SIRIM QAS INTERNATIONAL	**SIRIM QAS INTERNATIONAL SDN. BHD.** MANAGEMENT SYSTEM CERTIFICATION DEPARTMENT Block 4, SIRIM Complex, No.1, Persiaran Dato' Menteri, Section 2, 40700 Shah Alam, Selangor Darul Ehsan	File No IS/ 6-80
	INFORMATION SECURITY MANAGEMENT SYSTEM SURVEILLANCE AUDIT REPORT	

CLIENT : UNIVERSITI PUTRA MALAYSIA
INFOCOMM DEVELOPMENT CENTRE (IDEC)

ADDRESS OF MAIN SITE AUDITED :
(In the case of multisite certification, list additional sites audited in attachments) :

43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

CERTIFICATION NO :	**AR 5761**	**STANDARD :**	**ISO/IEC 27001:2013**
AUDIT DATE :	**29-30 Jan 2015 /__6__auditor day(s)**	**LAST AUDIT DATE : 24-25 Sept 2013**	

SCOPE OF CERTIFICATION : Sistem Pengurusan Keselamatan Maklumat bagi Sistem- Sistem Kritikal Merangkumi Sistem Aplikasi Pelajar , Sistem Pengurusan Sumber Manusia , Sistem Pengurusan Kewangan dan Laman Web Utama Universiti Putra Malaysia.

AUDIT TEAM :	1)	Efizan bt Zamri	Ketua Pasukan Audit
	2)	Nur Aisya Bt Mohd Zamri	Pasukan Audit
	3)	Sazlin Bt Alias	Pasukan Audit (Hari Kedua Sahaja)
	4)	Nor Aza Bt Ramli	Pasukan Audit (Hari Pertama Sahaja)

NO OF EMPLOYEES (Applicable to the scope of certification) : 43 anggota kerja

Report by Audit Team Leader

Name : Efizan Bt Zamri

Signature :

Date : 30/1/2015

SIRIM QAS INTERNATIONAL SDN BHD
EFIZAN BINTI ZAMRI

Acknowledgement by Client's Management Representative

Name :

Signature :

DATO' WAN AZMAN WAN OMAR
Wakil Pengurusan
Universiti Putra Malaysia

Date : 30/1/2015

The Audit Plan and following attachments form part of this report :

Nonconformity Report(s)	√
Opportunities for Improvement	√
List of additional site(s)	√
List of remote supporting functons	√

Tick (√) where applicable

Report reviewed by :

(Senior Auditor/ Section Head)

Date

SURVEILLANCE AUDIT REPORT

1. SIGNIFICANT CHANGES TO ORGANIZATION INFORMATION SECURITY MANAGEMENT SYSTEM

Organisasi menentukan hala tuju migrasi untuk ISMS versi standard baru (ISO/IEC 27001:2013) bermula Mac 2014.

Prof Madya Dr Fatimah Sidi dilantik sebagai Pengarah Baru IDEC menggantikan Dr Khairulnizam Samsudin mulai 1 September 2014.

SOA juga berubah mengikut kesesuaian untuk peralihan ke standard baru ISO/IEC 27001:2013.

(Perubahan keseluruhan kawalan A.5.1 sehinggan A.18.2) , merujuk No Semakan :05 dan No Isu :01 bertarikh 24 Oktober 2014.

2. SOA REFERENCE (including revision number) : SOA NO SEMAKAN 05, NO ISU 01 BERTARIKH 24 OKT 14.

3. SUMMARY OF REVIEW OF ACTIONS TAKEN ON NONCONFORMITIES IDENTIFIED DURING THE PREVIOUS AUDIT (detail of NCR's and the status are to be listed in the Appendix 1):

Terdapat 1 ketakakuran untuk audit terdahulu. Telah dilihat kembali dan sudah ditutup.

4. USE OF CERTIFICATION / ACCREDITATION MARKS

☐	Not in use	☐	Used; unacceptable
√	Used; acceptable		

5. COMMENTS ON FINDINGS :

5.1 Effectiveness of Internal Audit

Audit Dalaman telah dilaksanakan pada 11 – 12 November 2014 oleh 16 orang juruaudit yang dilantik. Merujuk kepada Perancangan Audit Dalaman Tahunan ISMS, Jadual Audit Dalaman ISMS dan Nota Audit Dalaman ISMS, didapati liputan audit adalah komprehensif dan kesaksamaan audit juga jelas. Sebanyak 13 laporan ketakakuran (NCR) dan 14 peluang penambahbaikan (OFI) direkodkan. Pengendalian penemuan-penemuan audit adalah baik. Walau bagaimanapun, penggunaan klausa dan kawalan yang dilaporkan di dalam borang ketakakuran / peluang penambahbaikan boleh ditambahbaik.

