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 RECERTIFICATION AUDIT REPORT	

CLIENT : Universiti Putra Malaysia

ADDRESS OF MAIN SITE AUDITED :
(In the case of multisite certification, additional sites are listed in the attachment) :

43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

CERTIFICATION NO : AR5761	**STANDARD : ISO/IEC 27001: 2013**
AUDIT DATE : 8-10 Dis 2015 /__6__auditor day(s)	**LAST AUDIT DATE : 29-30 Jan 2015**

SCOPE OF CERTIFICATION :

1.) Sistem Pengurusan Keselamatan Maklumat Bagi Proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra.
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.

AUDIT TEAM :

1)	Efizan Bt Zamri	Ketua Pasukan Audit
2)	Nor Aza Bt Ramli	Juruaudit (hari ke 1 dan ke 2 sahaja)
3)	Fazlin Bt Zakaria	Juruaudit (hari ke 3 sahaja)
4)		

NO OF EMPLOYEES (Applicable to the scope of certification) : 126 anggota kerja

Report by Audit Team Leader

Name : Efizan Bt Zamri
Signature :
Date : 10 Disember 2015

SIRIM QAS INTERNATIONAL SDN BHD ★ EFIZAN

Acknowledgement by Client's Management Representative

Name :
Signature :
Date : 10 Disember 2015

PROF. DR. M. IQBAL SARIPAN
Pengarah
Pusat Jaminan Kualiti
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

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 and recommendation approved by :

_____

(Section Head)

_____

RECERTIFICATION AUDIT REPORT

1. SIGNIFICANT CHANGES TO ORGANIZATION INFORMATION SECURITY MANAGEMENT SYSTEM /SCOPE OF CERTIFICATION / SOA (COVERAGE OF THE CONTROLS)

Pelantikan Prof Dr M.Iqbal Saripan selaku Pengarah Pusat Jaminan Kualiti merangkap Wakil Pengurusan Sistem Pengurusan Keselamatan Maklumat (ISMS) berkuatkuasa 1 November 2015.

Perubahan skop baru untuk audit kali ini dilihat dan skop merangkumi Sistem Pengurusan Keselamatan Maklumat Bagi Proses Pendaftaran Pelajar Baharu Prasiswazah semasa Minggu Perkasa Putra.
Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Data Bagi Proses Pendaftaran Pelajar Baharu Prasiswazah.
Sistem Pengurusan Keselamatan Maklumat Untuk Pengoperasian Pusat Pemulihan Bencana Bagi Proses Pendaftaran Pelajar Baharu Prasiswazah.

Proses terlibat meliputi aktiviti proses lapor diri pelajar baharu prasiswazah yang melibatkan aktiviti berikut iaitu semakan tawaran, penerimaan salinan pendua slip bayaran yuran CIMB, penerimaan borang permohonan kad pelajar, pengesahan status kesihatan, pengesahan pendaftaran dan pendaftaran kolej.

Manakala skop bagi Pusat Data dan Pusat Pemulihan Bencana dikekalkan dan cuma melibatkan untuk Proses Pendaftaran Pelajar Baharu Prasiswazah.

Pusat Jaminan Kualiti, Bahagian Kemasukan & Tadbir Urus Akademik, Bahagian Hal Ehwal Pelajar, Pusat Pembangunan & Komunikasi IDEC untuk Pusat Data dan Pusat Pemulihan Bencana, Kolej Kediaman (Kolej 2, Kolej Tun Dr Ismail, Kolej 5 , Kolej 6 dan Kolej 10) , Pejabat Penasihat Undang- Undang, Perpustakaan, Pejabat Strategik Korporat & Komunikasi, Bahagian Keselamatan dan Pusat Kesihatan Universiti adalah diaudit untuk audit Pensijilan kali ini.

Manakala dari segi dokumentasi, Dokumen Penyataan Pemakaian (SOA) juga berubah mengikut kesesuaian terkini organisasi.

