Information Security Management System MS ISO/IEC 27001:2007

INTERNAL AUDIT PROCEDURE

PROSEDUR AUDIT DALAM

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
Pn. Ummi Naiemah Saraih	Pn. Rohazna Wahab Deputy Director ICT	En. Nasrudin Abd. Shukor Director ICT Division ISMR

For Dept Use Only

Date: 11th October 2012 **Version 1.0**

Revision History

No	Date of Change	Description	Page	Version	Approved By

1.0 PURPOSE
1.0 TUJUAN

The purpose of this procedure is to:
Prosedur ini bertujuan untuk:

(i) To ensure that University Malaysia Perlis continually operates in accordance with the specified policies, procedures and external requirements in meeting its goals and objectives in relation to information security.

(i) Untuk memastikan bahawa Universiti Malaysia Perlis terus beroperasi selaras dengan dasar-dasar, prosedur-prosedur dan keperluan-keperluan luaran yang telah di tetapkan dalam memenuhi matlamat-matlamat dan objektif-objektif universiti berkaitan dengan keselamatan maklumat.

(ii) Determine the effectiveness of the Information Security Management System.

(ii) Menentukan keberkesanan Sistem Pengurusan Keselamatan Maklumat.

(iii) To determine compliance to legal, MS ISO/IEC 27001:2007 Standard and university's own policies and procedures.

(iii) Untuk memastikan pematuhan kepada perundangan, piawaian MS ISO/IEC 27001:2007 serta dasar-dasar dan prosedur- prosedur universiti.

2.0 SCOPE
2.0 SKOP

This procedure includes scheduling, planning, preparing, performing, reporting and follow-up of an internal ISMS audit for University Malaysia Perlis, Information and Communication Technology Centre that form the centre of the university's information security management system.

Prosedur ini merangkumi penjadualan, perancangan, penyediaan, pelaksanaaan, pelaporan dan audit dalam susulan ISMS untuk Pusat Teknologi Maklumat dan Komunikasi, Universiti Malaysia Perlis yang merupakan pusat bagi sistem pengurusan keselamatan maklumat universiti.

3.0 DEFINITION
3.0 DEFINISI

ISMS *ISMS*	► Information Security Management System ► *Sistem Pengurusan Keselamatan Maklumat*
ISMS Internal Audit Audit *Audit Dalam ISMS*	► Information Security Management System Internal ► *Audit Dalam Sistem Pengurusan Keselamatan Maklumat*
Auditee *Auditee*	► An organization or department to be audited ►*Organisasi atau jabatan di bawah skop perkhidmatan yang akan diaudit.*
NC *NC*	► Non-Conformity ► *Ketakakuran*
NCR *NCR*	► Non-Conformance Report ► *Laporan Ketakakuran*
LA *LA*	► Lead Auditor ► *Ketua Pasukan Audit Dalam*
IA *IA*	► Internal Auditor ► *Juruaudit Dalam*
ISMR *ISMR*	► Information Security Management Representative ► *Wakil Pengurusan Keselamatan Maklumat*

4.0 PROCEDURE DETAILS
4.0 BUTIR-BUTIR PROSEDUR

4.1 Scheduling, Planning and Preparing the Audit
4.1 Penjadualan, Perancangandan Penyediaan Audit

4.1.1 The Lead Auditor shall prepare the audit plan(s).

4.1.2 The Audit Plan/Notification shall be prepared by the Lead Auditor, and reviewed and accepted by the Information Security Management Representative (ISMR). The plan shall include:

- Audit objective and scope, including the information management system(s) to be audited.
- Department/Section and responsible individuals in charge.

4.1.1 Ketua pasukan audit akan menyediakan perancangan audit.

4.1.2 Rancangan/pemberitahuan Audit akan disediakan oleh ketua pasukan audit, dan dikaji semula dan diterima oleh Wakil Pengurusan Keselamatan Maklumat (ISMR). Rancangan tersebut akan mengandungi:

- *Skop dan objektif audit, termasuk sistem pengurusan maklumat yang akan di audit.*
- *Jabatan/Seksyen dan individu-individu bertugas yang dipertanggungjawabkan.*

4.2 Pre-audit Meeting
4.2 Mesyuarat Pra Audit

4.2.1 Pre-Audit meeting between the ISMR and Lead Auditor (and other auditors as applicable) shall be carried-out prior to the start of the audit. Objectives are as follows:

- To ensure the availability of all the resources needed and other logistics that may be required by the auditor.
- The scope of the audit is consistent with the Audit Plan

4.2.1 Mesyuarat Pra Audit diantara ISMR dan ketua pasukan audit (dan juruaudit-juruaudit lain yang berkenaan) akan dijalankan sebelum permulaan audit. Objektif-objektif ialah seperti berikut:

- *Untuk memastikan ketersediaan semua sumber-sumber yang diperlukan dan*
- *lain-lain keperluan logistik yang mungkin diperlukan oleh juruaudit.*
- *Skop audit adalah konsisten dengan Rancangan Audit.*

4.3 Opening Meeting
4.3 Mesyuarat Pembukaan

4.3.1 Opening meeting, where deemed appropriate by the ISMR and Lead Auditor, shall be held on the day of the start of the audit. The following may be discussed during the opening meeting:

- The purpose and scope of the audit.
- Confirmation of the audit plan
- Clarification of other matters that must be settled before the audit takes place.

