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

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

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.

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;