5.2 Management Review

Pelaksanaan kajian semula pengurusan dilakukan melalui beberapa platform seperti Mesyuarat Kajian Semula Pengurusan ISMS (MKSP), Mesyuarat Pengurusan ISMS dan Mesyuarat Jawatankuasa Jaminan Kualiti. Mesyuarat kajian semula pengurusan (MKSP) yang terkini telah dilaksanakan pada 1 Disember 2014 yang dipengerusikan oleh Naib Canselor, YBhg. Prof. Datuk Dr. Mohd. Fauzi Hj. Ramlan. Perbincangan terperinci mengenai isu-isu teknikal telah dibincangkan melalui mesyuarat Pengurusan ISMS dan jawatankuasa Jaminan Kualiti yang dijadualkan dari semasa ke semasa. Merujuk kepada sampel minit dari mesyuarat-mesyuarat tersebut, didapati isu-isu yang dibincangkan menepati kehendak klausa 9.3 Standard ISO/IEC 27001:2013.

5.3 Information Security Risks Assessment:

Proses penilaian risiko dan penguraian risiko telah dilaksanakan berdasarkan metolodologi yang dibangunkan oleh organisasi. Organisasi menggunakan Methodologi MYRAM yang telah dikemaskini. Didapati proses penilaian risiko ini telah dilaksanakan oleh unit- unit yang terlibat di bawah skop pensijilan Berdasarkan analisis penilaian risiko sebanyak 288 aset telah dikenal pasti, meliputi *hardware, software, people, information dan data, services (supporting) dan services (accessibility)*. Hasil Penilaian Risiko yang telah di jalankan aras risiko merangkumi risiko rendah ,sederhana dan tinggi. Terdapat 174 aset yang berisiko tinggi , 463 aset berisiko sederhana dan 174 aset berisiko rendah.Pihak pengurusan telah membuat keputusan dan mengesyorkan 76% iaitu aset yang berisiko tinggi dan sederhana menjalani proses penguraian risiko. Kerentatan (*vulnerability*) yang dilihat semasa perlaksanaan proses penguraian adalah seperti kekurangan dalam pengendalian prosedur dan kaedah, kekurangan penyelenggaraan perkakasan. Pelan-pelan rawatan yang dicadangkan adalah seperti penyelenggaraan berkala untuk Genset dan utiliti, program kesedaran untuk ISMS dan prosedur pengurusan pusat Data. Walaubagaimanapun untuk Keselamatan maklumat penilaian risiko ini terdapat satu laporan ketakakuran yang dikeluarkan.

5.4 Overall Implementation of Security Controls:

Tahap perlaksanaan ISMS adalah dilihat dari audit dijalankan
Walaubagaimanapun ruang-ruang penambahbaikan adalah direkodkan seperti di laporan peluang penambahbaikan (OFI) dan laporan ketakakuran (NCR).

5.4 Continual Improvement :

Inisiatif bagi memastikan peningkatan berterusan dilihat dari segi penambahbaikan yang telah diimplementasi dan dibincangkan di dalam mesyuarat pengurusan. Antara peningkatan berterusan yang dilihat adalah naik taraf infra Pusat Data, Sistem Aplikasi Utama, Server Pemulihan Bencana Universiti, Storan Khas Mengarkib Data Universiti dan Naiktaraf Bilik Persedian Server *(Staging Room)*.

5.5 Useful comparisons with previous audit results :

Terdapat ketakakuran dan beberapa peluang penambahbaikan di keluarkan pada audit ini. Di dapati pemahaman auditee terhadap keperluan standard boleh dipertingkatkan lagi .Perlaksanaan ISMS telah diperluaskan dari pengurusan operasi Pusat Data kepada Penyelenggaraan Aplikasi untuk Sistem- Sistem Kritikal di UPM. Pengauditan dilaksanakan merangkumi Pentadbir Sistem di Unit- Unit tersebut.

