File no. : IS / 6-80

Date : 6 January 2015
26 January 2015 (rev1)

Universiti Putra Malaysia,
Infocomm Development Centre (IDEC),
43400 Serdang,
Selangor Darul Ehsan,
Malaysia.

(Attn : Pn Noraihan Binti Noordin)

Tel No. : 03-89466150
Fax No. : 03-89472037
Email : /noraihan@upm.edu.my

Dear Sir/ Madam

ISO/IEC 27001: 2013 – SURVEILLANCE AUDIT PLAN-REV1

Please be informed that a Surveillance Audit of your organization's Information Security Management systems has been scheduled on **29-30 January 2015.**

Enclosed please find the audit plan. Please note that the audit plan serves as a guide and may change as the audit progresses.

Thank you

Yours sincerely

Efizan Binti Zamri
(……)

Lead Auditor
Service Section
Management System Certification Department
SIRIM QAS International Sdn. Bhd.
H/P No. : 019-2444833
Tel. No. : 03-55446485
Fax No. : 03-55446414
E-mail : efizan@sirim.my

SURVEILLANCE AUDIT PLAN

1. **Audit Objectives**

   a) To determine the continued compliance of the client's IT service management system to the ISO/IEC 27001:2013 standard;

   b) To evaluate the ability of the management system to ensure client meets applicable statutory, regulatory and contractual requirements, where applicable;

   c) To evaluate the effectiveness of the management system to ensure the client is continually meet its specified objectives;

   d) To identify areas of improvement of the management system, as applicable;

   e) To assess changes that has been made to the client's information security management system;

   f) To verify the effective implementation of corrective actions arising from the findings of the previous audit.

2. **Date of audit** : 29-30 January 2015

3.

Site of audit :
Universiti Putra Malaysia, Infocomm Development Centre (IDEC),
43400 Serdang,Selangor Darul Ehsan,Malaysia.

Scope of certification : ISMS For The Operation of UPM Data Centre Covering Information For The Following Applications:

1.) UPM Website (www.upm.edu.my)
2.) Financial Management System
3.) Human Resource Management System
4.) Student Information System (SMP- Sistem Maklumat Pelajar)

Site 2: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),
Beta Data Centre, 43400 Serdang, Selangor Darul Ehsan, Malaysia.
Scope of certification: ISMS For Data Centre Operation.

Site 3: Universiti Putra Malaysia, Infocomm Development Centre (IDEC),
Epsilon Data Recovery Centre, UPM/Server Farm, 43400 Serdang,
Selangor Darul Ehsan, Malaysia.
Scope of certification: ISMS for Data Recovery.

New Scope :
Site : Sekolah Pengajian Siswazah.
Scope of Certification : Sistem iGIMS (Sistem Berkaitan Pelajar Siswazah)

4. **Audit Criteria :**

   a) ISO/IEC 27001:2013
   b) Organization's ISMS Documentation

5. **Audit team & Role**

a)	Audit Team Leader	:	Efizan Bt Zamri
b)	Auditor	:	Nur Aisya Bt Mohd Zamri Nor Aza Bt Ramli (Day 1)
		:	Sazlin Bt Alias (Day 2)

(If there is any objection on the proposed audit team, the client is required to inform in writing to the Audit Team Leader or the Head of Section)

6. **Methodology of audit**

a) Review of documentation and records,
b) Observation of processes and activities,
c) Interview with client's personnel responsible for the audited area.

7. **Confidentiality requirements**

The members of the audit team from SIRIM QAS International Sdn. Bhd. undertake not to disclose any confidential information obtained during the audit including information contained in the final report to any third party, without the express approval of the client unless required by law.

8. **Working Language** **:** English and Bahasa Melayu

9. **Reporting**

i)	Language	:	~~English/~~Bahasa Melayu
ii)	Format	:	Verbal and written
iii)	Expected date of issue	:	After closing meeting
iv)	Distribution List	:	Original copy issued to the client and copy maintained in the client file.

10. **Facilities and assistance required** :

i) Meeting room
ii) Facilities for photocopying
iii) Personal protective equipment (where necessary)
iv) A representative appointed by the client, acting as a guide to assist the audit team.

11. **Details of Audit Plan** : As follows

DETAILS OF AUDIT PLAN

Day 1		
Time	**Agenda**	**Responsibility**
0930–0945	Opening Meeting 1. Brief overview of the organization and the ISMS established by organization's representative (on any changes) 2. Briefing on audit details by SIRIM QAS International's representative	SIRIM's auditors and client's representatives
0945-1700	Follow up on previous audit findings **Review of documentation against requirements of ISO/IEC 27001:2013** • **Context of the organization** inclusive of understanding the organization and its context, understanding the needs and expectations of interested parties, determining the scope of the ISMS. • **Documented information** inclusive of creating and updating and control of documented information. • **Planning** inclusive of actions to address risks and opportunities, information security risk assessment, information security risk treatment and information security objectives and plans to achieve them. • **Performance evaluation** inclusive of monitoring, measurement, analysis and evaluation, internal audit and management review. • **Improvement** inclusive of nonconformity and corrective action and continual improvement. • **Support** inclusive of resources, competence, awareness and communication (covering control A.7 Human Resource Security) **Leadership** inclusive of leadership and commitment, policy and organizational roles, responsibilities and authorities *(Covering control A.5 Information Security Policies and A.6 Organization of Information Security)*	Aisya and client's representatives

	Audit on the activities related to following requirements: *** Operation** (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.) **-** Verification on the effectiveness of control as per Statement of Applicability in relation to **Data Centre Operation.** • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13)	Efi & Client's Representative @ Site 2 (Beta Data Centre)
	Audit on the activities related to following requirements: *** Operation** (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.) **-** verification on the effectiveness of control as per Statement of Applicability in relation to UPM Website (www.upm.edu.my) & Student Information System (SMP-Sistem Maklumat Pelajar) • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) • System acquisition, development and maintenance (A.14)	Aza & Client's Representative
1700	Review of Day 1 Findings	SIRIM's auditors and client's representatives

Day 2		
Time	**Agenda**	**Responsibility**
0930–1530	Audit on requirements related to: Internal Audit & Management Review ISMS improvement covering the Continual Improvement activities, Corrective Action. Verification on the effectiveness of control as per Statement of Applicability in relation to Information Security Incident Management (A.16) Audit on requirements related to: • Compliance (A.18) ISMS Monitoring and Review covering overall regular review of effectiveness**, measurement of control effectiveness.**	Aisya and client's representatives
	Audit on the activities related to following requirements: *** Operation** (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.) **-** verification on the effectiveness of control as per Statement of Applicability in relation to Data Recovery • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13) Audit on requirements related to: • Information Security Aspect of Business Continuity Management (A.17)	Efi & Client's Representative @ Site 3 (Data Recovery Center)

	Audit on the activities related to following requirements: *** Operation** (Inclusive of operational planning and control, information security risk assessment and information security risk treatment.) **-** verification on the effectiveness of control as per Statement of Applicability in relation Sistem iGIMS **(new scope)** • Asset management (A.8) • Cryptography (A.10) • Physical and environmental security (A.11) • Access control (A.9) • Operations security (A.12) • Supplier Relationship (A.15) • Communications security (A.13)	Sazlin and client's representatives
1530–1700	Preparation of Report	SIRIM's auditor
1700	Closing Meeting : Presentation of Findings and Recommendation	SIRIM's auditor & client's management