



# SLOVENSKI STANDARD SIST ISO/IEC 27004:2011

01-marec-2011

---

**Informacijska tehnologija - Varnostne tehnike - Upravljanje informacijske varnosti -  
Merjenje**

Information technology - Security techniques - Information security management -  
Measurement

## iTeh STANDARD PREVIEW

Technologies de l'information - Techniques de sécurité - Management de la sécurité de  
l'information - Mesurage

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-817dc77a50c5/sist-iso-iec-27004-2011)

Ta slovenski standard je istoveten z: **ISO/IEC 27004:2009**

---

**ICS:**

35.040	Nabori znakov in kodiranje informacij	Character sets and information coding
--------	--	--

**SIST ISO/IEC 27004:2011**

**en**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

INTERNATIONAL  
STANDARD

ISO/IEC  
27004

First edition  
2009-12-15

---

---

**Information technology — Security  
techniques — Information security  
management — Measurement**

*Technologies de l'information — Techniques de sécurité —  
Management de la sécurité de l'information — Mesurage*

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

[https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-  
8f7de77a50c5/sist-iso-iec-27004-2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

---

---

Reference number  
ISO/IEC 27004:2009(E)



## ISO/IEC 27004:2009(E)

**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.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2009

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 and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
Case postale 56 • CH-1211 Geneva 20  
Tel. + 41 22 749 01 11  
Fax + 41 22 749 09 47  
E-mail [copyright@iso.org](mailto:copyright@iso.org)  
Web [www.iso.org](http://www.iso.org)

Published in Switzerland

## Contents

Page

Foreword .....	v
0 Introduction.....	vi
0.1 General .....	vi
0.2 Management overview .....	vi
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions .....	1
4 Structure of this International Standard .....	3
5 Information security measurement overview .....	4
5.1 Objectives of information security measurement.....	4
5.2 Information Security Measurement Programme .....	5
5.3 Success factors .....	6
5.4 Information security measurement model.....	6
5.4.1 Overview.....	6
5.4.2 Base measure and measurement method.....	7
5.4.3 Derived measure and measurement function.....	9
5.4.4 Indicators and analytical model.....	10
5.4.5 Measurement results and decision criteria .....	11
6 Management responsibilities .....	12
6.1 Overview.....	12
6.2 Resource management.....	13
6.3 Measurement training, awareness, and competence.....	13
7 Measures and measurement development.....	13
7.1 Overview.....	13
7.2 Definition of measurement scope.....	13
7.3 Identification of information need .....	14
7.4 Object and attribute selection.....	14
7.5 Measurement construct development.....	15
7.5.1 Overview.....	15
7.5.2 Measure selection .....	15
7.5.3 Measurement method .....	15
7.5.4 Measurement function .....	16
7.5.5 Analytical model .....	16
7.5.6 Indicators .....	16
7.5.7 Decision criteria.....	16
7.5.8 Stakeholders .....	17
7.6 Measurement construct.....	17
7.7 Data collection, analysis and reporting .....	17
7.8 Measurement implementation and documentation .....	18
8 Measurement operation .....	18
8.1 Overview.....	18
8.2 Procedure integration .....	18
8.3 Data collection, storage and verification .....	19
9 Data analysis and measurement results reporting.....	19
9.1 Overview.....	19
9.2 Analyse data and develop measurement results.....	19
9.3 Communicate measurement results .....	20

## ISO/IEC 27004:2009(E)

10	Information Security Measurement Programme Evaluation and Improvement.....	20
10.1	Overview .....	20
10.2	Evaluation criteria identification for the Information Security Measurement Programme .....	21
10.3	Monitor, review, and evaluate the Information Security Measurement Programme .....	21
10.4	Implement improvements .....	21
	Annex A (informative) Template for an information security measurement construct.....	22
	Annex B (informative) Measurement construct examples .....	24
	Bibliography .....	55

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

## 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 drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

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.

ISO/IEC 27004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

**STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

**ISO/IEC 27004:2009(E)****0 Introduction****0.1 General**

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved. It needs to be kept in mind that no measurement of controls can guarantee complete security.

The implementation of this approach constitutes an Information Security Measurement Programme. The Information Security Measurement Programme will assist management in identifying and evaluating non-compliant and ineffective ISMS processes and controls and prioritizing actions associated with improvement or changing these processes and/or controls. It may also assist the organization in demonstrating ISO/IEC 27001 compliance and provide additional evidence for management review and information security risk management processes.

