

Nederlandse norm

# NEN-ISO/IEC 27005

(en)

Information technology - Security techniques -  
Information security risk management (ISO/IEC  
27005:2018, IDT)

Vervangt NEN-ISO/IEC 27005:2011

ICS 03.100.70; 35.030

juli 2018

Als Nederlandse norm is aanvaard:

- ISO/IEC 27005:2018, DT

Normcommissie 381027 'Informatiebeveiliging, Cyber security en Privacy'



**THIS PUBLICATION IS COPYRIGHT/PROTECTED**

**DEZE PUBLICATIE IS AUTEURSRECHTELIJK BESCHERMD**

Apart from exceptions provided by the law, nothing from this publication may be duplicated and/or published by means of photocopy, microfilm, storage in computer files or otherwise, which also applies to full or partial processing, without the written consent of the Royal Netherlands Standardization Institute.

The Royal Netherlands Standardization Institute shall, with the exclusion of any other beneficiary, collect payments owed by third parties for duplication and/or act in and out of law, where this authority is not transferred or falls by right to the Reproduction Rights Foundation.

Auteursrecht voorbehouden. Behoudens uitzondering door de wet gesteld mag zonder schriftelijke toestemming van het Koninklijk Nederlands Normalisatie-instituut niets uit deze uitgave worden verveelvoudigd en/of openbaar gemaakt door middel van fotokopie, microfilm, opslag in computerbestanden of anderszins, hetgeen ook van toepassing is op gehele of gedeeltelijke bewerking.

Het Koninklijk Nederlands Normalisatie-instituut is met uitsluiting van ieder ander gerechtigd de door derden verschuldigde vergoedingen voor verveelvoudiging te innen en/of daartoe in en buiten rechte op te treden, voor zover deze bevoegdheid niet is overgedragen c.q. rechtens toekomt aan de Stichting Reprorecht.

Although the utmost care has been taken with this publication, errors and omissions cannot be entirely excluded. The Royal Netherlands Standardization Institute and/or the members of the committees therefore accept no liability, not even for direct or indirect damage, occurring due to or in relation with the application of publications issued by the Royal Netherlands Standardization Institute.

Hoewel bij deze uitgave de uiterste zorg is nagestreefd, kunnen fouten en onvolledigheden niet geheel worden uitgesloten. Het Koninklijk Nederlands Normalisatie-instituut en/of de leden van de commissies aanvaarden derhalve geen enkele aansprakelijkheid, ook niet voor directe of indirecte schade, ontstaan door of verband houdend met toepassing van door het Koninklijk Nederlands Normalisatie-instituut gepubliceerde uitgaven.

Copyright  
Preview

---

---

**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*



Copyright  
Preview



**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

# Contents

	Page
Foreword.....	v
Introduction.....	vi
<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>

**ISO/IEC 27005:2018(E)**

<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>

Preview

Forbiede

## 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.

Copyright  
Preview



# 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](#);

**ISO/IEC 27005:2018(E)**

- risk acceptance in [Clause 10](#);
- risk communication in [Clause 11](#);
- risk monitoring and review in [Clause 12](#).

Additional information for information security risk management activities is presented in the annexes. The context establishment is supported by [Annex A](#) (Defining the scope and boundaries of the information security risk management process). Identification and valuation of assets and impact assessments are discussed in [Annex B](#). [Annex C](#) gives examples of typical threats and [Annex D](#) discusses vulnerabilities and methods for vulnerability assessment. Examples of information security risk assessment approaches are presented in [Annex E](#).

Constraints for risk modification are presented in [Annex E](#).

All risk management activities as presented from [Clause 7](#) to [Clause 12](#) are structured as follows:

Input: Identifies any required information to perform the activity.

Action: Describes the activity.

Implementation guidance: Provides guidance on performing the action. Some of this guidance may not be suitable in all cases and so other ways of performing the action may be more appropriate.

Output: Identifies any information derived after performing the activity.

## 5 Background

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system (ISMS). This approach should be suitable for the organization's environment and, in particular, should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to the implementation and the ongoing operation of an ISMS.

Information security risk management should be a continual process. The process should establish the external and internal context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions. Risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce the risk to an acceptable level.

Information security risk management should contribute to the following:

- risks being identified;
- risks being assessed in terms of their consequences to the business and the likelihood of their occurrence;
- the likelihood and consequences of these risks being communicated and understood;
- priority order for risk treatment being established;
- priority for actions to reduce risks occurring;
- stakeholders being involved when risk management decisions are made and kept informed of the risk management status;
- effectiveness of risk treatment monitoring;
- risks and the risk management process being monitored and reviewed regularly;

- information being captured to improve the risk management approach;
- managers and staff being educated about the risks and the actions taken to mitigate them.

