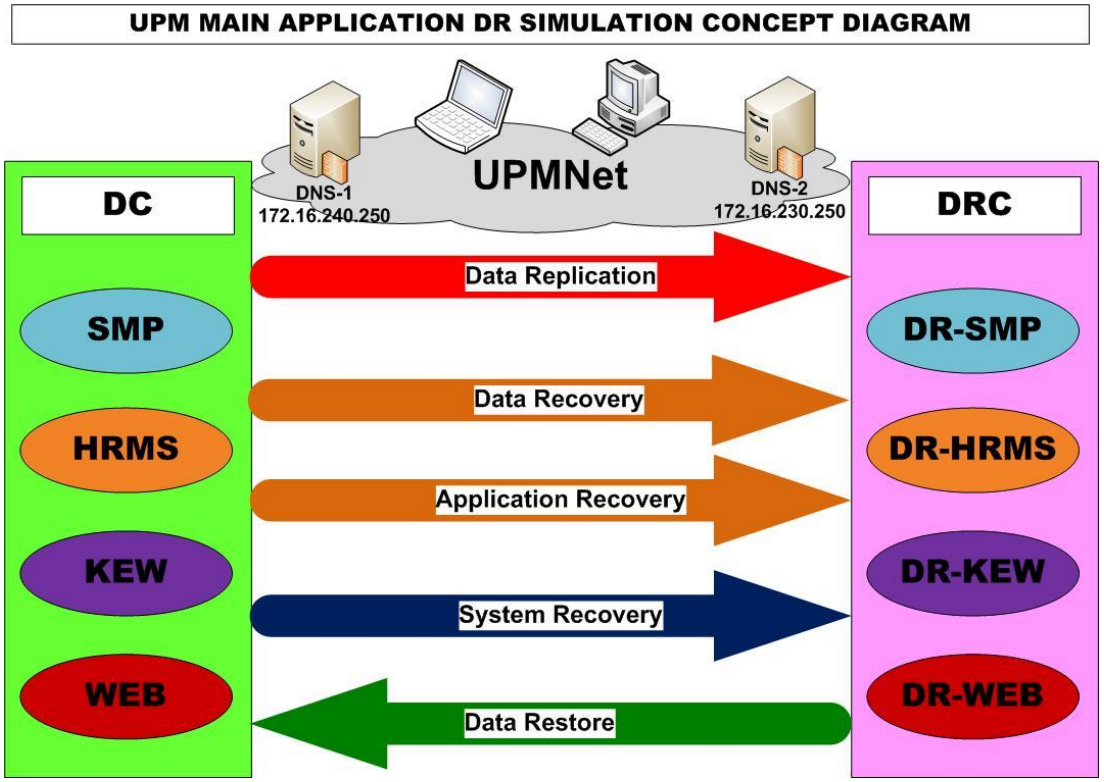
Semua ahli dalam pasukan pemulihan Bencana akan bersedia dengan Pelan DRP sistem aplikasi masing-masing.