6. NONCONFORMITY REPORT

Total no. of minor NCR(s) : **8** List : AIS-1,AIS-2,AIS-3, NR-1,NR-2,SAZ-1,SAZ-2,EFI-1

7. ANY UNRESOLVED ISSUES, IF IDENTIFIED

Tiada isu-isu yang tidak dapat diselesaikan.

SURVEILLANCE AUDIT REPORT

8. SUMMARY OF FINDINGS - Maturity of system and effectiveness of system in meeting set objectives including agreed requirements and other positive and negative observations

Penemuan audit yang didapati oleh kumpulan juruaudit merumuskan bahawa sistem pengurusan keselamatan maklumat yang dilaksanakan di UNIVERSITI PUTRA MALAYSIA, INFOCOMM DEVELOPMENT CENTRE (IDEC) telah memenuhi keperluan standard ISO /IEC 27001:2013.

Penambahbaikan terhadap sistem yang sedia ada boleh dipertingkatkan lagi berdasarkan pemerhatian yang dilaporkan di laporan ketakakuran (NCR) dan peluang penambahbaikan (OFI) yang dikeluarkan oleh juruaudit.

9. RECOMMENDATION :

☐ No NCR recorded. Recommended to continue certification *with/ without change.

☑ NCR (s) recorded. Recommended to continue certification *with/ ~~without~~ change conditional upon satisfactory verification of corrective actions taken. Recommendation to continue certification *with/ ~~without~~ change will be made after :

- ☐ On-site audit of the following area(s) including verification of corrective action : _____
- ■ Off-site verification of corrective action(s). Records of implementation of proposed corrective action to be submitted for verification.

* Nature of change : (if applicable) Perubahan peralihan standard persijilan ke ISO /IEC 27001:2013 dan SOA ISU 01.

- ☐ Suspension of certification, a reaudit of the system shall be carried out before a recommendation is made to lift the suspension.
- ☐ Withdrawal

Note :

a) *Corrective Action Plans for all nonconformities (minor/ major) raised shall be submitted to the Audit Team Leader within one month and evidence of implementation within 3 months of the date of this report. Failure to comply shall result in either suspension or withdrawal of the certification.*

b) *If there is any unresolved issue at the end of the audit, it shall be brought to the attention of the management of SIRIM QAS Intl for resolution.The client will be notified in writing of the decision within two weeks of the date of this report.*

FOLLOW UP ON NCR(s)

It is confirmed that all corrective actions taken have been satisfactorily verified. Recommended to continue certification.

Audit Team Leader : Efizan Bt Zamri

(Name)	(Signature)	(Date)

SURVEILLANCE AUDIT REPORT

SUMMARY BY FUNCTION/ DEPARTMENT/ PROCESS/ PROJECT SITE

ISO/IEC 27001: 2013		Requirement audited	FUNCTION / DEPARTMENT/ PROJECT SITE												NCR
			Pengurusan	Unit Rangkaian	Unit Keselamatan ICT	Unit Pusat Data (Beta DC & Epsilon DC)	Unit Pentadbiran Data	Unit Operasi Aplikasi	Bahagian Akademik (SMP)	Sekolah Pengajian Siswazah (iGIMS)	Sokongan (HR & Legal)				
4	**Context of the organizations.**														
4.1	Understanding the organization and its context.	√	√	√	√	√	√	√	√	√	√				
4.2	Understanding the needs and expectations of interested parties	√	√	√	√	√	√	√	√	√	√				
4.3	Determining the scope of the information security management system	√	√	√	√	√	√	√	√	√	√				
4.4	Information security management system	√	√	√	√	√	√	√	√	√	√				
5	**Leadership**														
5.1	Leadership and commitment	√	√	√	√	√	√	√	√	√	√				
5.2	Policy	√	√	√	√	√	√	√	√	√	√				
5.3	Organizational roles, responsibilities and authorities	√	√	√	√	√	√	√	√	√	√				
6	**Planning**														
6.1	Actions to address risks and opportunities	√	**2**	√	√	√	√	√	√	√	√			2	
6.2	Information security objectives and plans to achieve them	√	√	√	√	√	√	√	√	√	√				
7	**Support**														
7.1	Resources	√	√	√	√	√	√	√	√	√	√				
7.2	Competence	√													
7.3	Awareness	√	√												
7.4	Communication	√	√												
7.5	Documented information	√	**1**	√	√	√	√	√	√	√	√			1	
8	**Operation**														
8.1	Operation planning and control	√	√	**1**	√	√	√	√	**1**	**2**	√			4	
8.2	Information security risk assessment	√	√	√	√	√	√	√	√	√	√				
8.3	Information security risk treatment	√	√	√	√	√	√	√	√	√	√				
9	**Performance evaluation**														
9.1	Monitoring, measurement, analysis and evaluation	√	**1**	√	√	√	√	√	√	√	√			1	
9.2	Internal Audit	√	√	√	√	√	√	√	√	√	√				
9.3	Management Review	√	√	√	√	√	√	√	√	√	√				
10	**Improvement**														
10.1	Nonconformity and corrective action	√	√	√	√	√	√	√	√	√	√				
10.2	Continual improvement	√	√	√	√	√	√	√	√	√	√				
	Total No. of NCR(s)		3	1					1					8	