4.3.1 Mesyuarat pembukaan, di mana dianggap sesuai oleh ISMR dan ketua pasukan audit, akan diadakan pada hari permulaan audit. Perkara berikut mungkin dibincangkan semasa mesyuarat pembukaan:

- *Tujuan dan skop audit*
- *Pengesahan rancangan audit*
- *Penjelasan untuk perkara-perkara lain yang mesti diselesaikan sebelum audit dimulakan*

4.4 Audit Performing
4.4 Pelaksanaan Audit

4.4.1 Audit findings are determined through interviews, examination of documents and observation of activities and conditions in the areas of concern and will be documented.

Objective evidence to support identified major or minor non-conformities shall be obtained and documented in audit work papers.

4.4.1 Penemuan-penemuan audit dipastikan melalui temu bual, pemeriksaan dokumen-dokumen dan pemerhatian aktiviti-aktiviti dan syarat-syarat dalam perkara berkenaan dan akan didokumenkan.

Bukti objektif untuk menyokong ketakakuran major atau minor yang dikenal pasti akan diperolehi dan didokumenkan dalam kertas-kertas kerja audit.

4.5 Audit Reporting
4.5 Pelaporan Audit

4.5.1 The auditors shall have a pre-closing meeting at the conclusion of the audit. Agenda includes:

- Review and analysis of findings
- Consolidation of all findings including grouping and tabulation.
- Classification of findings (see below 1.6.4)
- Preparation of recommendations and audit report

4.5.2 The audit team shall review all of their findings to determine whether they are to be reported as non-conformities or as observations. Audit findings shall be supported by objective evidence.

4.5.3 The Lead Auditor consolidates all the audit findings for the preparation of the audit report.

4.5.4 Classification of findings shall be:

Major non-conformity – This pertains to a major deficiency in the ISMS. Non-conformity exists if one or more elements of the ISO 27001 is not implemented. Non-conformities have a direct effect on information security, specifically on the preservation of confidentiality, integrity and availability of information assets.

Minor non-conformity – A minor deficiency. One or more elements of the ISMS is/are only partially complied with. Minor non-conformities have an indirect effect on information security.

Note: Both major and minor non-conformities shall require the appropriate area's management to document corrective actions.

4.5.1 Juruaudit-juruaudit akan mengadakan mesyuarat pra penutupan apabila audit selesai. Agenda termasuk:

- *Menyemak semula dan menganalisis penemuan-penemuan*
- *Menggabungkan semua penemuan termasuk kumpulan dan penjadualan*
- *Klasifikasi penemuan-penemuan (lihat 1.6.4)*
- *Menyediakan cadangan-cadangan dan laporan audit*

4.5.2 Pasukan audit akan mengkaji semula kesemua penemuan-penemuan untuk menentukan sama ada ianya akan dilaporkan sebagai ketakakuran atau pemerhatian. Penemuan-penemuan audit akan disokong oleh bukti objektif.

4.5.3 Ketua pasukan audit akan manggabungkan kesemua penemuan untuk menyediakan laporan audit.

4.5.4 Klasifikasi penemuan:

***Ketakakuran major –** Merujuk kepada kekurangan utama dalam ISMS.*

Ketakakuran wujud jika satu atau lebih unsur-unsur ISO 27001 tidak dilaksanakan. Ketakakuran mempunyai akibat langsung ke atas keselamatan maklumat, khususnya ke atas pemeliharaan kerahsiaan, integriti dan ketersediaan asset-aset maklumat.

Ketakakuran minor - *Merupakan kekurangan kecil. Satu atau lebih unsur-unsur mematuhi hanya sebahagian keperluan ISMS. Ketakakuran minor mempunyai kesan tidak langsung ke atas keselamatan maklumat.*

Nota: Kedua-dua ketakakuran major dan minor memerlukan bahagian pengurusan yang berkenaan untuk mendokumenkan tindakan-tindakan pembetulan.

Potential improvements – An audit recommendation for improvement for consideration by the auditee.

Note: Potential improvements which pertain to information security weaknesses shall require appropriate preventive actions to be documented, or be upgraded to non-conformity.

Positive findings – Findings that pertain to processes and/or systems that go beyond what is required by the standard.