Perubahan kawalan merujuk No Dokumen UPM/ISMS/OPR/SOA, bertarikh 7 Disember 2015, No Semakan 08, No Isu : 01.

2. STATEMENT OF APPLICABILITY REVISION LEVEL: UPM/ISMS/OPR/SOA, 7 Disember 2015, No Semakan 08, No Isu : 01.

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):

8 Ketidakpatuhan dikeluarkan pada audit terdahulu dan terdapat 1 ketidakpatuhan yang dikeluarkan kembali. (EFI-1). Untuk 7 ketidakpatuhan yang dikeluarkan adalah ditutup dengan memuaskan.

4. USE OF CERTIFICATION / ACCREDITATION MARKS

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

5. COMMENTS ON FINDINGS :

5.1 Documentation

Sistem dokumentasi yang telah dibangunkan oleh organisasi adalah mencukupi seperti mana keperluan standard. Ianya di dalam bentuk *softcopy* (e-ISO) yang hanya boleh diakses oleh Pelaksana ISMS dan pemilik dokumen . Dokumen di bangunkan di dalam 3 kategori iaitu Pengurusan, Operasi dan Sokongan.

Garis Panduan Keselamatan Teknologi Maklumat dan Komunikasi (GPKTMK) (Isu 2, Semakan 0) dan Penyata Pemakaian (SOA) (Semakan 00, Isu 01) juga telah dibangunkan.

5.2 Effectiveness of internal audit

Audit Dalaman telah dilaksanakan pada 18-19 November 2015 oleh 3 kumpulan juruaudit yang di anggotai oleh 15 anggota yang dilantik. Merujuk kepada laporan audit sebanyak 3 laporan ketakakuran (NCR) dan 14 peluang penambahbaikan (OFI) direkodkan. Perlaksanaan Audit Dalaman dilihat memuaskan dan memenuhi keperluan standard.

5.3 Management review

Pelaksanaan kajian semula pengurusan dilaksanakan melalui Mesyuarat Kajian Semula Pengurusan Bil 1/2015 pada 27 November 2015 yang dipengerusikan oleh Naib Canselor , Prof Dato'Dr Mohd Fauzi Hj Ramlan. Merujuk kepada minit dari mesyuarat tersebut, didapati isu-isu yang dibincangkan adalah merangkumi dan memenuhi keperluan standard.

5.4 Implementation of Security Controls:

Tahap perlaksanaan ISMS adalah dilihat semasa perlaksanaa audit dalaman dan perlaksanaan kawalan- kawalan di dalam Annex A juga adalah baik dan memuaskan, walaubagaimanapun penambahbaikan juga diperlukan bagi mengukuhkan kawalan-kawalan yang dipilih.

5.5 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 seperti penambahbaikan terhadap pelaksanaan pendaftaran baharu secara atas talian sebelum hari pendaftaran sebenar, sifar bayaran yuran pendaftaran secara tunai dan menambah ciri pelaporan dalam sistem capaian pintu secara biometrik di Pusat Data Utama.

5.6 Useful comparisons with previous audit results :

Terdapat satu ketidakpatuhan dikeluarkan pada audit kali ini. Kefahaman auditee ke atas sistem pengurusan keselamatan maklumat adalah dilihat bertambah baik. Skop baharu juga diusulkan untuk audit kali ini.

RECERTIFICATION AUDIT REPORT

6. NONCONFORMITY REPORT

Total no. of minor NCR(s) : 1 List : NR-1

7. ANY UNRESOLVED ISSUES, IF IDENTIFIED

Nil

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 oleh kumpulan juruaudit merumuskan bahawa sistem pengurusan keselamatan maklumat yang dilaksanakan oleh Universiti Putra Malaysia telah memenuhi keperluan standard ISO /IEC 27001:2013.