Note :

a) Indicate in the "Requirement audited" column with a (√) the requirements that were audited and (-) for requirements that were not audited.

b) In the case where requirements were audited and nonconformities detected, replace the (√) with the number of nonconformities (No of major/ no. of minor)

c) Indicate with (NA) if the requirement is not applicable

APPENDIX 1

VERIFICATION OF PREVIOUSLY RAISED NONCONFORMITY REPORTS

No.	NCR Reference No.	Evidence sighted for the implementation of the corrective action	Effectiveness of corrective action (Y/N)	Remarks
1	EFI-1	Sample di CCTV dan di Sistem adalah bertepatan.	Y	

Note:
If the corrective action has not been effectively implemented, a new NCR shall be reissued and indicate in the "Remarks" column.

Auditor Name: ___Efizan Bt Zamri_____ Date: __30 Januari 2015_____

APPENDIX 2

LIST OF ADDITIONAL SITE(S)				
No.	**Address of site**	**Scope (if different from the main site)**	**No. of employees**	**Audited / Not Audited**
1	Beta Data Centre, 43400 Serdang, Selangor Darul Ehsan.	Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Data.	28	Di Audit
2	Epsilon Data Recovery Centre, UPM Server Farm, 43400 Serdang, Selangor Darul Ehsan.	Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Pemulihan Bencana.	-	Di Audit

APPENDIX 3

LIST OF REMOTE SUPPORT FUNCTIONS				
No.	**Address**	**Activities**	**No. of employees**	**Audited / Not Audited**
1	Bahagian Media dan Arkib, Aras Bawah, Perpustakaan Sultan Abdul Samad, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor.	Penyimpanan Pita Luar	-	Di Audit

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS/6-080	**NON-CONFORMITY REPORT (NCR)**	NCR No. : AIS-1
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 29 - 30 Jan. 2015

Client : UNIVERSITI PUTRA MALAYSIA - IDEC

Section 1 - Details of non-conformity

Requirement :
ISO/IEC 27001:2013 ***Clause 7.5.3 Control of documented procedure*** – *For the control of documented information, the organization shall address the following activities as applicable: e) control of changes*
Prosedur Kawalan Dokumen ISMS, No. Semakan: 02, No. Isu: 01, bertarikh 24/10/2014.

Finding :

Diperhatikan bahawa kawalan bagi keperluan klausa di atas tidak dilaksanakan dengan berkesan.

Objective evidence :

1. Dokumen lapuk tidak dicop sebagai "DOKUMEN LUPUS". Sampel yang dilihat, Manual Sistem Pengurusan Keselamatan Maklumat, No. Semakan 04, No. Isu 01.
2. ~~Dokumen lapuk tidak dicop sebagai "DOKUMEN TIDAK TERKAWAL". Sampel yang dilihat, Manual Sistem Pengurusan Keselamatan Maklumat, No. Semakan 04, No. Isu 01. Statement of Applicability (SoA) No. Semakan 04, No. Isu 01.~~
3. Dokumen Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi, No. Semakan 00, No. Isu 02.
4. Surat Aku Janji telah digantikan dengan Surat Aku Janji Pihak Luar tetapi tidak di cop batal.

Auditor : _____ (Nur Aisya Mohd. Zamri)

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ ( )

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ ( ) Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )

NCR Close Out : ☐ Yes ☐ No
Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS/6-080	**NON-CONFORMITY REPORT (NCR)**	NCR No. : AIS-2
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 29 - 30 Jan. 2015

Client : UNIVERSITI PUTRA MALAYSIA - IDEC

Section 1 - Details of non-conformity

Requirement :

ISO/IEC 27001:2013 ***Clause 6.1.3 Information security risk treatment*** – *The organization shall define and apply as information risk treatment process to: d) produce a Statement of Applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A.*

Finding :

Merujuk kepada documen Statement of Applicability (SoA), penggunaan dan justifikasi kawalan tidak dinyatakan mengikut keperluan klausa di atas.

