INTERNATIONAL STANDARD

**ISO/IEC 27004**

Second edition
2016-12-15

# Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

*Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation*

Reference number
ISO/IEC 27004:2016(E)

© ISO/IEC 2016



## COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, 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

# Contents

Page

**Foreword** ... **iv**
**Introduction** ... **v**
**1 Scope** ... **1**
**2 Normative references** ... **1**
**3 Terms and definitions** ... **1**
**4 Structure and overview** ... **1**
**5 Rationale** ... **2**
5.1 The need for measurement ... 2
5.2 Fulfilling the ISO/IEC 27001 requirements ... 3
5.3 Validity of results ... 3
5.4 Benefits ... 3
**6 Characteristics** ... **4**
6.1 General ... 4
6.2 What to monitor ... 4
6.3 What to measure ... 5
6.4 When to monitor, measure, analyse and evaluate ... 6
6.5 Who will monitor, measure, analyse and evaluate ... 6
**7 Types of measures** ... **7**
7.1 General ... 7
7.2 Performance measures ... 7
7.3 Effectiveness measures ... 8
**8 Processes** ... **9**
8.1 General ... 9
8.2 Identify information needs ... 10
8.3 Create and maintain measures ... 11
8.3.1 General ... 11
8.3.2 Identify current security practices that can support information needs ... 11
8.3.3 Develop or update measures ... 12
8.3.4 Document measures and prioritize for implementation ... 13
8.3.5 Keep management informed and engaged ... 13
8.4 Establish procedures ... 14
8.5 Monitor and measure ... 14
8.6 Analyse results ... 15
8.7 Evaluate information security performance and ISMS effectiveness ... 15
8.8 Review and improve monitoring, measurement, analysis and evaluation processes ... 15
8.9 Retain and communicate documented information ... 15
**Annex A** (informative) **An information security measurement model** ... **17**
**Annex B** (informative) **Measurement construct examples** ... **19**
**Annex C** (informative) **An example of free-text form measurement construction** ... **57**
**Bibliography** ... **58**

© ISO/IEC 2016 – 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.

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 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.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition of ISO/IEC 27004 cancels and replaces the first edition (ISO/IEC 27004:2009), which has been technically revised.

This edition includes the following significant changes with respect to the previous edition:

A total restructuring of the document because it has a new purpose – to provide guidance on ISO/IEC 27001:2013, 9.1 – which, at the time of the previous edition, did not exist.

The concepts and processes have been modified and expanded. However, the theoretical foundation (ISO/IEC 15939) remains the same and several of the examples given in the previous edition are preserved, albeit updated.


© ISO/IEC 2016 – All rights reserved

# Introduction

This document is intended to assist organizations to evaluate the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1: monitoring, measurement, analysis and evaluation.

The results of monitoring and measurement of an information security management system (ISMS) can be supportive of decisions relating to ISMS governance, management, operational effectiveness and continual improvement.

As with other ISO/IEC 27000 documents, this document should be considered, interpreted and adapted to suit each organization's specific situation. The concepts and approaches are intended to be broadly applicable but the particular measures that any particular organization requires depend on contextual factors (such as its size, sector, maturity, information security risks, compliance obligations and management style) that vary widely in practice.

This document is recommended for organizations implementing an ISMS that meets the requirements of ISO/IEC 27001. However, it does not establish any new requirements for ISMS which conform to ISO/IEC 27001 or impose any obligations upon organizations to observe the guidelines presented.

© ISO/IEC 2016 – All rights reserved

# Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation

## 1 Scope

This document provides guidelines intended to assist organizations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013, 9.1. It establishes:

a) the monitoring and measurement of information security performance;

b) the monitoring and measurement of the effectiveness of an information security management system (ISMS) including its processes and controls;

c) the analysis and evaluation of the results of monitoring and measurement.

This document is applicable to all types and sizes of organizations.

## 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.

There are no normative references in this document.

## 3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

## 4 Structure and overview

This document is structured as follows:

a) Rationale (Clause 5);

b) Characteristics (Clause 6);

c) Types of measures (Clause 7);

d) Processes (Clause 8).

The ordering of these clauses is intended to aid understanding and map to ISO/IEC 27001:2013, 9.1 requirements, as is illustrated in Figure 1.

Starting with the information needed to fulfil that requirement, referred to as information needs, the organization determines the measures that it will use to fulfil those information needs. The process

© ISO/IEC 2016 – All rights reserved