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

9. RECOMMENDATION

☐ No NCR recorded. Renewal of certification *with/-without change.

☑ NCR(s) recorded. Recommendation for renewal of 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) SOA dipinda pada 7 Disember 2015, No Semakan 08, No Isu : 01, dan penyataan skop juga berubah.

☐ Withdrawal (Non-renewal)

Note :

a) *Corrective action plans and evidence of implementation for all nonconformities (minor/ major) raised shall be submitted to the Audit Team Leader before the expiry of the certificate. Failure to comply shall result in withdrawal, i.e. non-renewal of certificate.*

b) *Certificate will only be issued upon satisfactory verification of corrective actions for nonconformities raised.*

c) *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)

RECERTIFICATION AUDIT REPORT

SUMMARY BY FUNCTION/ DEPARTMENT/ PROCESS/ PROJECT SITE

ISO/IEC 27001: 2013		Requirement audited	Adequacy of documentation	FUNCTION / DEPARTMENT/ PROJECT SITE											NCR
				Pengurusan / Pusat Jaminan Kualiti	Bah Kemasukan & Tadbir Urus Akademik	Bah HEP	Pusat Pembangunan & Komunikasi IDEC (DC & DRC)	Pej Pendaftar (HR)	Kolej Kediaman (Kolej 2, Kolej Tun Dr Ismail, Kolej 5,Kolej 6, Kolej 10)	Pej Penasihat Undang-Undang (A.18)	Perpustakaan	Pej Strategik Korporat & Komunikasi (BCP)	Bahagian Keselamatan	Pusat Kesihatan Universiti	
4	Context of the organization														
4.1	Understanding the needs and expectations of interested parties	/	/	/	/	/	/	/	/	/	/	/	/	/	
4.2	Establishing and Managing the ISMS	/	/	/	/	/	/	/	/	/	/	/	/	/	
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	/	/	/	/	/	/	/	/	/	/	/	/	/	
6.2	Information security objectives and planning to achieve them	/	/	/	/	/	/	/	/	/	/	/	/	/	
7	**Support**														
7.1	Resources	/	/	/	/	/	/	/	/	/	/	/	/	/	
7.2	Competence	/	/	/	/	/	/	/	/	/	/	/	/	/	
7.3	Awareness	/	/	/	/	/	/	/	/	/	/	/	/	/	
7.4	Communication	/	/	/	/	/	/	/	/	/	/	/	/	/	
7.5	Documented information	/	/	/	/	/	/	/	/	/	/	/	/	/	
8	**Operation**														
8.1	Operational planning and control	/	/	/	/	/	/	/	/	/	/	/	/	/	
8.2	Information security risk assessment	/	/	/	/	/	/	/	/	/	/	/	/	/	
8.3	Information security risk treatment	/	/	/	/	/	/	/	/	/	/	/	/	/	
9	**Performance evaluation**	/	/	/	/	/	/	/	/	/	/	/	/	/	
9.1	Monitoring, measurement, analysis and evaluation	/	/	/	/	/	/	/	/	/	/	/	/	/	
9.2	Internal audit	/	/	/	/	/	/	/	/	/	/	/	/	/	
9.3	Management review	/	/	/	/	/	/	/	/	/	/	/	/	/	
10	**Improvement**	/	/	/	/	/	/	/	/	/	/	/	/	/	
10.1	Nonconformity and corrective action	/	/	/	/	/	1	/	/	/	/	/	/	/	1
10.2	Continual improvement	/	/	/	/	/	/	/	/	/	/	/	/	/	
	Total No. of NCR(s)						1								1

Note :

a) *Indicate in the "Requirement audited" column with a (√) the requirements that were audited and (-) for requirements that were not audited. Indicate with (NA) if the requirement is not applicable.*

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

c) *Tick (√) for adequacy of documentation. For requirements which have been deemed to be inadequately addressed in the documented quality system, NCR shall be raised.*