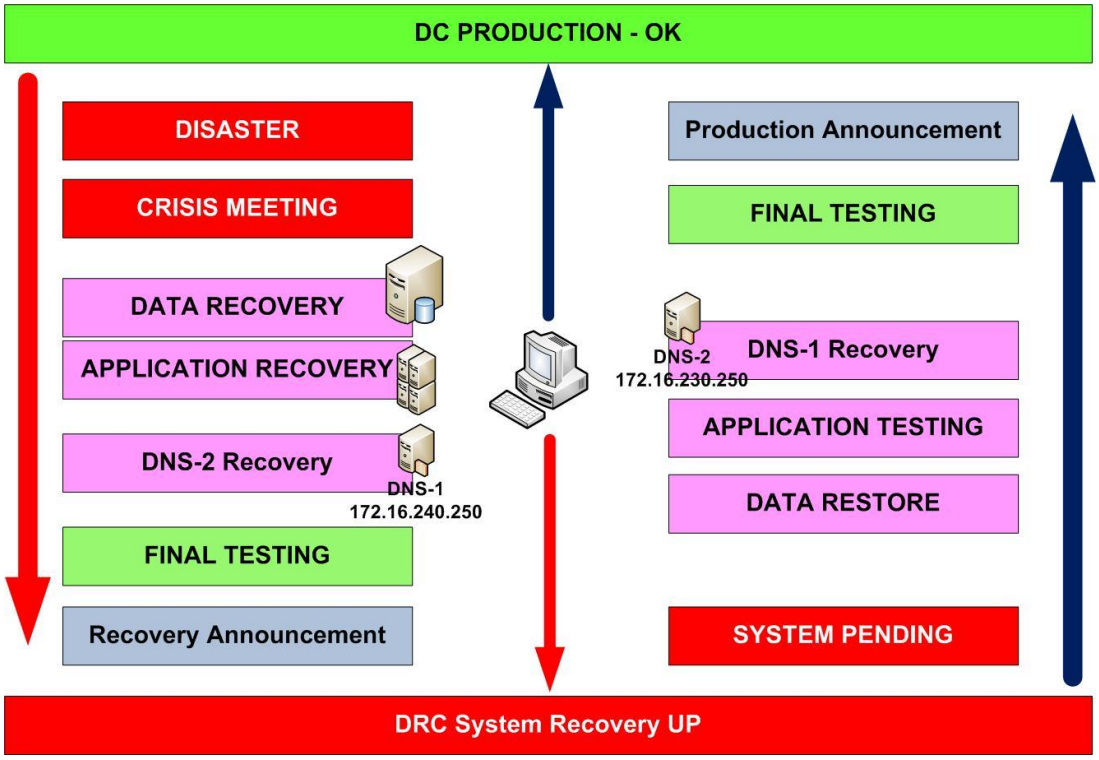
LAMPIRAN 2

FASA PEMULIHAN

Rajah 1: Proses-proses Dalam Fasa Pemulihan



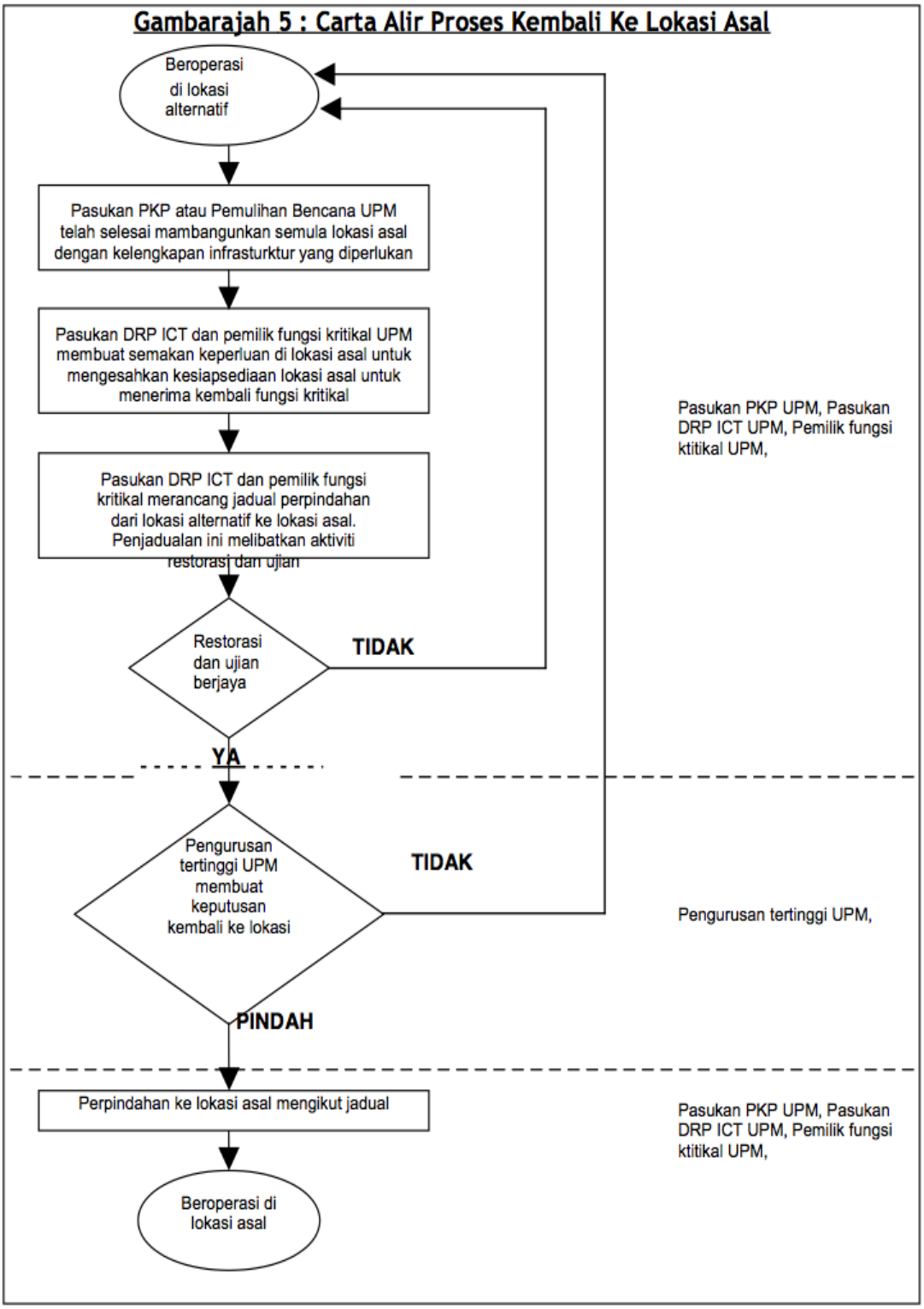

UPM MAIN APPLICATION DR SIMULATION CONCEPT DIAGRAM
UPMNet
DNS-1
172.16.240.250
DNS-2
172.16.230.250
DC
DRC
Data Replication
SMP
DR-SMP
Data Recovery
HRMS
DR-HRMS
Application Recovery
KEW
DR-KEW