4.5.5 The Lead Auditor shall prepare a standard internal audit report that may contain the following information.

- Audit Reference Number
- Date of Audit
- Department/Section Audited/Process Name
- Name of Auditee and auditors
- Statement of findings (all non-conformities found)
- Reference to the information security management system and standard
- Corrective and Preventive Actions with completion date
- Follow-up actions for non-conformities
- Verification of follow-up actions

4.5.6 The auditors shall follow a code of conduct in the manner of reporting as stated in this document.

- The report should be concise but factual and presented in a constructive manner.
- The findings should be within the scope of audit and show the relationship of the standard used.
- The report should not show bias by the auditor.

4.5.7 The Lead Auditor shall issue a formal Audit Report to the ISMR.

Potensi untuk penambahbaikan *– Cadangan audit untuk penambahbaikan untuk dipertimbangkan oleh auditee.*

Nota: Potensi untuk penambaikan yang berkaitan dengan kelemahan-kelemahan keselamatan maklumat akan memerlukan tindakan pencegahan yang bersesuaian untuk didokumentasikan, atau dinaik taraf kepada ketakakuran.

Penemuan-penemuan positif- *Penemuan-penemuan yang berkaitan dengan proses-proses dan / atau sistem-sistem yang melampaui keperluan piawaian.*

4.5.5 Ketua pasukan audit akan menyediakan laporan audit dalaman piawaian yang boleh mengandungi maklumat berikut:

- *Nombor Rujukan Audit*
- *Tarikh Audit*
- *Nama Jabatan/Bahagian Yang Diaudit/Proses*
- *Nama Auditee Dan Juruaudit-Juruaudit*
- *Penyataan Penemuan-Penemuan (Kesemua Penemuan-Penemuan Yang Ditemui)*
- *Rujukan Kepada Sistem Pengurusan Keselamatan Maklumat Dan Piawaian*
- *Tindakan Pembetulan dan Pencegahan Beserta Tarikh Selesai*
- *Tindakan-Tindakan Susulan Untuk Ketakakuran*
- *Pengesahan Tindakan-Tindakan Susulan*

4.5.6 Juruaudit-juruaudit akan mengikut tatacara pelaporan seperti yang dinyatakan dalam dokumen ini.

- *Laporan harus ringkas dan padat tetapi berfakta dan disampaikan dengan cara yang membina.*
- *Penemuan-penemuan harus berada dalam skop audit dan menunjukkan hubungan piawaian yang digunakan.*
- *Laporan tidak boleh menunjukkan kecenderungan juruaudit.*

4.5.7 Ketua pasukan audit akan menghantar Laporan Audit Rasmi kepada ISMR.

4.6 Closing Meeting
4.6 Mesyuarat Penutup

4.6.1 The Lead Auditor shall preside over the closing meeting attended by the audit team and the auditees. The auditors shall report their findings, observations

and recommendations.

4.6.1 Ketua pasukan audit akan mengetuai mesyuarat penutup yang dihadiri oleh pasukan audit dan auditees. Juruaudit-juruaudit akan melaporkan penemuan-penemuan, pemerhatian-pemerhatian dan cadangan-cadangan masing-masing.

4.7 Corrective Action Follow-up
4.7 Susulan Tindakan Pembetulan

1.8.1 The auditor is only responsible for identifying the non-conformitiesand following up on corrective actions implemented by the responsible area management.

