

# American National Standard

INCITS/ISO/IEC 27005:2018 (2019)

(ISO/IEC 27005:2018, IDT)

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

**Developed by**



*Where IT all begins*



## INCITS/ISO/IEC 27005:2018 (2019)

### PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 10/24/2019

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2019 by Information Technology Industry Council  
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

Third edition  
2018-07

---

---

## 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*



Reference number  
ISO/IEC 27005:2018(E)

© ISO/IEC 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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

This is a preview of "INCITS/ISO/IEC 27005...". Click here to purchase the full version from the ANSI store.

## Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Structure of this document</b> .....	<b>1</b>
<b>5 Background</b> .....	<b>2</b>
<b>6 Overview of the information security risk management process</b> .....	<b>3</b>
<b>7 Context establishment</b> .....	<b>5</b>
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
<b>8 Information security risk assessment</b> .....	<b>8</b>
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
<b>9 Information security risk treatment</b> .....	<b>16</b>
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
<b>10 Information security risk acceptance</b> .....	<b>20</b>
<b>11 Information security risk communication and consultation</b> .....	<b>20</b>
<b>12 Information security risk monitoring and review</b> .....	<b>21</b>
12.1 Monitoring and review of risk factors.....	21
12.2 Risk management monitoring, review and improvement.....	22
<b>Annex A (informative) Defining the scope and boundaries of the information security risk management process</b> .....	<b>24</b>
<b>Annex B (informative) Identification and valuation of assets and impact assessment</b> .....	<b>28</b>
<b>Annex C (informative) Examples of typical threats</b> .....	<b>37</b>

This is a preview of "INCITS/ISO/IEC 27005...". [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of "INCITS/ISO/IEC 27005...". Click here to purchase the full version from the ANSI store.

## 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](http://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](http://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](http://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*.

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](http://www.iso.org/members.html).

This third edition cancels and replaces the second edition (ISO/IEC 27005:2011) 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.

## 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.



This is a preview of "INCITS/ISO/IEC 27005...". Click here to purchase the full version from the ANSI store.

# 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](#);