BS ISO/IEC 27021:2017+A1:2021

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27021:2017+A1:2021

National foreword

This British Standard is the UK implementation of ISO/IEC 27021:2017+A1:2021. It supersedes BS ISO/IEC 27021:2017, which is withdrawn.

The start and finish of text introduced or altered by amendment is indicated in the text by tags. Tags indicating changes to ISO/IEC text carry the number of the ISO/IEC amendment. For example, text altered by ISO/IEC amendment 1 is indicated by 〖A1〉 〈A1〗.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management Systems.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2021
Published by BSI Standards Limited 2021

ISBN 978 0 539 05412 5

ICS 03.100.70; 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2017.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2021	Implementation of ISO/IEC amendment 1:2021

AVA Documents Document Sharing Hub

Full document details: BS ISO/IEC 27021:2017+A1:2021

BS ISO/IEC 27021:2017+A1:2021

INTERNATIONAL STANDARD

ISO/IEC 27021

First edition
2017-10-18

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

Technologies de l'information — Tecniques de sécurité — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité

Reference number
ISO/IEC 27021:2017(E)

Documents
Document Sharing Hub
© ISO/IEC 2017

Full document details: BS ISO/IEC 27021:2017+A1:2021

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Documents
Document Sharing Hub

© ISO/IEC 2017 – All rights reserved

Full document details: BS ISO/IEC 27021:2017+A1:2021

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 5
5.8 Competence: Risk management 6
5.9 Competence: Resource management 6
5.10 Competence: Information systems architecture 7
5.11 Competence: Project and portfolio management 7
5.12 Competence: Supplier management 8
5.13 Competence: Problem management 8
6 Information security competence for ISMS professionals **8**
6.1 ISMS Competence: Information Security 8
6.1.1 General 8
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 10
6.3 ISMS Competence: Information Security Operation 11
6.3.1 General 11
6.3.2 Competence: Information security operations 11
6.4 ISMS Competence: Information Security Support 12
6.4.1 General 12
6.4.2 Competence: Information security awareness, education and training 12
6.4.3 Competence: Documentation 12
6.5 ISMS Competence: Information Security Performance evaluation 13
6.5.1 General 13
6.5.2 Competence: ISMS monitoring, measurement, analysis and evaluation 13
6.5.3 Competence: ISMS auditing 13
6.5.4 Competence: Management review 14
6.6 ISMS Competence: Information Security Improvement 14
6.6.1 General 14
6.6.2 Competence: Continual improvement 14
6.6.3 Competence: Technological trends and developments 15
Annex A (informative) **Including knowledge for ISMS professionals as part of a body of knowledge** **16**

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27021:2017+A1:2021

Bibliography **20**

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27021:2017+A1:2021

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27021:2017+A1:2021

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.

© ISO/IEC 2017 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27021:2017+A1:2021

INTERNATIONAL STANDARD **ISO/IEC 27021:2017+A1:2021(E)**

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.

© ISO/IEC 2017 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27021:2017+A1:2021