Objective evidence :

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.

Auditor : _____ (Nur Aisya Mohd. Zamri)

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )	NCR Close Out : ☐ Yes ☐ No Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS/6-080	**NON-CONFORMITY REPORT (NCR)**	NCR No. : AIS-3
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 29 - 30 Jan. 2015

Client : UNIVERSITI PUTRA MALAYSIA - IDEC

Section 1 - Details of non-conformity

Requirement :
ISO/IEC 27001:2013 ***Clause 9.1 Monitoring, measurement, analysis and evaluation*** – *The organization shall evaluate the information security performance and the effectiveness of the information security management system. The organization shall determine: b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results.*
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.

Finding :

Keperluan di atas tidak dilaksanakan secara berkesan.

Objective evidence :

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 dala 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.

Auditor : _____
(Nur Aisya Mohd. Zamri)

Client's Representative : _____
(DATO' WAN AZMAN WAN OMAR
Wakil Pengurusan
Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____
(DATO' WAN AZMAN WAN OMAR
Wakil Pengurusan
Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____
(DATO' WAN AZMAN WAN OMAR
Wakil Pengurusan
Universiti Putra Malaysia)

Accepted by : _____
( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____
( )

NCR Close Out : ☐ Yes ☐ No
Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS / 6 - 80	**NON-CONFORMITY REPORT (NCR)**	NCR No. : EFI-1
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 29-30 Jan 2015

Client : UNIVERSITI PUTRA MALAYSIA
INFOCOMM DEVELOPMENT CENTRE (IDEC)

Section 1 - Details of non-conformity

Requirement :
6.1.3 Information Security Risk Treatment
The organization shall define and apply an information security risk treatment process to:
e.) formulate an information security risk treatment plan

Finding :
Di dapati semakan terhadap laporan penguraian risiko (RTP) adalah tidak memenuhi keperluan kawalan standard.

Objective evidence :
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).

Auditor : _____ (EFIZAN BT ZAMRI)

SIRIM QAS INTERNATIONAL SDN BHD EFIZAN BINTI ZAMRI

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Accepted by : _____ (EFIZAN BT ZAMRI)

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ (EFIZAN BT ZAMRI)

NCR Close Out : ☐ Yes ☐ No
Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS / 6 - 80	**NON-CONFORMITY REPORT (NCR)**	NCR No. : NR-2
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1 Audit Date : 29 Jan 2015

Client: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),

Section 1 - Details of non-conformity

Requirement :

i) 8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

A.9.3.1 Use of secret authentication information

Users shall be required to follow the organization's practices in the use of secret authentication information.

ii) UPM/ISMS/SOK/GP01/Kata Laluan (Isu No. 2 Semakan 00)

Finding :

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.

Objective evidence :

Penukaran *kata laluan semasa 'first time login' tidak dilaksanakan mengikut keperluan garis panduan kata laluan UPM/IDEC untuk Sistem Maklumat Pelajar (SMP).*

Auditor : _____ (NOR AZA RAMLI) — SIRIM QAS INTERNATIONAL SDN BHD — EFIZAN BINTI ZAMRI

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )

NCR Close Out : ☐ Yes ☐ No

Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS / 6 - 80	**NON-CONFORMITY REPORT (NCR)**	NCR No. : NR-1
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 29 Jan 2015

Client: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),

Section 1 - Details of non-conformity

Requirement :
8.1 Operational planning and control
The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

A.9.2.3 Management of privileged access rights
The allocation and use of privileged access rights shall be restricted and controlled

Finding :
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.

Objective evidence :
Login ID dengan *admin privilege* dikongsi untuk capaian ke core switches (core 24 dan core 23)

6/9

Auditor : _____ (NOR AZA RAMLI)

SIRIM QAS INTERNATIONAL SDN BHD EFIZAN BINTI ZAMRI

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR Wakil Pengurusan Universiti Putra Malaysia)

Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )

NCR Close Out : ☐ Yes ☐ No
Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS / 6 - 80	**NON-CONFORMITY REPORT (NCR)**	NCR No. : SAZ-1
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 30 Jan 2015

Client: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),

Section 1 - Details of non-conformity

Requirement :
8.1 Operational planning and control
The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

A.9.4.1 Information access restriction
Access to information and application system functions shall be restricted in accordance with the access control policy.