System Recovery
WEB
DR-WEB
Data Restore


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.

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

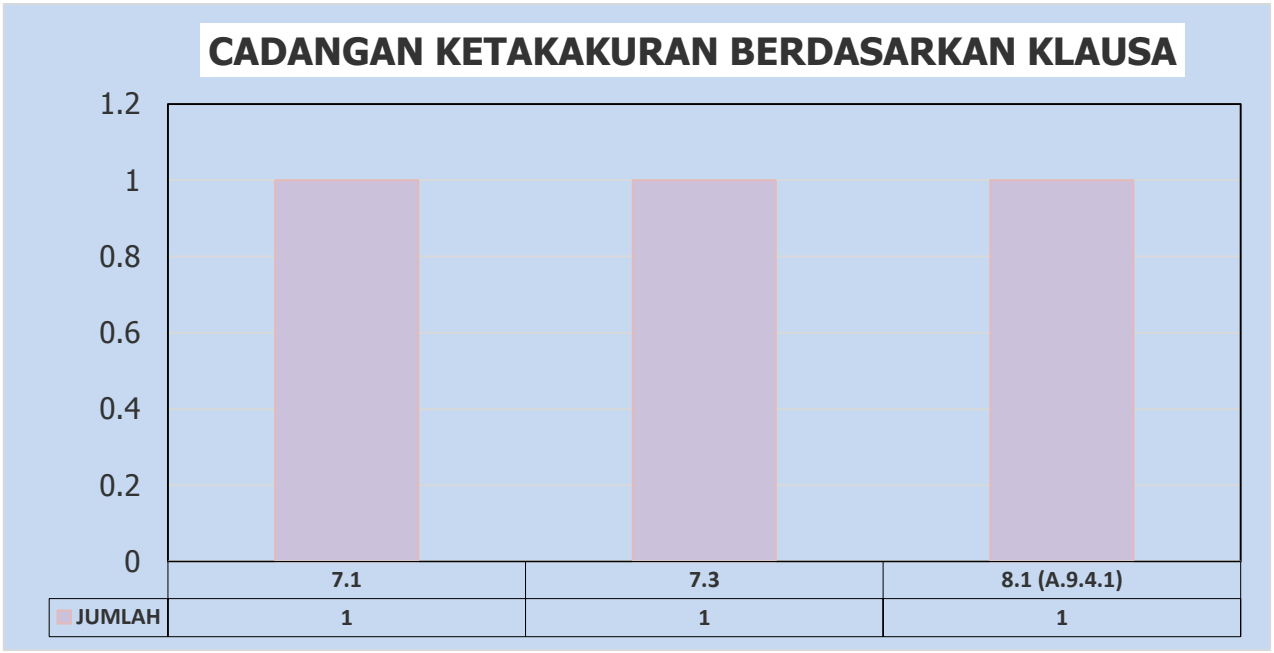
Hasil dari proses audit dalaman yang telah dijalankan, ketakakuran yang ditemui adalah menjurus kepada sumber, tahap kesedaran serta perancangan dan kawalan operasi.

