

**MAURITIAN
STANDARD**

**MS ISO/IEC
27005:2018**

Third Edition
2019-07-19

**Information technology - Security
techniques - Information security risk
management**

ICS: 03.100.70 Management systems 35.030 IT Security



**Mauritius Standards Bureau
Moka**

National foreword

This Mauritian Standard is identical with the International Standard ISO/IEC 27005:2018, **Information technology -- Security techniques -- Information security risk management**

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 30 May 2019 and was notified in the Government Gazette on 19 July 2019*.

This Mauritian Standard cancels and replaces the Mauritian Standard MS ISO/IEC 27005:2011, 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'

The main changes compared to the previous edition are:

- all direct references to the MS ISO/IEC 27001:2005 have been removed;
- clear information has been added that this document does not contain direct guidance on the implementation of the ISMS requirements specified in MS ISO/IEC 27001 (see Introduction);
- MS ISO/IEC 27001:2005 has been removed from Clause 2;
- MS ISO/IEC 27001 has been added to the Bibliography;
- Annex G and all references to it have been removed;
- editorial changes have been made accordingly.

* General Notice No 1281 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 Structure of this document	1
5 Background	2
6 Overview of the information security risk management process	3
7 Context establishment	5
7.1 General considerations.....	5
7.2 Basic criteria.....	6
7.2.1 Risk management approach.....	6
7.2.2 Risk evaluation criteria.....	6
7.2.3 Impact criteria.....	6
7.2.4 Risk acceptance criteria.....	7
7.3 Scope and boundaries.....	7
7.4 Organization for information security risk management.....	8
8 Information security risk assessment	8
8.1 General description of information security risk assessment.....	8
8.2 Risk identification.....	9
8.2.1 Introduction to risk identification.....	9
8.2.2 Identification of assets.....	9
8.2.3 Identification of threats.....	10
8.2.4 Identification of existing controls.....	10
8.2.5 Identification of vulnerabilities.....	11
8.2.6 Identification of consequences.....	12
8.3 Risk analysis.....	12
8.3.1 Risk analysis methodologies.....	12
8.3.2 Assessment of consequences.....	13
8.3.3 Assessment of incident likelihood.....	14
8.3.4 Level of risk determination.....	15
8.4 Risk evaluation.....	15
9 Information security risk treatment	16
9.1 General description of risk treatment.....	16
9.2 Risk modification.....	18
9.3 Risk retention.....	19
9.4 Risk avoidance.....	19
9.5 Risk sharing.....	19
10 Information security risk acceptance	20
11 Information security risk communication and consultation	20
12 Information security risk monitoring and review	21
12.1 Monitoring and review of risk factors.....	21
12.2 Risk management monitoring, review and improvement.....	22
Annex A (informative) Defining the scope and boundaries of the information security risk management process	24
Annex B (informative) Identification and valuation of assets and impact assessment	28
Annex C (informative) Examples of typical threats	37

Annex D (informative) Vulnerabilities and methods for vulnerability assessment	41
Annex E (informative) Information security risk assessment approaches	45
Annex F (informative) Constraints for risk modification	51
Bibliography	53

PREVIEW

Introduction

This document provides guidelines for information security risk management in an organization. However, this document does not provide any specific method for information security risk management. It is up to the organization to define their approach to risk management, depending for example on the scope of an information security management system (ISMS), context of risk management, or industry sector. A number of existing methodologies can be used under the framework described in this document to implement the requirements of an ISMS. This document is based on the asset, threat and vulnerability risk identification method that is no longer required by ISO/IEC 27001. There are some other approaches that can be used.

This document does not contain direct guidance on the implementation of the ISMS requirements given in ISO/IEC 27001.

This document is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

PREVIEW

Information technology — Security techniques — Information security risk management

1 Scope

This document provides guidelines for information security risk management.

This document supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach.

Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this document.

This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that can compromise the organization's information security.

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

3 Terms and definitions

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

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

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

4 Structure of this document

This document contains the description of the information security risk management process and its activities.

The background information is provided in [Clause 5](#).

A general overview of the information security risk management process is given in [Clause 6](#).

All information security risk management activities as presented in [Clause 6](#) are subsequently described in the following clauses:

- context establishment in [Clause 7](#);
- risk assessment in [Clause 8](#);
- risk treatment in [Clause 9](#);