This International Standard assumes that the starting point for the development of measures and measurement is a sound understanding of the information security risks that an organization faces, and that an organization's risk assessment activities have been performed correctly (i.e. based on ISO/IEC 27005), as required by ISO/IEC 27001. The Information Security Measurement Programme will encourage an organization to provide reliable information to relevant stakeholders concerning its information security risks and the status of the implemented ISMS to manage these risks.

Effectively implemented, the Information Security Measurement Programme would improve stakeholder confidence in measurement results, and enable the stakeholders to use these measures to effect continual improvement of information security and the ISMS.

The accumulated measurement results will allow comparison of progress in achieving information security objectives over a period of time as part of an organization's ISMS continual improvement process.

**0.2 Management overview**

ISO/IEC 27001 requires the organization to “undertake regular reviews of the effectiveness of the ISMS taking into account results from effectiveness measurement” and to “measure the effectiveness of controls to verify that security requirements have been met”. ISO/IEC 27001 also requires the organization to “define how to measure the effectiveness of the selected controls or groups of controls and specify how these measures are to be used to assess control effectiveness to produce comparable and reproducible results”.

The approach adopted by an organization to fulfil the measurement requirements specified in ISO/IEC 27001 will vary based on a number of significant factors, including the information security risks that the organization faces, its organizational size, resources available, and applicable legal, regulatory and contractual requirements. Careful selection and justification of the method used to fulfil the measurement requirements are important to ensure that excessive resources are not devoted to these activities of the ISMS to the detriment of others. Ideally, ongoing measurement activities are to be integrated into the regular operations of the organization with minimal additional resource requirements.

This International Standard gives recommendations concerning the following activities as a basis for an organization to fulfil measurement requirements specified in ISO/IEC 27001:

- a) developing measures (i.e. base measures, derived measures and indicators);



- b) implementing and operating an Information Security Measurement Programme;
- c) collecting and analysing data;
- d) developing measurement results;
- e) communicating developed measurement results to the relevant stakeholders;
- f) using measurement results as contributing factors to ISMS-related decisions;
- g) using measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
- h) facilitating continual improvement of the Information Security Measurement Programme.

One of the factors that will impact the organization's ability to achieve measurement is its size. Generally the size and complexity of the business in combination with the importance of information security affect the extent of measurement needed, both in terms of the numbers of measures to be selected and the frequency of collecting and analysing data. For SMEs (Small and Medium Enterprises) a less comprehensive information security measurement program will be sufficient, whereas large enterprises will implement and operate multiple Information Security Measurement Programmes.

A single Information Security Measurement Programme may be sufficient for small organizations, whereas for large enterprises the need may exist for multiple Information Security Measurement Programmes.

The guidance provided by this International Standard will result in the production of documentation that will contribute to demonstrating that control effectiveness is being measured and assessed.

## iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-8f7de77a50c5/sist-iso-iec-27004-2011>

# Information technology — Security techniques — Information security management — Measurement

## 1 Scope

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This International Standard is applicable to all types and sizes of organization.

**NOTE** This document uses the verbal forms for the expression of provisions (e.g. “shall”, “shall not”, “should”, “should not”, “may”, “need not”, “can” and “cannot”) that are specified in the ISO/IEC Directives, Part 2, 2004, Annex H. See also ISO/IEC 27000:2009, Annex A.

## 2 Normative references

The following referenced documents are indispensable for the application 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 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary* [SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-01d0742509/sist-iso-iec-27000-2009)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-01d0742509/sist-iso-iec-27001-2005>  
ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

### 3.1

#### **analytical model**

algorithm or calculation combining one or more base and/or derived measures with associated decision criteria

[ISO/IEC 15939:2007]

### 3.2

#### **attribute**

property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

[ISO/IEC 15939:2007]

### 3.3

#### **base measure**

measure defined in terms of an attribute and the method for quantifying it

[ISO/IEC 15939:2007]

