AUDIT PLAN

File No.	:	20190602821
Date	:	27-Aug-2019
Client Name & Address	:	UNIVERSITI PUTRA MALAYSIA
		- 43400 SERDANG
		SELANGOR DARUL EHSAN MALAYSIA
Attention	:	PUAN ROZI BINTI TAMIN
Telephone No.	:	03-89471512 / 019-6621400
Fax No.	:	03-89472037

Dear Sir/Madam,

SURVEILLANCE 1 AUDIT PLAN ISO/IEC 27001:2013

Please be informed that the audit of your organization's management system has been scheduled from 01-Sep-2019 to 09-Oct-2019.

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.

Nur Aisya bt Mohd Zamri
Services
Management System Certification Department
SIRIM QAS International Sdn Bhd,
H/P No :011-32141332
Fax. No :
E-Mail :aisya.zamri@gmail.com

THIS IS A COMPUTER GENERATED DOCUMENT. NO SIGNATURE IS REQUIRED

SURVEILLANCE 1 AUDIT PLAN

1. Audit Objectives

a) Compliance to the requirements of the standard, applicable statutory, regulatory and contractual requirements

b) Performance monitoring, measuring, reporting and reviewing against key performance objectives and targets.

c) Operational control of the organization's processes, internal auditing and management review, management responsibility for the organization's policies.

2. Site of Audit

- 43400 SERDANG
SELANGOR DARUL EHSAN MALAYSIA

3. Scope of certification

1) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENDAFTARAN PELAJAR BAHARU PRASISWAZAH MERANGKUMI AKTIVITI SEMAKAN TAWARAN HINGGA PENDAFTARAN KOLEJ KEDIAMAN.
2) SISTEM PENGURUSAN KESELAMATAN MAKLUMAT BAGI PROSES PENILAIAN PENGAJARAN PRASISWAZAH DI FAKULTI.

INI ADALAH MENEPATI PENYATAAN PEMAKAIAN:
TARIKH KEMASKINI 04 SEPTEMBER 2018

4. Audit Criteria

a) ISO/IEC 27001:2013

b) Client's management system documentation

c) Applicable statutory and regulatory requirements

5. Audit Team & Role

ISO/IEC 27001 : 2013

Name of Auditor	Role	Number of Days	Audit Date
AZRAN BIN MOHAMMAD RIDZUAN	AUDITOR	1	01 SEP 19
NORIDAH BINTI YAHYA	AUDITOR	2	07 OCT 19 - 08 OCT 19
NUR AISYA BT MOHD ZAMRI	AUDIT TEAM LEADER	3	07 OCT 19 - 09 OCT 19

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 client approval unless required by law.

8. Working Language

English

9. Reporting

Language	English
Format	Verbal and written
Expected date of issue	After closing meeting
Distribution list	Original copy issued to the client and copy maintained in the client file

10. Facilities and assistance required

a) Meeting room
b) Facilities for photocopying and printing
c) Personal Protective Equipment (PPE)
d) A guide (who may also be the auditee) to assist the audit team

Day 1

Time	Agenda	Responsibility
0930 - 1000	Opening Meeting (Site: Bintulu Campus) • Briefing on the Information Security Management System by organization's representative on any changes to the system since last audit • Briefing on audit details by SIRIM QAS International's representative	SIRIM's auditor and client's representatives
1000 - 1230	Follow-up previous audit findings Onsite observation and verification of the effectiveness controls as in Statement of Applicability covering Prasiswazah student registration processes.	Azran
1230 - 1400	Lunch break	All
1400 - 1500	Review of Day 1 audit findings (if any)	SIRIM's auditor and client's representatives

Day 2

Time	Agenda	Responsibility
0930 - 1000	Opening Meeting (Site: UPM Serdang) • Briefing on the Information Security Management System by organization's representative on any changes to the system since last audit • Briefing on audit details by SIRIM QAS International's representative	SIRIM's auditors and client's representatives

SURVEILLANCE 1 AUDIT PLAN

1000 - 16300	Follow-up previous audit findings Documented information inclusive of creating and updating and control of documented information. Covering A.5 and A.6 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. Leadership inclusive of leadership and commitment, policy and organizational roles, responsibilities and authorities. Planning inclusive of actions to address 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.	Aisya
	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 at Pusat Pembangunan Maklumat dan Komunikasi IDEC - Data centre operation - A.16 Information security incident management	Noridah
1630	Review of Day 2 audit findings (if any)	SIRIM's auditors and client's representatives

Day 3

Time	Agenda	Responsibility
0930 - 1630	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 at Bahagian Kemasukan dan Bahagian Urus Tadbir Akedemik. 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 at Bahagian Hal Ehwal Pelajar.	Aisya
	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 at Fakulti Kejuruteraan dan Fakulti Rekabentuk dan Senibina. 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 at Kolej Sepuluh (K10) dan Kolej Tun Dr. Ismail (KTDI). ** (pindaan ke atas kolej)	Noridah
1630	Review of Day 3 audit findings (if any)	SIRIM's auditor & client's management

SURVEILLANCE 1 AUDIT PLAN

Day 4

Time	Agenda	Responsibility
0930 - 1500	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 at Pejabat Strategi Korporat & Komunikasi (covering A.17 information security business continuity management) 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 at Pejabat Penasihat Undang-Undang (covering A.18 compliance)	Aisya
1500 - 1600	Preparation of Report	SIRIM's auditors
1600	Closing Meeting. **(pindaan ke atas masa bagi mesyuarat penutup) Presentation of Findings and Recommendation	SIRIM's auditor & client's management
	-	
Note:	Notes: * Afternoon break will follow organization's break. * Operations will cover control A.8 Asset Management, A.9 Access Control, A.10 Cryptography, A.11 Physical and Environmental Security, A.12 Operations Security, A.13 Communications Security, A.14 System Acquisition, Development and Maintenance and A.15 Supplier Relationships. ** At least 50% of applicable controls as per the Statement of Applicability will be sampled that shall also consider the risk exposed as per the Risk Assessment Report and Risk Treatment Plan.	