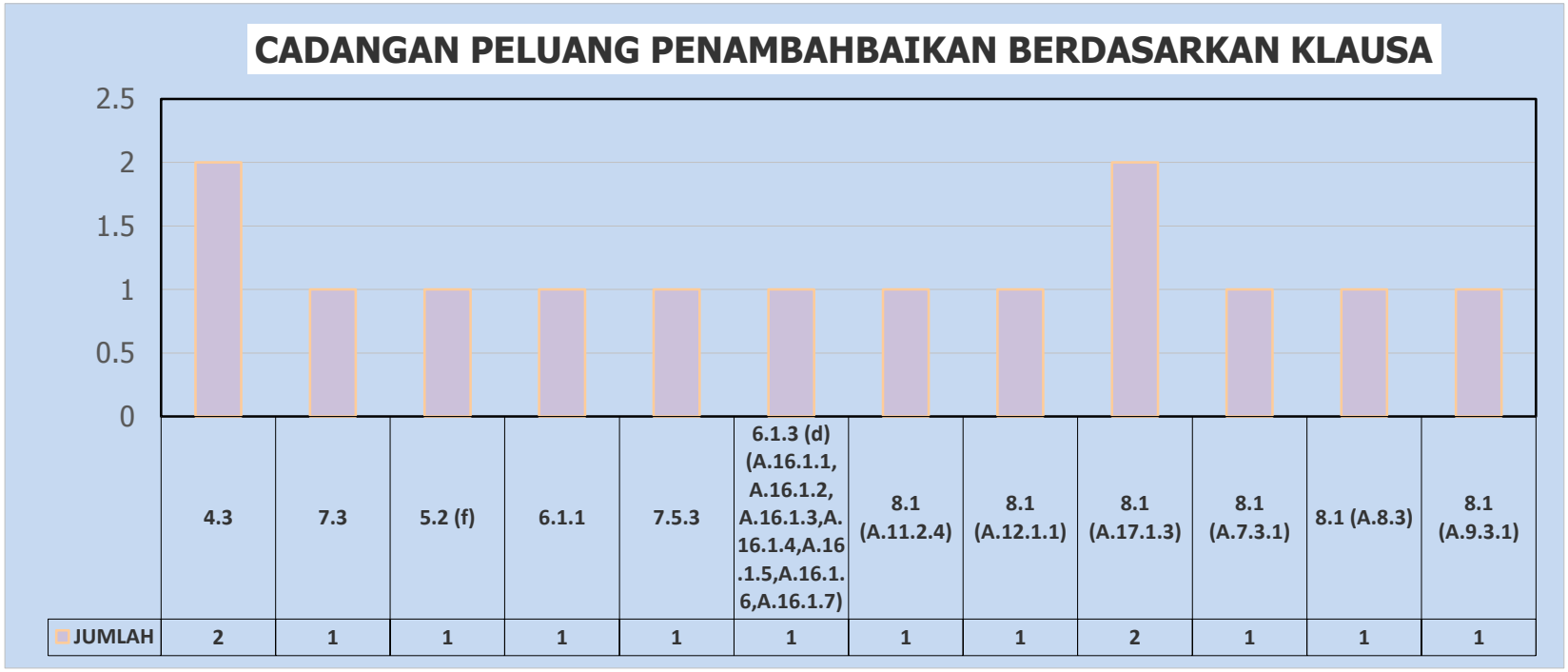
Dari segi perlaksanaan ISMS, Universiti Putra Malaysia adalah bersedia untuk diaudit oleh badan pensijilan tertakluk kepada tindakan pembetulan yang berkesan diambil terhadap ketakakuran yang ditemui dalam masa yang telah ditetapkan.

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

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%

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 (sistem pengoperasian (OS) yang telah luput) yang digunakan oleh	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
		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 Kemasukan Pelajar (BPKP/UPU)	Tidak perlu pelan pemulihan	

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

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