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service), any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

## 6 Overview of the information security risk management process

A high level view of the risk management process is specified in ISO 31000 and shown in [Figure 1](#).

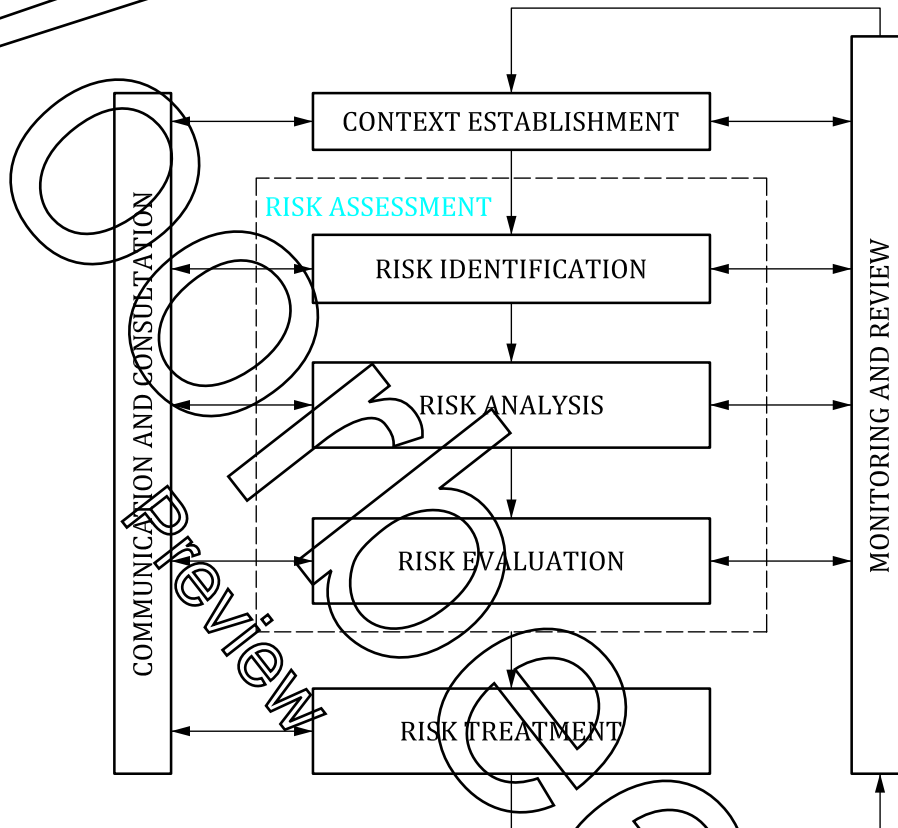
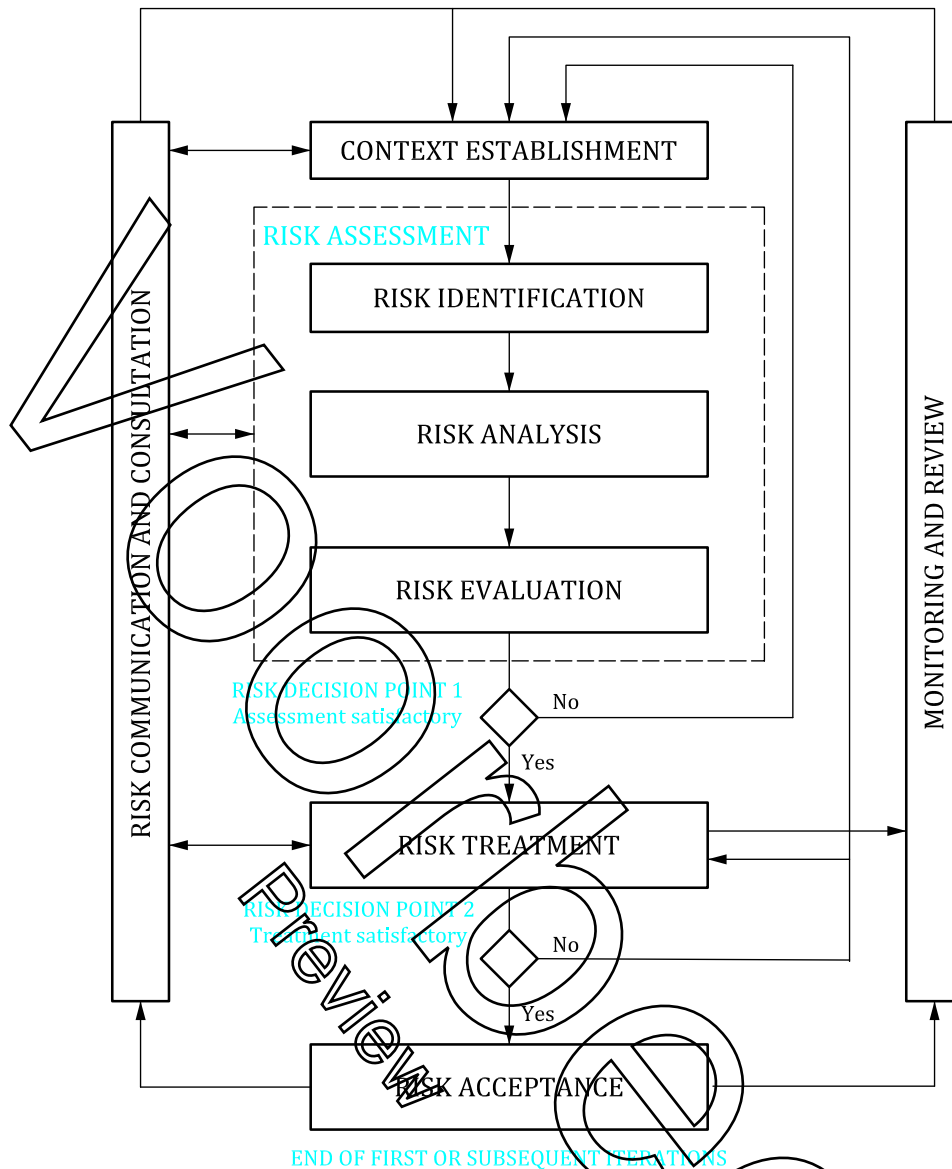


