BS ISO/IEC 27004:2016

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27004:2016

National foreword

This British Standard is the UK implementation of ISO/IEC 27004:2016. It supersedes BS ISO/IEC 27004:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/1, Information Security Management.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 83513 1

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 December 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27004:2016

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)

Documents
Document Sharing Hub
© ISO/IEC 2016

Full document details: BS ISO/IEC 27004:2016

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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27004:2016

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

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
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

Documents
Document Sharing Hub

INTERNATIONAL STANDARD ISO/IEC 27004:2016(E)

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

AVA Documents Document Sharing Hub

Full document details: BS ISO/IEC 27004:2016

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.

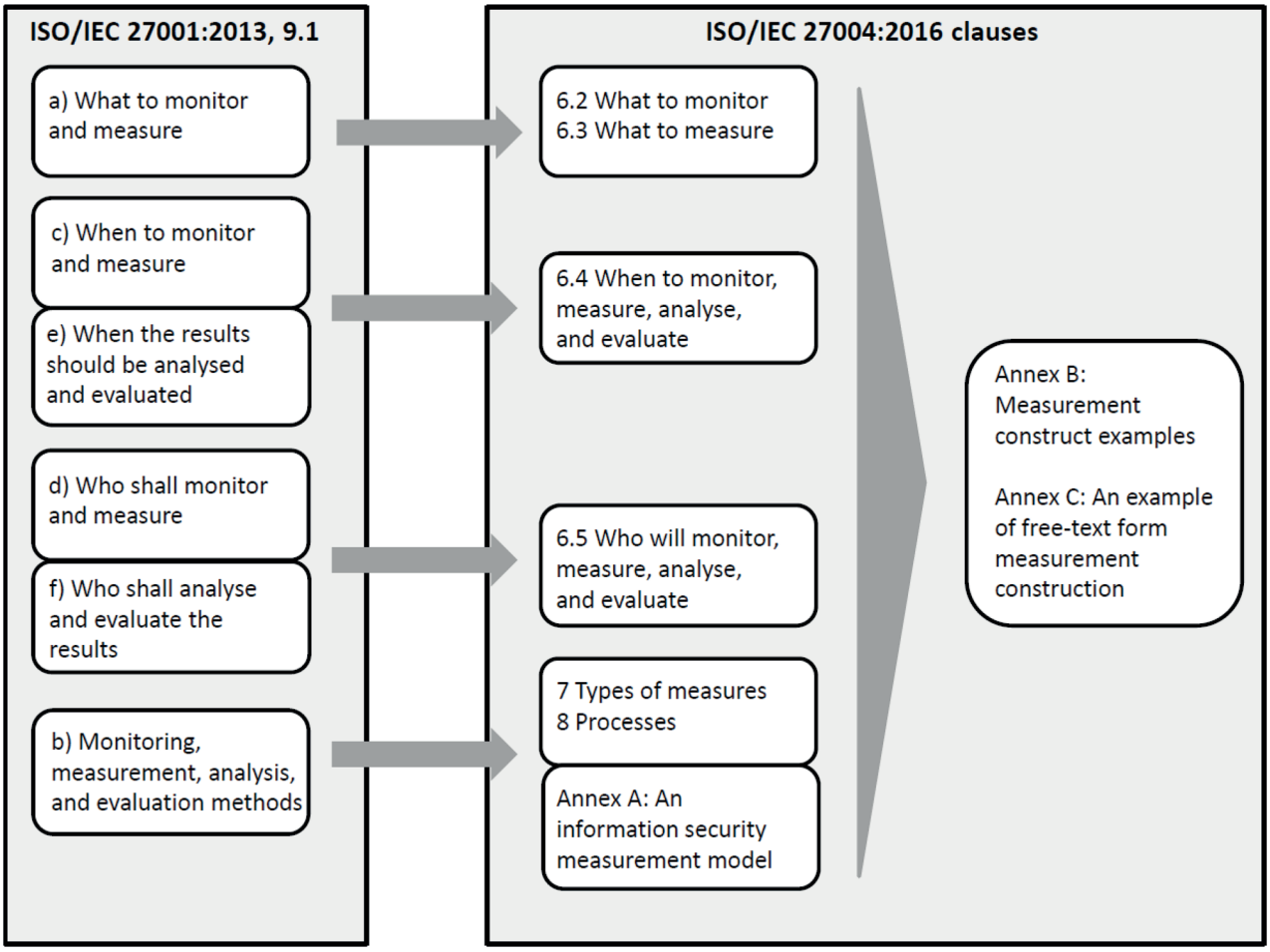

Figure 1 — Mapping to ISO/IEC 27001:2013, 9.1 requirements

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.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

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;

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

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

© ISO/IEC 2016 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

have been designed by the organization. As the purpose of a control is to modify risk, there are a variety of attributes that can be measured, such as:

j) the degree to which a control reduces the likelihood of the occurrence of an event;

k) the degree to which a control reduces the consequence of an event;

l) the frequency of events that a control can cope with before failure; and

m) how long after the occurrence of an event does it take for the control to detect that the event has occurred.

