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)

COPYRIGHT PROTECTED DOCUMENT

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

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.

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.

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

of monitoring and measurement produces data which is then analysed. The results of analysis are evaluated in fulfilment of the organization's information needs.

In addition, Annex A describes a measurement model for information security, including the relationship between the components of the measurement model and the requirements of ISO/IEC 27001:2013, 9.1.

Annex B provides a wide range of examples. These examples are intended to provide practical guidance on how organizations can monitor, measure, analyse and evaluate their chosen ISMS processes and areas of information security performance. These examples use the suggested template given in Table 1. Annex C provides a further example using an alternative free-form text-based format.

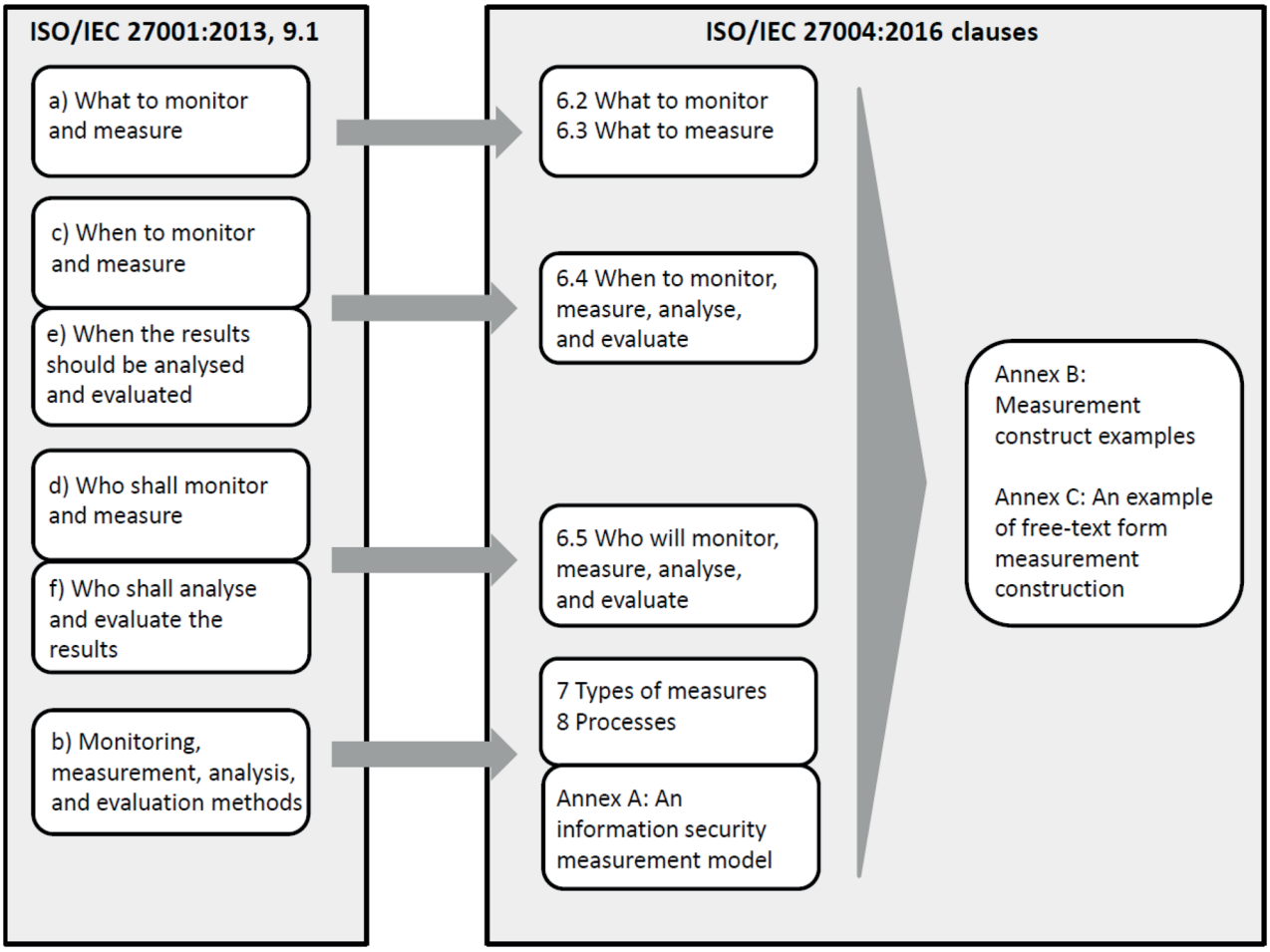

Figure 1 — Mapping to ISO/IEC 27001:2013, 9.1 requirements

5 Rationale

5.1 The need for measurement

The overall objective of an ISMS is the preservation of confidentiality, integrity and availability of information within its scope. There are ISMS activities that concern the planning of how to do this, and the implementation of those plans. However, by themselves, these activities cannot guarantee that the realisation of those plans fulfil the information security objectives. Therefore, in the ISMS as defined by ISO/IEC 27001, there are several requirements to evaluate if the plans and activities ensure the fulfilment of the information security objectives.

5.2 Fulfilling the ISO/IEC 27001 requirements

ISO/IEC 27001:2013, 9.1 requires the organization to evaluate the information security performance and the effectiveness of the ISMS. Measure types able to fulfil these requirements can be found in Clause 7.

ISO/IEC 27001:2013, 9.1 further requires the organization to determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated; and

f) who shall analyse and evaluate these results.

The mapping of these requirements is provided in Figure 1.

Finally, ISO/IEC 27001:2013, 9.1 requires the organization to retain appropriate documented information as evidence of the monitoring and measurement results (See 8.9).