Figure 1 — The risk management process

[Figure 2](#) shows how this document applies this risk management process.

The information security risk management process consists of context establishment ([Clause 7](#)), risk assessment ([Clause 8](#)), risk treatment ([Clause 9](#)), risk acceptance ([Clause 10](#)), risk communication and consultation ([Clause 11](#)), and risk monitoring and review ([Clause 12](#)).



**Figure 2 — Illustration of an information security risk management process**

As [Figure 2](#) illustrates, the information security risk management process can be iterative for risk assessment and/or risk treatment activities. An iterative approach to conducting risk assessment can increase depth and detail of the assessment at each iteration. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that high risks are appropriately assessed.

The context is established first. Then, a risk assessment is conducted. If this provides sufficient information to effectively determine the actions required to modify the risks to an acceptable level, then the task is complete and the risk treatment follows. If the information is insufficient, another iteration of the risk assessment with revised context (e.g. risk evaluation criteria, risk acceptance criteria or impact criteria) is conducted, possibly on limited parts of the total scope (see [Figure 2](#), Risk Decision Point 1).

The effectiveness of the risk treatment depends on the results of the risk assessment.

Note that risk treatment involves a cyclical process of:

- assessing a risk treatment;

# Bestelformulier

## Stuur naar:

NEN Standards Products & Services  
t.a.v. afdeling Klantenservice  
Antwoordnummer 10214  
2600 WB Delft



**NEN** Standards Products & Services

Postbus 5059  
2600 GB Delft

Vlinderweg 6  
2623 AX Delft

T (015) 2 690 390  
F (015) 2 690 271

[www.nen.nl/normshop](http://www.nen.nl/normshop)

## Ja, ik bestel

\_\_ ex. NEN-ISO/IEC 27005:2018 en

€ 163.02

**Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via [www.nen.nl/normshop](http://www.nen.nl/normshop)**

### Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. [www.nen.nl/nieuwsbrieven](http://www.nen.nl/nieuwsbrieven)

## Gegevens

Bedrijf / Instelling

T.a.v.  O M O V

E-mail

Klantnummer NEN

Uw ordernummer  BTW nummer

Postbus / Adres

Postcode  Plaats

Telefoon  Fax

**Factuuradres** (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode  Plaats

Datum  Handtekening

### Retourneren

Fax: 015 2 690 271

E-mail: [klantenservice@nen.nl](mailto:klantenservice@nen.nl)

Post: NEN Standards Products & Services,

t.a.v. afdeling Klantenservice  
Antwoordnummer 10214,  
2600 WB Delft

(geen postzegel nodig).

### Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typfouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: [www.nen.nl/leveringsvoorwaarden](http://www.nen.nl/leveringsvoorwaarden).