**NOTE** A base measure is functionally independent of other measures.

**ISO/IEC 27004:2009(E)**

- 3.4**  
**data**  
collection of values assigned to base measures, derived measures and/or indicators  
[ISO/IEC 15939:2007]
- 3.5**  
**decision criteria**  
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result  
[ISO/IEC 15939:2007]
- 3.6**  
**derived measure**  
measure that is defined as a function of two or more values of base measures  
[ISO/IEC 15939:2007]
- 3.7**  
**indicator**  
measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs
- 3.8**  
**information need**  
insight necessary to manage objectives, goals, risks and problems  
[ISO/IEC 15939:2007]
- 3.9**  
**measure**  
variable to which a value is assigned as the result of measurement  
[ISO/IEC 15939:2007]
- NOTE The term “measures” is used to refer collectively to base measures, derived measures, and indicators.
- EXAMPLE A comparison of a measured defect rate to planned defect rate along with an assessment of whether or not the difference indicates a problem.
- 3.10**  
**measurement**  
process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria
- 3.11**  
**measurement function**  
algorithm or calculation performed to combine two or more base measures  
[ISO/IEC 15939:2007]
- 3.12**  
**measurement method**  
logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale  
[ISO/IEC 15939:2007]

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

[SIST ISO/IEC 27004:2011](https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-87d57e59f5e5/iso-iec-27004-2011)

<https://standards.iteh.ai/catalog/standards/sist/9047f365-0532-4a98-b683-87d57e59f5e5/iso-iec-27004-2011>

NOTE The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

- subjective: quantification involving human judgment;
- objective: quantification based on numerical rules.

### 3.13

#### measurement results

one or more indicators and their associated interpretations that address an information need

### 3.14

#### object

item characterized through the measurement of its attributes

### 3.15

#### scale

ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped

[ISO/IEC 15939:2007]

NOTE The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined:

- nominal: the measurement values are categorical;
- ordinal: the measurement values are rankings;
- interval: the measurement values have equal distances corresponding to equal quantities of the attribute;
- ratio: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

### 3.16

#### unit of measurement

particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity

[ISO/IEC 15939:2007]

### 3.17

#### validation

confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

### 3.18

#### verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005]

NOTE This could also be called compliance testing.

## 4 Structure of this International Standard

This International Standard provides an explanation of measures and measurement activities needed to assess the effectiveness of ISMS requirements for the management of adequate and proportionate security controls as required in ISO/IEC 27001:2005, 4.2.

**ISO/IEC 27004:2009(E)**

This International Standard is structured as follows:

- Overview on the Information Security Measurement Programme and the Information Security Measurement Model (Clause 5);
- Management responsibilities for information security measurements (Clause 6); and
- Measurement constructs and the processes (i.e. planning and developing, implementing and operating, and improving measurements: communicating measurement results) to be implemented in the Information Security Measurement Programme (Clauses 7-10).

In addition, Annex A provides an example template for the measurement construct of which the constituents are the elements of the Information Security Measurement Model (see Clause 7). Annex B provides the measurement construct examples for specific controls or processes of an ISMS, using the template provided in Annex A.

These examples are intended to help an organization on how to implement the Information Security Measurement and how to record measurement activities and outcomes from them.

