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

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.

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]

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.

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 ISMS-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.

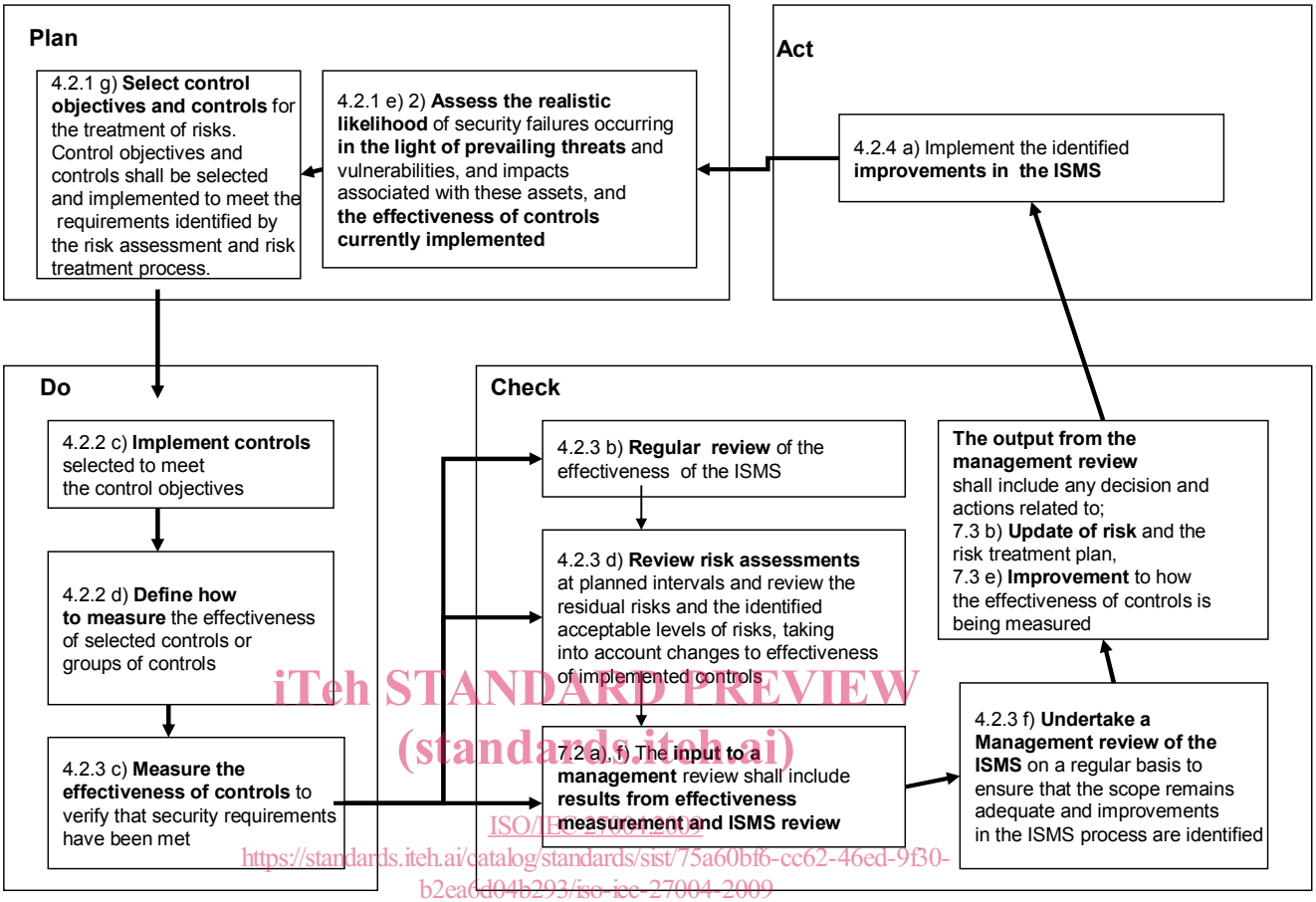

Figure 1 — Measurement inputs and outputs in ISMS PDCA cycle of information security management

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

a) The role of information security in support of the organization's overall business activities and the risks it faces;
b) Applicable legal, regulatory, and contractual requirements;
c) Organizational structure;
d) Costs and benefits of implementing information security measures;
e) Risk acceptance criteria for the organization; and
f) 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.