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	NR-1	Sample pada OS/Admin access untuk core switches- 4 serves OS unix adalah ok.	Y	
2	NR-2	Pertukaran kata laluan pada login pertama adalah dilihat. (SMP)	Y	
3	SAZ-1	Staff ID, Password dan Tarikh Valid dilihat .	Y	
4	SAZ-2	Inventori untuk Sistem iGIMS (Beta dan Epsilon DC) tiada dalam skop lagi.	Y	
5	AIS-1	Dokumen – Dokumen dilihat telah dikawal.	Y	
6	AIS-2	SOA telah dipinda dan dilihat. OK	Y	
7	AIS-3	Merujuk laporan MyRAM dan pengukuran kawalan dan objektif dilihat dan ok.	Y	
8	EFI-1	Jangkamasa pelan penguraian perlu dilihat kembali. Manakala existing safeguard adalah ok.	N	NR-1

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: ____10 Disember 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
	Tidak Berkaitan			

APPENDIX 3

LIST OF REMOTE SUPPORT FUNCTIONS				
No.	Address	Activities	No. of employees	Audited / Not Audited
	Tidak Berkaitan			

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 :8 – 9 Dec 2015

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

Section 1 - Details of non-conformity

Requirement :
10.1 Nonconformity and corrective action
When a nonconformity occurs, the organization shall: b) – g)

Finding :
Audit mendapati tindakan pembetulan yang diambil untuk ketakakuran yang di laporkan semasa audit pemantauan yang lepas tidak dijalankan secara menyeluruh. Keberkesanan tindakan-tindakan yang diambil tidak dapat dilihat memandangkan masih terdapat ruang di mana ketakakuran itu telah dan mungkin berulang.

Objective evidence :
NR-2: A.9.3.1 Use of secret authentication information
Tiada bukti pelaksanaan kawalan *first time login* untuk sistem SMP yang dilaksanakan sebagai tindakan pembetulan diuji dengan sepenuhnya.

EFI-1 : Clause 6.1.3 Information security risk treatment
Risk treatment plan yang dirancang untuk pengendalian risiko bagi 11 *high risks* yang dikenalpasti bagi tahun 2015 tidak menepati keperluan organisasi untuk merawat risiko-risiko tersebut. Kawalan yang dipilih tidak bertepatan dengan rancangan yang terlibat dengan jangkamasa pelaksanaan sehingga December 2015 yang tidak sesuai.

OFI : A.12.4.1 Event logging, A.12.4.2 Protection of log information, A.12.4.3 Administrator and operator logs
Kawalan *centralised log server* yang dirancang tidak dapat dilaksanakan akibat beberapa kekangan. Kawalan alternatif telah dilaksanakan. Walaubagaimanapun tiada perancangan menyeluruh dapat dilihat untuk mencapai objektif 'A.12.4 Logging and monitoring'.

Auditor : _____ (NOR AZA RAMLI)

SIRIM QAS INTERNATIONAL SDN BHD EFIZAN

Client's Representative : _____ (PROF. DR. M. IQBAL SARIPAN)

Pengarah
Pusat Jaminan Kualiti
Universiti Putra Malaysia
43400 UPM Serdang
Selangor Darul Ehsan

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 :