1.8.2 The auditees are responsible for determining the root cause and correcting the reported non-conformities.

1.8.3 Approved corrective actions shall be based on the agreed time scale.

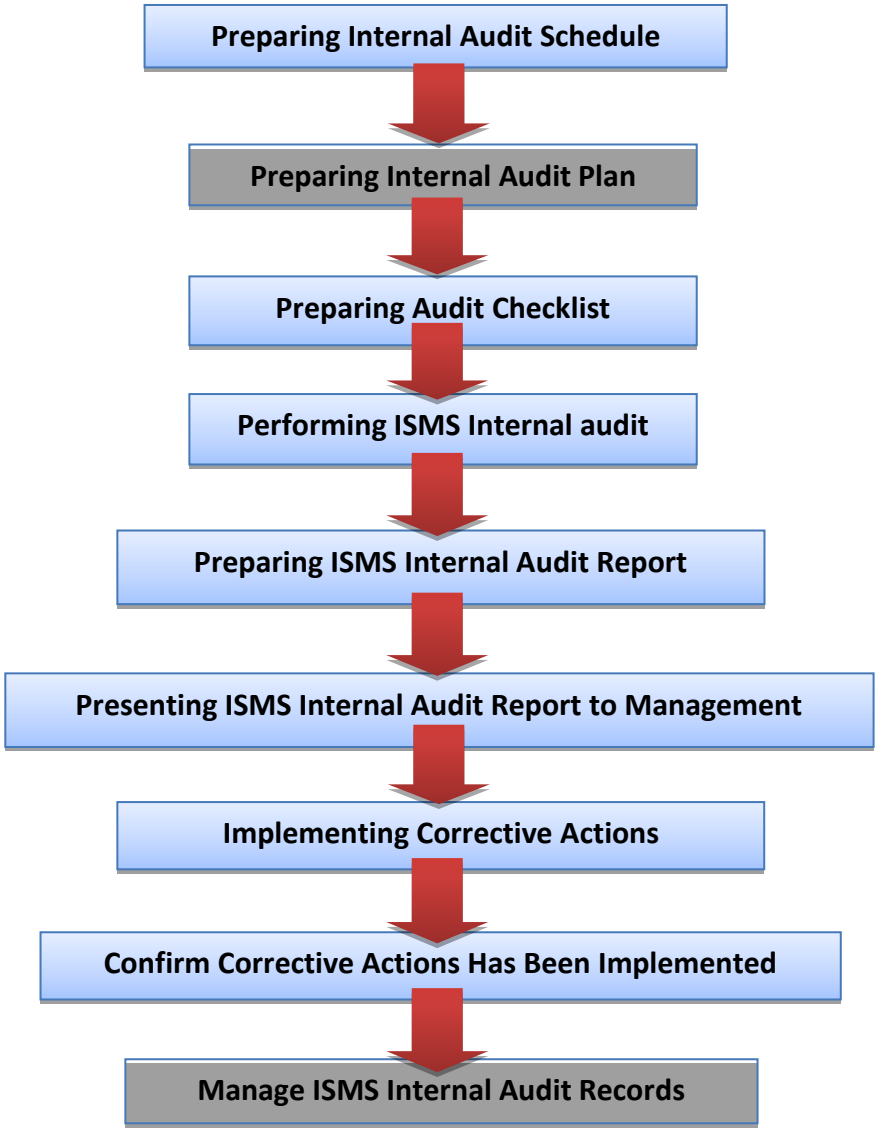
1.8.1 Juruaudit hanya bertanggungjawab untuk mengenalpasti ketakakuran dan membuat susulan bagi memastikan tindakan pembetulan dilaksanakan oleh bahagian pengurusan yang bertanggungjawab.

1.8.2 Auditees bertanggungjawab untuk menentukan punca dan membetulkan ketakakuran yang dilaporkan.

1.8.3 Tindakan pembetulan yang diluluskan akan berdasarkan skala masa yang dipersetujui.

5.0 PROCESS FLOW

5.0 ALIRAN PROSES



6.0 OTHERS

6.0 LAIN-LAIN

6.1 Classification of Audit Findings
6.1 Klasifikasi Penemuan-Penemuan Audit

Audit findings shall be classified as follows:
Penemuan-penemuan audit akan diklasifikasikan seperti berikut:

(i) Satisfactory (SA)
No deficiencies observed

(i) Memuaskan (SA)
Tiada kekurangan-kekurangan yang dijumpai

(ii) Observation (Obs)
The procedure or practice could be improved to provide better assurance

(ii) Pemerhatian (Obs)
Prosedur atau amalan boleh dipertingkatkan bagi memberi jaminan yang lebih baik

(iii) Non-conformance(NCR)
The basic intent has not been carried out and cause failure or an inability to achieve agreed requirements
To be reviewed in next internal security audit.

(iii) Ketakakuran (NCR)
Tujuan asas belum dijalankan dan menyebabkan kegagalan atau tidak dapat mencapai keperluan-keperluan yang dipersetujui.
Akan disemak semula semasa audit dalam keselamatan yang akan datang.

6.2 Frequency of ISMS Audit
6.2 Kekerapan Audit ISMS

For each functional activity, the frequency of ISMS Audit shall be determined based on the importance of the activity & the findings of previous audits. However, each department/function/process is subject to be audited at least once a year.

Untuk setiap aktiviti fungsi, kekerapan Audit ISMS akan ditentukan berdasarkan kepentingan aktiviti & penemuan-penemuan audit sebelumnya. Bagaimanapun, setiap bahagian / fungsi / proses tertakluk kepada audit sekurang-kurangnya sekali dalam setahun.

6.3 Internal Audit Memo
6.3 Memo Audit Dalam

The content of the Internal Audit Memo should cover but not limited to the following:
Kandungan Memo Audit Dalam harus merangkumi tetapi tidak dihadkan kepada berikut:

(i) Audit criteria
(i) Kriteria Audit

(ii) Scope of audit
(ii) Skop audit

(iii) Purpose
(iii) Tujuan

(iv) Date
(iv) Tarikh

(v) Auditor Assigned
(v) Juruaudit yang Ditugaskan