INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS) ISO/IEC 27001:2015
AUDIT PLAN FOR REMOTE AUDIT

1. Type of Audit

Surveillance Audit

2. Audit objectives :

a) To review certification scheme documented information

b) To evaluate the implementation, including effectiveness, of the client's certification system

c) To evaluate the continued compliance of the client's certification system to the requirements of the standard and ability of the certification system to ensure client meets applicable statutory, regulatory and contractual requirements, where applicable

d) To confirm the continued conformity and effectiveness of the certification system as a whole, and its continued relevance and applicability for the scope of certification

e) To verify adequacy and effectiveness implementation of corrections and corrective actions to close NCR arising from the findings of previous audit

3. Date of audit : 30 November, 7 – 10 December 2020

4. Site of audit/Scope :

Universiti Putra Malaysia
43400 Serdang
Selangor

Scope:

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.

5. Audit criteria

a) ISO/IEC 27001:2013
b) Client's documentation

6. Audit team & role :

a)	Audit Team Leader	Nur Aisya Mohd. Zamri
b)	Auditors	-

7. Methodology of audit :

a) Remote audit (web conference e.g. SKYPE / Microsoft Teams, etc.)
b) Review of documentation and records
c) Observation of processes and activities
d) Interview with client's personnel responsible for the audited area
e) Information Communication Technology (ICT): example as followed
   - The virtual walkthrough will be conducted in real time using a videocall with Skype / WhatsApp / Zoom / GoToMeeting / MS Teams / Google Hangouts, etc. on a mobile phone / laptop / handheld device / wearable technology etc. that allows the auditor to cover the entire scope of certification.

8. 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

9. Working language : English and Bahasa Melayu

10. 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

11. Facilities and assistance required:

i) Guide and designated personnel (who may also be the auditee) to assist SIRIM audit team.

ii) Email, telephone, handphone and suitable electronic media platform shall be available.

iii) Ensure the documents and records are available and accessible during audit.

iv) A quiet environment to avoid interference and background noise.

12. List of documented information :

a) Organization policy and objectives.
b) Organization structure.
c) Evidence of previous audit findings (if applicable);
d) Risk assessment.
e) Results of internal and external audit (if applicable).
f) Minutes of management review.
g) Status of corrective actions including customer complaints.
h) Others (based on scheme)

13. Details of audit plan : As follows

DETAILS OF AUDIT PLAN

Day 1 / 5 (30 November 2020)		
Time	**Agenda**	**Responsibility**
0930–1000	**Opening Meeting.** • Briefing on the Information 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
1000–1630	Operation inclusive of operational planning and control, information security risk assessment, information security risk treatment and verification on the effectiveness of controls implemented from Annex A (organization's Statement of Applicability) in relation to Proses Penilaian Pengajaran Prasiswazah at: i. **Pusat Pembangunan Akademik** ii. **Fakulti Perubatan Veterinar** iii. **Fakulti Pengajian Pendidikan**.	Aisya and process owner
1630	Review of Day 1 Findings	SIRIM's auditors and client's representatives

Day 2 / 5 (7 November 2020)		
Time	**Agenda**	**Responsibility**
0930- 1530	Review of documentation against requirements of ISO/IEC 27001:2013. Audit on the activities related to following requirements: • Documented information inclusive of creating and updating and control of documented information. • Context of the organization - 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 risks and opportunities, and quality objectives and plans to achieve them. • Performance evaluation inclusive of monitoring, measurement, analysis and evaluation, and implementation of internal audit and management review. **Pusat Jaminan Kualiti**	Aisya and process owner

Day 2 / 5 (7 November 2020)		
Time	**Agenda**	**Responsibility**
	• Improvement inclusive of nonconformity and corrective action and continual improvement. *Expected document/records to be sighted:* • *ISMS Manual, Scope document, risk assessment report, risk treatment plan, information security policies, security objectives measurement, internal audit related records, management review related records, and other related document/records which relevant with the above audit requirement.*	
1630	Review Day 2 audit findings (if any).	SIRIM's auditor & client's management

Day 3 / 5 (8 November 2020)		
Time	**Agenda**	**Responsibility**
0930 - 1630	**Operation** inclusive of operational planning and control, information security risk assessment, information security risk treatment and verification on the effectiveness of controls implemented from Annex A (organization's Statement of Applicability) in relation to **Pusat Pembangunan Maklumat dan Komunikasi (IDEC)**, including security control A.16 Information Security Incident Management. *Expected document/records to be sighted:* *Risk assessment report, risk treatment plan, access control, backup management, change management, preventive maintenance, incident management, demonstration on related activities for the above system and other related document/records which relevant with the above audit requirement.* **Virtual site visit to Server Room**. *Expected document/records to be sighted:* *Logbook, access door, physical facilities in Data Centre*	Aisya and process owner
1630	Review Day 3 audit findings (if any).	SIRIM's auditor & client's management

Day 4 / 5 (9 November 2020)		
Time	**Agenda**	**Responsibility**
0930 - 1630	Virtual site visit to Offsite Backup Storage (**Perpustakaan dan iDEC**). Operation inclusive of operational planning and control, information security risk assessment, information security risk treatment and verification on the effectiveness of controls implemented from Annex A (organization's Statement of Applicability) in relation to: • Proses Pendaftaran Pelajar Baharu Prasiswazah at Bahagian Hal Ehwal Pelajar. • A.17 Information Security in the aspect of Business Continuity Management at **Pejabat Strategi Korporat & Komunikasi**. *Expected document/records to be sighted:* *Risk assessment report, risk treatment plan, demonstration on related activities for the above system and other related document/records which relevant with the above audit requirement.*	Aisya and process owner
1630	Review Day 4 audit findings (if any).	SIRIM's auditor & client's management

Day 5 / 5 (10 December 2020)		
Time	**Agenda**	**Responsibility**
0930 -1500	Operation inclusive of operational planning and control, information security risk assessment, information security risk treatment and verification on the effectiveness of controls implemented from Annex A (organization's Statement of Applicability) in relation to Proses Pendaftaran Pelajar Baharu Prasiswazah at: • **Kolej Tujuh Belas** • **Kolej Pendeta Za'aba** *Expected document/records to be sighted:* *Risk assessment report, risk treatment plan, demonstration on related activities for the above system and other related document/records which relevant with the above audit requirement*	Aisya and process owner
1500 -1630	Consolidation of audit findings and preparation of audit report	SIRIM's auditors

Day 5 / 5 (10 December 2020)		
Time	**Agenda**	**Responsibility**
1600	**Closing Meeting.** Presentation of Findings and Recommendation.	SIRIM's auditor & client's management

Notes

- *Audit processes will include actions taken to address risks and opportunities, its effectiveness.*
- *Verification of previous audit findings will be conducted during the audit by respective auditors.*
- *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, Maintenance and A.15 Supplier Relationships and A.16 Information Security Incident Management.*
- *Audit is based on sample basis.*
- *Lunch break will follow organization time.*