An Information Security Measurement Programme should include the following processes:

a) Measures and measurement development (see Clause 7) ;
b) Measurement operation (see Clause 8);
c) Data analysis and measurement results reporting (see Clause 9); and
d) Information Security Measurement Programme evaluation and improvement (see Clause 10).

The organisational and operational structure of an Information Security Measurement Programme should be determined by taking into account the scale and complexity of the ISMS of which it is a part. In all cases, roles and responsibilities for the Information Security Measurement Programme should be explicitly assigned to competent personnel (see 7.5.8).

The measures selected and implemented by the Information Security Measurement Programme should be directly related to the operation of an ISMS, other measures, as well as organization's business processes. Measurement can be integrated into regular operational activities or performed at regular intervals determined by ISMS management.

5.3 Success factors

The following are some contributing factors to the success of Information Security Measurement Programme in facilitating continual ISMS improvement:

a) Management commitment supported by appropriate resources;
b) Existence of ISMS processes and procedures;
c) A repeatable process capable of capturing and reporting meaningful data to provide relevant trends over a period of time;
d) Quantifiable measures based on ISMS objectives;
e) Easily obtainable data that can be used for measurement;
f) Evaluation of effectiveness of Information Security Measurement Programme and implementation of identified improvements;
g) Consistent periodic collection, analysis, and reporting of measurement data in a manner that is meaningful;
h) Use of the measurement results by relevant stakeholders to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures;
i) Acceptance of feedback on measurement results from relevant stakeholders; and
j) Evaluations of the usefulness of measurement results and implementation of identified improvements.

Once successfully implemented, an Information Security Measurement Programme can:

1) Demonstrate an organization's compliance with applicable legal or regulatory requirements and contractual obligations;
2) Support identification of previously undetected or unknown information security issues;
3) Assist in satisfying management reporting needs when stating measures for historical and current activities; and
4) Be used as input into information security risk management process, internal ISMS audits and management reviews.

5.4 Information security measurement model

NOTE. The concepts of the information security measurement model and measurement constructs adopted in this International Standard are based on those in ISO/IEC 15939. The term "information product" used in ISO/IEC 15939 is a synonym with "measurement results" in this International Standard and "measurement process" used in ISO/IEC 15939 is a synonym with "Measurement Programme" in this International Standard.

5.4.1 Overview

The information security measurement model is a structure linking an information need to the relevant objects of measurement and their attributes. Objects of measurement may include planned or implemented processes, procedures, projects and resources.

The information security measurement model describes how the relevant attributes are quantified and converted to indicators that provide a basis for decision making. Figure 2 depicts the information security measurement model.

