INTERNATIONAL STANDARD

ISO/IEC 27005

Redline version
compares Third edition to
Second edition

Information technology — Security techniques — Information security risk management

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018

Reference number
ISO/IEC 27005:redline:2018(E)

© ISO/IEC 2018

IMPORTANT — PLEASE NOTE

This is a mark-up copy and uses the following colour coding:

Text example 1 — indicates added text (in green)

~~Text example 2~~ — indicates removed text (in red)

— indicates added graphic figure

— indicates removed graphic figure

1.x ... — Heading numbers containg modifications are highlighted in yellow in the Table of Contents

DISCLAIMER

This Redline version provides you with a quick and easy way to compare the main changes between this edition of the standard and its previous edition. It doesn't capture all single changes such as punctuation but highlights the modifications providing customers with the most valuable information. Therefore it is important to note that this Redline version is not the official ISO standard and that the users must consult with the clean version of the standard, which is the official standard, for implementation purposes.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/0d255761-0bcc-4009-9714-8b113a4a4251/iso-iec-27005-2018

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Structure of this ~~International Standard~~ document 5
5 Background 6
6 Overview of the information security risk management process 7
7 Context establishment 11
7.1 General considerations 11
7.2 Basic criteria 11
7.2.1 Risk management approach 11
7.2.2 Risk evaluation criteria 12
7.2.3 Impact criteria 12
7.2.4 Risk acceptance criteria 12
7.3 Scope and boundaries 13
7.4 Organization for information security risk management 14
8 Information security risk assessment 14
8.1 General description of information security risk assessment 14
8.2 Risk identification 15
8.2.1 Introduction to risk identification 15
8.2.2 Identification of assets 15
8.2.3 Identification of threats 16
8.2.4 Identification of existing controls 16
8.2.5 Identification of vulnerabilities 17
8.2.6 Identification of consequences 18
8.3 Risk analysis 18
8.3.1 Risk analysis methodologies 18
8.3.2 Assessment of consequences 20
8.3.3 Assessment of incident likelihood 21
8.3.4 Level of risk determination 21
8.4 Risk evaluation 22
9 Information security risk treatment 23
9.1 General description of risk treatment 23
9.2 Risk modification 25
9.3 Risk retention 26
9.4 Risk avoidance 26
9.5 Risk sharing 26
10 Information security risk acceptance 27
11 Information security risk communication and consultation 27
12 Information security risk monitoring and review 28
12.1 Monitoring and review of risk factors 28
12.2 Risk management monitoring, review and improvement 29
Annex A (informative) **Defining the scope and boundaries of the information security risk management process** 31
Annex B (informative) **Identification and valuation of assets and impact assessment** 37
Annex C (informative) **Examples of typical threats** 53

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018

Annex D (informative) **Vulnerabilities and methods for vulnerability assessment** **58**
Annex E (informative) **Information security risk assessment approaches** **64**
Annex F (informative) **Constraints for risk modification** **71**
~~**Annex G** (informative) **Differences in definitions between ISO/IEC 27005:2008 and ISO/IEC 27005:2011** ..... **75**~~
Bibliography **84**

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018

 © ISO/IEC 2018 – All rights reserved

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.

~~International Standards are~~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 ~~rules given in~~editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

~~The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.~~

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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018

~~ISO/IEC 27005~~This document was prepared by ~~Joint~~ Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This ~~second~~third edition cancels and replaces the ~~first~~second edition (ISO/IEC 27005:~~2008~~2011) which has been technically revised. The main changes from the previous edition are as follows:

— all direct references to the 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 ISO/IEC 27001 (see Introduction);

— ISO/IEC 27001:2005 has been removed from Clause 2;

— 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.

© ISO/IEC 2018 – All rights reserved

Introduction

This ~~International Standard~~document provides guidelines for information security risk management in an organization~~, supporting in particular the requirements of an information security management (ISMS) according to ISO/IEC 27001~~. However, this ~~International Standard~~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 ~~the ISMS~~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 ~~International Standard~~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 ~~International Standard~~document is relevant to managers and staff concerned with information security risk management within an organization and, where appropriate, external parties supporting such activities.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bcc-4009-9714-bb115a4a4251/iso-iec-27005-2018

 © ISO/IEC 2018 – All rights reserved

Information technology — Security techniques — Information security risk management

1 Scope

This ~~International Standard~~document provides guidelines for information security risk management.

This ~~International Standard~~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 ~~International Standard~~document.

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

2 Normative references

The following ~~referenced~~ documents are ~~indispensable for the application of~~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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
ISO/IEC 27005:2018
https://standards.iteh.ai/catalog/standards/iso/6d253761-0bce-4009-9714-bb115a4a4251/iso-iec-27005-2018

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

~~ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*~~

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.

~~NOTE Differences in definitions between ISO/IEC 27005:2008 and this International Standard are shown in Annex G.~~

~~**3.1**~~
~~**consequence**~~
~~outcome of an *event* (3.3) affecting objectives~~

~~[SOURCE: ISO Guide 73:2009]~~

~~Note 1 to entry: An event can lead to a range of consequences.~~

~~Note 2 to entry: A consequence can be certain or uncertain and in the context of information security is usually negative.~~

~~Note 3 to entry: Consequences can be expressed qualitatively or quantitatively.~~

~~Note 4 to entry: Initial consequences can escalate through knock-on effects.~~

© ISO/IEC 2018 – All rights reserved