Finding :
Login ID ke aplikasi iGIMS di Sekolah Pengajian Siswasah tidak dikawal dan diselenggara dengan berkesan.

Objective evidence :
1. *Login ID* tidak unik dan konsistent (ID: ex5tuff)
2. *Login ID* bagi pegawai yang bertukar tidak dikemaskini (KA0406 dan farah)
3. Hak capaian keistimewaan pengguna (GSO.Admin / iGIMS.Admin) diberikan kepada kakitangan yang tidak sepatutnya. (A03205, maizatul, A03856 dan linda)

Auditor : _____ (SAZLIN BT. ALIAS)

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 2 - Result of investigation and determination of root cause

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : _____ (DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia)

Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )

NCR Close Out : ☐ Yes ☐ No
Date :

SIRIM QAS INTERNATIONAL SDN. BHD.

File No. : IS / 6 - 80	**NON-CONFORMITY REPORT (NCR)**	NCR No. : SAZ-2
Audit Type : ☐ Initial Certification Stage 2 ■ Surveillance ☐ Recertification	**Standard : ISO/IEC 27001:2013**	Page 1 of 1
		Audit Date : 30 Jan 2015

Client: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),

Section 1 - Details of non-conformity

Requirement :
8.1 Operational planning and control
The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

A 8.1.1 Inventory of assets
Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.

Finding :
Aset- aset yang berkaiatan sistem iGIMS tidak dikenalpasti didalam Aset Register

Objective evidence :
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)

Auditor : _____ (SAZLIN BT. ALIAS)

Client's Representative : DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia

Section 2 - Result of investigation and determination of root cause

Client's Representative : DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia

Section 3 – Correction (if applicable) and Corrective action plan including completion date:

Client's Representative : DATO' WAN AZMAN WAN OMAR, Wakil Pengurusan, Universiti Putra Malaysia

Accepted by : _____ ( )

Section 4 – Verification (to be filled up by Auditor)

Verified by : _____ ( )

NCR Close Out : ☐ Yes ☐ No
Date :

Rujukan fail : IS/6-080

PELUANG PENAMBAHBAIKKAN		
Klausa	**Butiran**	**Komen terhadap tindakan yang telah diambil**
4.2 (b)	***Understanding the needs and expectations of interested parties*** 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.	
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).	
9.1	***Monitoring, measurement, analysis and evaluation*** 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. *Nota: Laporan bagi penemuan di atas perlu dijawab kepada pihak SIRIM dalam tempoh yang telah ditetapkan.*	
7.2 (c)	***Competence*** Organisasi masih belum melaksanakan penilaian keberkesanan latihan bagi Bengkel Pemantapan Juruaudit Dalaman ISMS.	
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.	

Juruaudit : Nur Aisya Mohd. Zamri Tarikh: 29-30 Jan. 2015

Rujukan fail : IS/6 - 80

PELUANG PENAMBAHBAIKKAN		
Klausa	**Butiran**	**Komen terhadap tindakan yang telah diambil**
A.11.2.1	**Equipment Siting and Protection** Didapati bilik rangkaian yang menempatkan perkakasan rangkaian boleh ditambahbaik dari segi pengudaraan suhu bilik.	
A.12.1.3	**Capacity Management** Pengurusan kapasiti untuk storan pendua boleh ditambahbaik bagi mengelakkan pendua gagal kerana storan penuh.	
A.13.2.4	**Confidentiality or non-disclosure agreements.** Surat Akuan Pematuhan GPKTMK UPM tidak digunapakai secara konsisten untuk pihak ketiga. (pembekal). LAPORAN TAMAT	

Juruaudit : EFIZAN BT ZAMRI

SQAS INTERNATIONAL SDN BHD EFIZAN BINTI ZAMRI

Tarikh: 29-30 Jan 2015

File ref. : IS / 6 - 80

OPPORTUNITIES FOR IMPROVEMENT		
Clause	**Details**	**Comments on action taken**
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. Walaubagaimanapun, pemantauan untuk memastikan kawalan terus dilaksanakan dengan berkesan perlu diberi perhatian memandangkan jangkamasa Januari 2015 untuk pelaksanaan tersebut hampir tamat.	
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.	

Auditor : Nor Aza Ramli Date: 29 Januari 2015