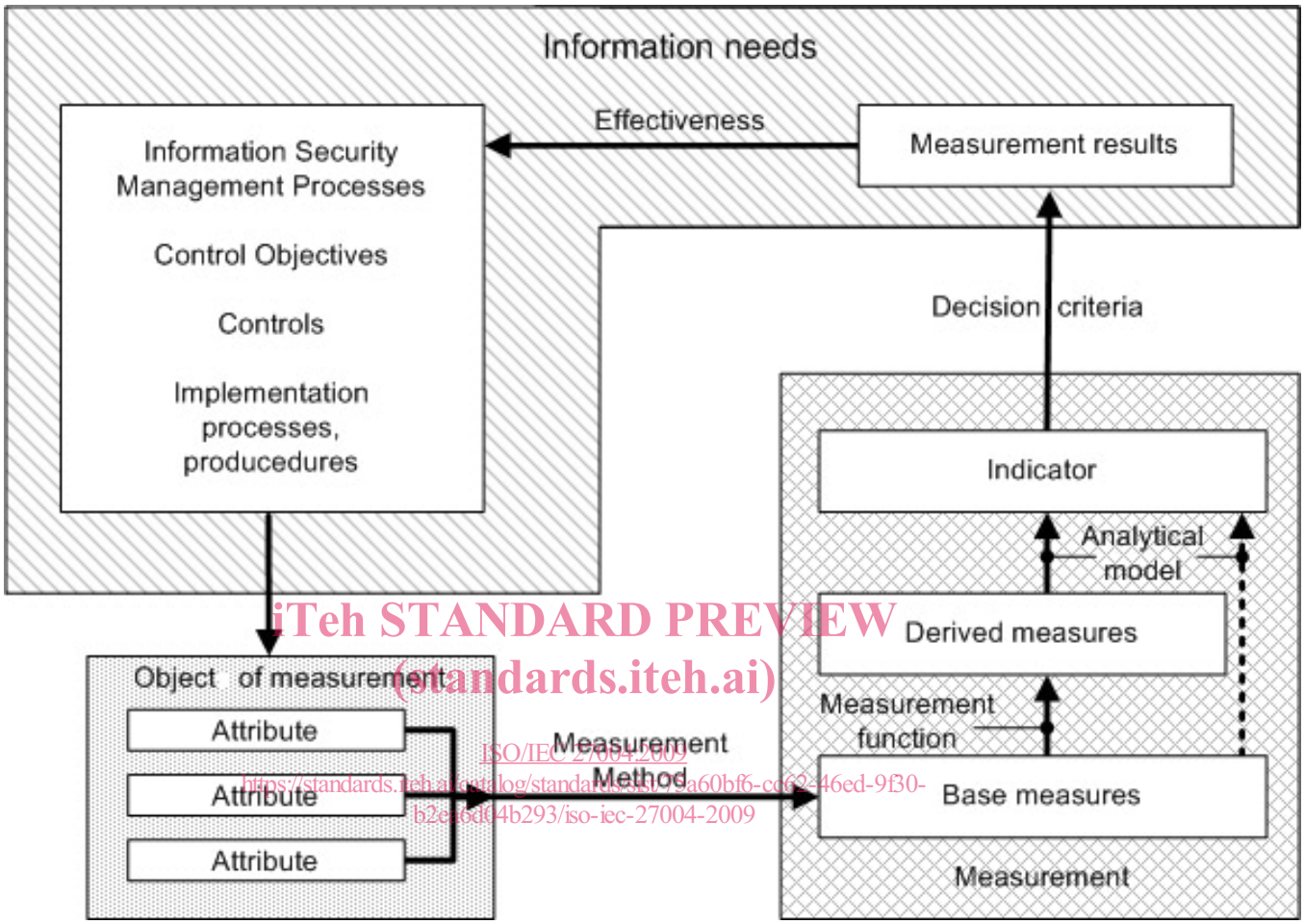

Figure 2 — Information security measurement model

NOTE Clause 7 provides detailed information about the individual elements of information security measurement model.

Subsequent sub-clauses introduce individual elements of the model. They also provide examples of how these individual elements are used.

The information needs or purpose of measurement used in examples contain in Tables 1 to 4 of the following sub-clauses is to assess the awareness status of compliance with organization security policy among relevant personnel (Control objective.A.8.2, and Controls A.8.2.1 and A.8.2.2. of ISO/IEC 27001:2005).

5.4.2 Base measure and measurement method

A base measure is the simplest measure that can be obtained. A base measure results from applying a measurement method to the attributes selected of an object of measurement. An object of measurement may have many attributes, only some of which may provide useful values to be assigned to a base measure. A given attribute may be used for several different base measures.