ISO/IEC 27001:2013, 9.1 also notes that methods selected should produce comparable and reproducible results in order for them to be considered valid (See 6.4).

5.3 Validity of results

ISO/IEC 27001:2013, 9.1 b) requires that organizations choose methods for measurement, monitoring, analysis and evaluation to ensure valid results. The clause notes that to be valid, results should be comparable and reproducible. To achieve this, organizations should collect, analyse, and report measures, taking the following points into consideration:

a) in order to get comparable results on measures that are based on monitoring at different points in times, it is important to ensure that scope and context of the ISMS are not changed;

b) changes in the methods or techniques used for measuring and monitoring do not generally lead to comparable results. In order to retain comparability, specific tests such as parallel application of the original as well as the changed methods can be required;

c) if subjective elements are part of the methods or techniques used for measuring and monitoring, specific steps can be needed to obtain reproducible results. As an example, questionnaire results should be evaluated against defined criteria; and

d) in some situations, reproducibility can only be given in specific circumstances. For example, there are situations where results are non-reproducible, but are valid when aggregated.

5.4 Benefits

Fulfilling ISMS processes and controls and ensuring information security performance can provide a number of organizational and financial benefits. Major benefits can include:

a) **Increased accountability:** Monitoring, measurement, analysis and evaluation can increase accountability for information security by helping to identify specific information security processes or controls that are implemented incorrectly, are not implemented, or are ineffective.

b) **Improved information security performance and ISMS processes:** Monitoring, measurement, analysis and evaluation can enable organizations to quantify improvements in securing information

within the scope of their ISMS and demonstrate quantifiable progress in accomplishing the organization's information security objectives.

c) **Evidence of meeting requirements:** Monitoring, measurement, analysis and evaluation can provide documented evidence that helps demonstrate fulfilling of ISO/IEC 27001 (and other standards) requirements, as well as applicable laws, rules, and regulations.

d) **Support decision-making:** Monitoring, measurement, analysis and evaluation can support risk-informed decision-making by contributing quantifiable information to the risk management process. It can allow organizations to measure successes and failures of past and current information security investments, and should provide quantifiable data that can support resource allocation for future investments.

6 Characteristics

6.1 General

Monitoring and measurement is the first step in a process to evaluate information security performance and ISMS effectiveness.

Faced with a potentially overwhelming variety of attributes of information security-related entities that can be measured, it is not entirely obvious which ones should be measured. This is an important issue because it is impracticable, costly and counterproductive to measure too many or the wrong attributes. Aside from the obvious costs of measuring, analysing and reporting numerous attributes, there is a distinct possibility that key issues can be obscured within a large volume of information or missed altogether if suitable measures are not in place.

In order to determine what to monitor and measure, the organization should first consider what it wishes to achieve in evaluating information security performance and ISMS effectiveness. This can allow it to determine its information needs.

Organizations should next decide what measures are needed to support each discrete information need and what data are required to derive the requisite measures. Hence, measurement should always correspond to the information needs of the organization.

6.2 What to monitor

Monitoring determines the status of a system, a process or an activity in order to meet a specified information need.

Systems, processes and activities which can be monitored include, but are not limited to:

a) implementation of ISMS processes;

b) incident management;

c) vulnerability management;

d) configuration management;

e) security awareness and training;

f) access control, firewall and other event logging;

g) audit;

h) risk assessment process;

i) risk treatment process;

j) third party risk management;

k) business continuity management;

l) physical and environmental security management; and

m) system monitoring.

These monitoring activities produce data (event logs, user interviews, training statistics, incident information, etc.) that can be used to support other measures. In the process of defining attributes to be measured, additional monitoring can be required to provide supporting information.

Note that monitoring can allow an organization to determine whether a risk has materialized, and thereby indicate what action it can take to treat such a risk itself. Note also that there can be certain types of information security controls that have the explicit purpose of monitoring. When using outputs of such controls to support measurement, organizations should ensure that the measurement process takes into account whether the data used was obtained before or after any treatment action was taken.

6.3 What to measure

Measurement is an activity undertaken to determine a value, status or trend in performance or effectiveness to help identify potential improvement needs. Measurement can be applied to any ISMS processes, activities, controls and groups of controls.

As an example, consider ISO/IEC 27001:2013, 7.2 c), which requires an organization to take action, where applicable, to acquire necessary competence. An organization can determine whether all individuals who require training have received it and whether the training was delivered as planned. This can be measured by the number or percentage of people trained. An organization can also determine whether the individuals who have been trained actually acquired and retained the necessary competence (which can be measured with a post-training questionnaire).

With regards to ISMS processes, organizations should note that there are a number of clauses in ISO/IEC 27001 that explicitly require the effectiveness of some activity to be determined. For example, ISO/IEC 27001:2013, 10.1 d) requires organizations to "*review the effectiveness of any corrective action taken*". In order to perform such a review, the effectiveness of corrective actions should first be determined in terms of some defined form of measure. In order to do this the organization should first define an appropriate information need and a measure, or measures, to satisfy it. The process for doing this is explained in Clause 8.

ISMS processes and activities that are candidates for measurement include:

a) planning;

b) leadership;

c) risk management;

d) policy management;

e) resource management;

f) communicating;

g) management review;

h) documenting; and

i) auditing.

With regards to information security performance, the most obvious candidates are the organization's information security controls or groups of such controls (or even the entire risk treatment plan). These controls are determined through the process of risk treatment and are referred to in ISO/IEC 27001 as necessary controls. They can be ISO/IEC 27001:2013, Annex A controls, sector-specific controls (e.g. as defined in standards such as ISO/IEC 27010), controls specified by other standards and controls that