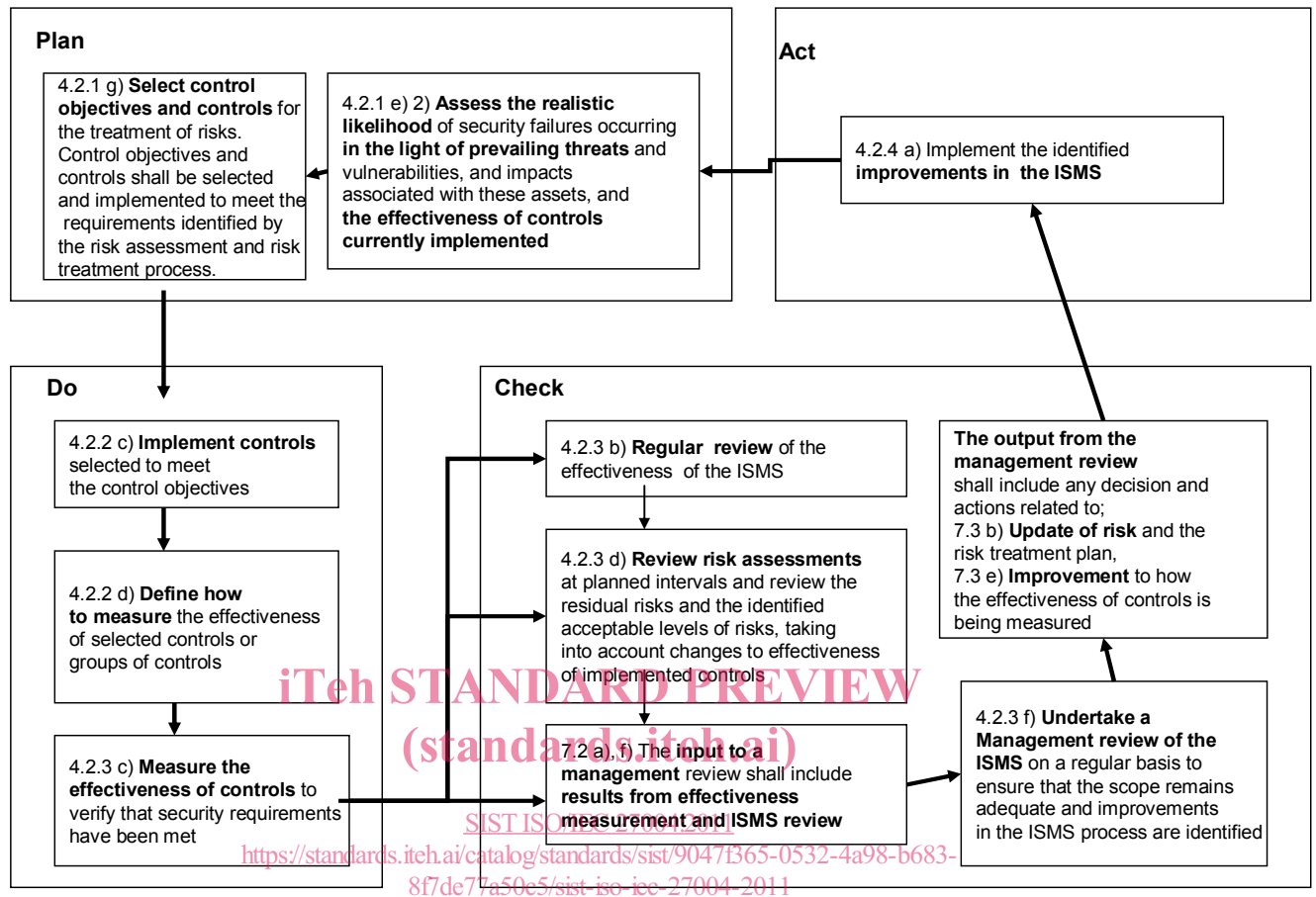
## **5 Information security measurement overview**

### **5.1 Objectives of information security measurement**

The objectives of information security measurement in the context of an ISMS includes:

- a) evaluating the effectiveness of the implemented controls or groups of controls (See “4.2.2 d)” in Figure 1);
- b) evaluating the effectiveness of the implemented ISMS (See “4.2.3 b)” in Figure 1);
- c) verifying the extent to which identified security requirements have been met (See “4.2.3 c)” in Figure 1);
- d) facilitating performance improvement of information security in terms of the organization’s overall business risks;
- e) providing input for management review to facilitate SMS-related decision making and justify needed improvements of the implemented ISMS.

Figure 1 illustrates the cyclical input–output relationship of the measurement activities in relation to the Plan-Do-Check-Act (PDCA) cycle, specified in ISO/IEC 27001. Numbers in each figure represent relevant sub-clauses of ISO/IEC 27001:2005.



**Figure 1 — Measurement inputs and outputs in ISMS PDCA cycle of information security management**

The organization should establish measurement objectives based on a number of considerations, including:

- The role of information security in support of the organization's overall business activities and the risks it faces;
- Applicable legal, regulatory, and contractual requirements;
- Organizational structure;
- Costs and benefits of implementing information security measures;
- Risk acceptance criteria for the organization; and
- A need to compare several ISMSs within the same organization.

## 5.2 Information Security Measurement Programme

An organization should establish and manage an Information Security Measurement Programme in order to achieve the established measurement objectives and adopt the PDCA model within the organization's overall measurement activities. An organization should also develop and implement measurement constructs in order to obtain repeatable, objective and useful results of measurement based on the Information Security Measurement Model (see 5.4).

The Information Security Measurement Programme and the developed measurement construct should ensure that an organization effectively achieves objective and repeatable measurement and provides measurement results for relevant stakeholders to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.