File ref. : IS / 6 - 80

OPPORTUNITIES FOR IMPROVEMENT		
Clause	**Details**	**Comments on action taken**
A.7.1.1	**Screening** Saringan keselamatan untuk Pengawal Keselamatan perlu dilihat kembali bagi memastikan mereka di akses bagi mengurangkan sebarang risiko dan ancaman kepada organisasi. Dokumen prosedur atau garis panduan juga perlu di kemaskini bagi memperlihatkan kategori anggota kerja yang perlu menjalani saringan keselamatan.	
A.8.2.1	**Classification of information** Didapati pemakaian borang-borang tidak mengandungi dokumentasi klasifikasi. Ini boleh dilihat kembali bagi memastikan sebarang borang yang memiliki sensitiviti informasi atau peribadi dapat dijaga dan diatur melalui prosedur yang sepatutnya.	
A.8.2.3	**Handling of assets** Borang untuk permohonan kad pelajar di lihat mengandungi nama penuh dan no kad pengenalan pelajar, difahamkan borang ini menjadi kertas kitar semula (recycle paper). Menerusi prosedur simpanan borang haruslah dalam tempoh 4 tahun. Pemilik proses perlu melihat kembali akan kawalan ini bagi mengelakkan isu pelanggaran sekuriti.	
A.11.2.1	**Equipment siting and protection** Didapati untuk Borang Maklumat Peribadi Pelajar yang sudah bergraduan di letakkan di dalam Stor Kolej. Lokasi bagi meletakkan borang tersebut yang mengandungi maklumat peribadi pelajar boleh dilihat kembali bagi menghindarkan dari segi risiko di akses oleh anggota yang tidak berkaitan.	
A.12.1.3	**Capacity management** Difahamkan pengeluaran kad pelajar hanya berlaku dalam tempoh 2 bulan selepas pelajar mendaftar di Minggu Perkasa Putra. Organisasi boleh melihat kembali dari segi pengurusan kapasiti bagi memastikan kemampuan anggota kerja untuk proses pengeluaran ke atas kad pelajar. Selain dari itu kad pelajar juga dilihat sebagai lambang identiti pelajar dan merupakan pengenalan diri dan dilihat dari segi sekuriti akan memberikan impak keselamatan kepada organisasi.	

A.13.2.4	**Confidentiality or non disclosure agreements** Bahagian Penasihat Undang- Undang boleh menambahbaik dari segi meneliti akan perjanjian ke atas kontrak- kontrak yang melibatkan penerimaan dan pertukaran maklumat.	

Auditor: Efizan Zamri

Date: 8-10 Disember 2015

File ref. : IS / 6 - 80

OPPORTUNITIES FOR IMPROVEMENT		
Clause	**Details**	**Comments on action taken**
A.16.1.2	Reporting information security events Tidak ada laporan insiden yang dilaporkan untuk tempoh Feb 2015 sehingga tarikh audit dijalankan. Garispanduan berkenaan insiden telah dibangunkan dan digunapakai oleh organisasi. Walaubagaimanapun kefahaman mengenai definisi insiden di dalam organisasi dan kesedaran untuk melaporkan insiden yang menepati definisi tersebut oleh semua pihak yang terlibat boleh ditambahbaik.	

Auditor : Nor Aza Ramli Date: 8 – 9 December 2015

OPPORTUNITIES FOR IMPROVEMENT		
Clause	**Details**	**Comments on action taken**
6.1.2	**Information security risk assessment** Laporan penilaian dan pentaksiran risiko telah dibangunkan (dibawah Pusat Kesihatan Universiti), namun begitu laporan ini perlu ditambahbaik berdasarkan isu masa CCTV yang tidak selaras berikutan berlaku gangguan bekalan tenaga elektrik.	
6.1.3	**Information security risk treatment** Penilaian risko untuk aset 'Laporan Pemeriksaan Kesihatan' (dibawah Pusat Kesihatan Universiti) dan untuk aset bagi Pengurusan Kolej telah dilaksanakan, walaubagaimanapun penguraian risiko untuk aset tersebut perlu disemak semula.	
	Operational planning and control	
8.1	**A.9.4.3 Password management system** Katalaluan untuk capaian Sistem Maklumat Pelajar telah ditetapkan kepada lapan (8) aksara (*alphanumeric*), walaubagaimanapun pengurusan katalaluan boleh ditambahbaik selaras dengan Garis Panduan Pengurusan Identiti.	
	LAPORAN TAMAT	

Auditor: Fazlin Bt Zakaria Date: 10 Dec 2015