

**MAURITIAN
STANDARD**

**MS ISO/IEC
27007:2017**

Second Edition
2019-02-23

**Information technology --
Security techniques -- Guidelines
for information security
management systems auditing**

ICS: 03.100.70; 35.030



**Mauritius Standards Bureau
Moka**

National foreword

This Mauritian Standard is identical with the International Standard ISO/IEC 27007:2017, *Information technology -- Security techniques -- Guidelines for information security management systems auditing*

It has been adopted as a national standard upon the recommendation of the **Information Technology Standards Committee**.

It was approved by the Standards Council on 29 January 2019 and was notified in the Government Gazette on 23 February 2019.

This Mauritian Standard cancels and replaces the Mauritian Standard MS/ISO/IEC 27007:2011, which has been technically revised.

For the purpose of this standard the following changes should be made:

- (i) the words 'International Standard' should be replaced by 'Mauritian Standard'
- (ii) the 'decimal comma' should be replaced by 'decimal point'.

The main changes compared to the previous edition are:

- Annex A has been completely reworked to align to ISO/IEC 27001:2013;
- the main part of this document has been aligned with ISO/IEC 27001:2013.

General Notice No 258 of 2019



COPYRIGHT PROTECTED DOCUMENT

© MSB 2019

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission from Mauritius Standards Bureau at the address below

*Mauritius Standards Bureau
Villa Road
Moka
Mauritius*

Telephone + (230) 433 3648
Fax + (230) 433 5051/ 433 5150

E-mail msb@intnet.mu
Website <http://msb.intnet.mu>

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles of auditing	1
5 Managing an audit programme	1
5.1 General.....	1
5.1.1 IS 5.1 General.....	2
5.2 Establishing the audit programme objectives.....	2
5.2.1 IS 5.2 Establishing the audit programme objectives.....	2
5.3 Establishing the audit programme.....	2
5.3.1 Role and responsibilities of the person managing the audit programme.....	2
5.3.2 Competence of the person managing the audit programme.....	2
5.3.3 Establishing the extent of the audit programme.....	2
5.3.4 Identifying and evaluating audit programme risks.....	3
5.3.5 Establishing procedures for the audit programme.....	3
5.3.6 Identifying audit programme resources.....	3
5.4 Implementing the audit programme.....	4
5.4.1 General.....	4
5.4.2 Defining the objectives, scope and criteria for an individual audit.....	4
5.4.3 Selecting the audit methods.....	4
5.4.4 Selecting the audit team members.....	5
5.4.5 Assigning responsibility for an individual audit to the audit team leader.....	5
5.4.6 Managing the audit programme outcome.....	5
5.4.7 Managing and maintaining audit programme records.....	5
5.5 Monitoring the audit programme.....	5
5.6 Reviewing and improving the audit programme.....	5
6 Performing an audit	5
6.1 General.....	5
6.2 Initiating the audit.....	5
6.2.1 General.....	5
6.2.2 Establishing initial contact with the auditee.....	5
6.2.3 Determining the feasibility of the audit.....	6
6.3 Preparing audit activities.....	6
6.3.1 Performing document review in preparation for the audit.....	6
6.3.2 Preparing the audit plan.....	6
6.3.3 Assigning work to the audit team.....	6
6.3.4 Preparing work documents.....	6
6.4 Conducting the audit activities.....	7
6.4.1 General.....	7
6.4.2 Conducting the opening meeting.....	7
6.4.3 Performing document review while conducting the audit.....	7
6.4.4 Communicating during the audit.....	7
6.4.5 Assigning roles and responsibilities of guides and observers.....	7
6.4.6 Collecting and verifying information.....	7
6.4.7 Generating audit findings.....	8
6.4.8 Preparing audit conclusions.....	8
6.4.9 Conducting the closing meeting.....	8
6.5 Preparing and distributing the audit report.....	8
6.5.1 Preparing the audit report.....	8
6.5.2 Distributing the audit report.....	8

6.6	Completing the audit	8
6.7	Conducting audit follow-up	8
7	Competence and evaluation of auditors	8
7.1	General	8
7.2	Determining auditor competence to fulfil the needs of the audit programme	9
7.2.1	General	9
7.2.2	Personal behaviour	9
7.2.3	Knowledge and skills	9
7.2.4	Achieving auditor competence	9
7.2.5	Audit team leader	10
7.3	Establishing the auditor evaluation criteria	10
7.4	Selecting the appropriate auditor evaluation method	10
7.5	Conducting auditor evaluation	10
7.6	Maintaining and improving auditor competence	10
	Annex A (informative) Guidance for ISMS auditing practice	11
	Bibliography	41

PREVIEW

Introduction

This document provides guidance on:

- a) the management of an information security management system (ISMS) audit programme;
- b) the conduct of internal and external ISMS audits in accordance with ISO/IEC 27001;
- c) the competence and evaluation of ISMS auditors.

This document should be used in conjunction with the guidance contained in ISO 19011:2011.

This document follows the structure of ISO 19011:2011. Additional ISMS-specific guidance on the application of ISO 19011:2011 for ISMS audits is identified by the letters "IS".

ISO 19011:2011 provides guidance on the management of audit programmes, the conduct of internal or external audits of management systems, as well as on the competence and evaluation of management system auditors.

NOTE For accredited certification, auditor requirements are given in ISO/IEC 27006.

This document does not state requirements and is intended for all users, including small and medium-sized organizations.

PREVIEW

Information technology — Security techniques — Guidelines for information security management systems auditing

1 Scope

This document provides guidance on managing an information security management system (ISMS) audit programme, on conducting audits, and on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011:2011.

This document is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 19011:2011, *Guidelines for auditing management systems*

ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 19011:2011 and ISO/IEC 27000 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <http://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

4 Principles of auditing

The principles of auditing of ISO 19011:2011, Clause 4 apply.

5 Managing an audit programme

5.1 General

The guidelines of ISO 19011:2011, 5.1 apply. In addition, the following guidance applies.