MAURITIAN STANDARD

MS ISO/IEC 27021:2017

First Edition
2019-02-23

Information technology -- Security techniques -- Competence requirements for information security management systems professionals

PREVIEW

ICS: 03.100.70; 35.030

Mauritius Standards Bureau
Moka

© MSB 2019

National foreword

This Mauritian Standard is identical with the International Standard ISO /IEC 27021:2017, ***Information technology -- Security techniques -- Competence requirements for information security management systems professionals***

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.

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'.

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*

PREVIEW

© MSB 2019 – All rights reserved

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**

4 Concept and structure ... **1**
4.1 General ... 1
4.2 Concept of ISMS competence ... 2
4.3 Structure of ISMS competence ... 2
4.4 Demonstration of competence ... 3
4.5 Structure of this document ... 3

5 Business management competence for ISMS Professionals ... **3**
5.1 General ... 3
5.2 Competence: Leadership ... 3
5.3 Competence: Communication ... 4
5.4 Competence: Business Strategy and ISMS ... 4
5.5 Competence: Organization design, culture, behaviour and stakeholder management ... 5
5.6 Competence: Process design and organizational change management ... 5
5.7 Competence: Human Resource, team and individual management ... 6
5.8 Competence: Risk management ... 6
5.9 Competence: Resource management ... 7
5.10 Competence: Information systems architecture ... 7
5.11 Competence: Project and portfolio management ... 8
5.12 Competence: Supplier management ... 8
5.13 Competence: Problem management ... 8

6 Information security competence for ISMS professionals ... **9**
6.1 ISMS Competence: Information Security ... 9
6.1.1 General ... 9
6.1.2 Competence: Information security governance ... 9
6.1.3 Competence: Context of the organization ... 9
6.2 ISMS Competence: Information Security Planning ... 10
6.2.1 General ... 10
6.2.2 Competence: Scope of ISMS ... 10
6.2.3 Competence: Information security risk assessment and treatment ... 11
6.3 ISMS Competence: Information Security Operation ... 11
6.3.1 General ... 11
6.3.2 Competence: Information security operations ... 12
6.4 ISMS Competence: Information Security Support ... 12
6.4.1 General ... 12
6.4.2 Competence: Information security awareness, education and training ... 13
6.4.3 Competence: Documentation ... 13
6.5 ISMS Competence: Information Security Performance evaluation ... 13
6.5.1 General ... 13
6.5.2 Competence: ISMS monitoring, measurement, analysis and evaluation ... 14
6.5.3 Competence: ISMS auditing ... 14
6.5.4 Competence: Management review ... 15
6.6 ISMS Competence: Information Security Improvement ... 15
6.6.1 General ... 15
6.6.2 Competence: Continual improvement ... 15
6.6.3 Competence: Technological trends and developments ... 16

Annex A (informative) **Including knowledge for ISMS professionals as part of a body of knowledge** ... **17**

PREVIEW

© ISO/IEC 2017 – All rights reserved

Bibliography **21**

PREVIEW

 © ISO/IEC 2017 – All rights reserved

Introduction

This document is intended for use by:

a) individuals who would like to demonstrate their competence as information security management system (ISMS) professionals, or who wish to understand and accomplish the competence required for working in this area, as well as wishing to broaden their knowledge,

b) organizations seeking potential ISMS professional candidates to define the competence required for positions in ISMS related roles,

c) bodies to develop certification for ISMS professionals which need a body of knowledge (BOK) for examination sources, and

d) organizations for education and training, such as universities and vocational institutions, to align their syllabuses and courses to the competence requirements for ISMS professionals.

This document should be read and used in conjunction with ISO/IEC 27001.

PREVIEW

© ISO/IEC 2017 – All rights reserved

Information technology — Security techniques — Competence requirements for information security management systems professionals

1 Scope

This document specifies the requirements of competence for ISMS professionals leading or involved in establishing, implementing, maintaining and continually improving one or more information security management system processes that conforms to ISO/IEC 27001.

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 http://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
competence
ability to apply knowledge and skills to achieve intended results

[SOURCE: ISO/IEC 17024:2012, 3.6]

3.2
information security management system professional
ISMS professional
person who establishes, implements, maintains and continually improves one or more information security management system processes

4 Concept and structure

4.1 General

ISMS professionals are people whose role is to manage the establishment, implementation, maintenance and continual improvement of one or more ISMS processes. They shall have and maintain knowledge and skills required in this document to fulfil their role successfully.

PREVIEW

© ISO/IEC 2017 – All rights reserved