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

Reference number
ISO/IEC 27004:2009(E)

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
Web 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

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

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*.

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.

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*

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.