6.4 When to monitor, measure, analyse and evaluate

Organizations should define specific timeframes in which to monitor, measure, analyse, and evaluate, based on individual information needs, required measures, and the lifecycle of data supporting individual measures. The data supporting measures can be collected more frequently than the analysis and reporting of such measures to individual interested parties. For example, while data on security incidents can be collected continually, reporting of such data to external interested parties should be based on specific requirements, such as severity (possibly requiring immediate notification as in the case of a reportable breach) or aggregated values (as might be the case for attempted intrusions which were detected and blocked).

Organizations should note that in order to satisfy certain information needs, before analysis and evaluation can proceed, an appropriate volume of data needs to be collected in order to provide a meaningful basis for assessment and comparison (e.g. when conducting statistical analysis). In addition, the processes of monitoring, measurement, analysis, and evaluation can need testing and fine-tuning before the resulting measures can be useful to the organization. Organizations should therefore determine a limit to the duration of any fine-tuning (so as to proceed with the real objective, measurement of the ISMS) and for how long monitoring and collection should continue before analysis and evaluation can commence.

Organizations can adjust their measurement timeframes, as they update their measurement activities, to address specific environmental changes listed in 8.2. For example, if an organization is transitioning from a manual data source to an automated source, a change in frequency of collection can be required. Furthermore, a baseline is needed to compare two sets of measures taken at different points in time and potentially by different methods but aiming to fulfil the same information need.

An organization can choose to structure their monitoring, measurement, analysis, and evaluation activities into a measurement programme. It is important to note, however, that ISO/IEC 27001 has no requirement for organizations to have such a programme.

6.5 Who will monitor, measure, analyse and evaluate

Organizations (considering requirements of ISO/IEC 27001:2013, 9.1 and 5.3) should specify who monitors, measures, analyses and evaluates in terms of individuals or roles. Monitoring, measurement, analysis, and evaluation can be performed using either manual or automated means. Whether the measurement is performed manually or automatically, organizations can define the following measurement-related roles and responsibilities:

a) measurement client: the management or other interested parties requesting or requiring information about the effectiveness of an ISMS, controls or group of controls;

b) measurement planner: the person or organizational unit that defines the measurement constructs that links measurable attributes to a specified information need;

c) measurement reviewer: the person or organizational unit that validates that the developed measurement constructs are appropriate for evaluating information security performance and the effectiveness of an ISMS, controls or group of controls;

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

d) information owner: the person or organizational unit that owns the information that provides input into measures. This person is responsible for providing the data and is also frequently (but not always) responsible for conducting measurement activities;

e) information collector: the person or organizational unit responsible for collecting, recording and storing the data;

f) information analyst: the person or organizational unit responsible for analysing data; and

g) information communicator: the person or organizational unit responsible for communicating the results of analysis.

Organizations can combine some, or possibly all, of these roles.

Individuals performing different roles and responsibilities throughout the processes can require diverse skill sets and associated awareness and training.

7 Types of measures

7.1 General

For the purposes of this guidance, the performance of planned activities and the effectiveness of the results can be measured by applying the two following types of measures:

a) performance measures: measures that express the planned results in terms of the characteristics of the planned activity, such as head counts, milestone accomplishment, or the degree to which information security controls have been implemented;

b) effectiveness measures: measures that express the effect that realization of the planned activities has on the organization's information security objectives.

These measures can be inherently organization-specific since each organization has its own particular information security objectives, policies and requirements.

Note that the terms "performance measures" and "effectiveness measures" should not be confused with the ISO/IEC 27001:2013, 9.1 requirement to evaluate information security performance and ISMS effectiveness.

7.2 Performance measures

Performance measures can be used to demonstrate progress in implementing ISMS processes, associated procedures and specific security controls. Whereas effectiveness concerns the extent to which planned activities have been realised and intended results achieved, performance measures should concern the extent to which information security processes and controls have been implemented. These measures help determine whether the ISMS processes and information security controls have been implemented as specified.

Performance measures use data that can be obtained from minutes, attendance records, project plans, automated scanning tools and other commonly-used means of documenting, recording, and monitoring ISMS activities.

The collection, analysis, and reporting of measures should be automated wherever possible, in order to reduce the cost and effort required and the potential for human error.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

Example 1

When measuring the degree of implementation of specific information security controls, such as the percentage of laptops with hard disk encryption, the results of this measure will likely be, at first, less than 100%. When the result reaches and remains at 100%, it can be concluded that the information systems have fully implemented the security controls addressed by this measure, and measurement activities can refocus on other controls in need of improvement.

Example 2

For a new ISMS, the organization should first seek to ensure that top management attends the review and other meetings that can be called. The planned (or intended) result in this case is full attendance at all meetings, barring sickness and permitted prior commitments. The measure is simply how many attend versus how many ought to attend, with a possible modifier that absence was for good reason. At first, the results of these measures might indicate a shortfall. However, with time, results should reach and remain close to their planned targets. At this point, the organization should begin to focus its measurement efforts on effectiveness measures (see 7.3).

After most performance measures reach and remain at 100%, the organization should begin to focus its measurement efforts on effectiveness measures. Organizations should never fully retire performance measures because they can be helpful in pointing out specific security controls that are in need of improvement; however, over time, the emphasis and resources being applied to measurement should shift away from these measures and towards effectiveness measures (see 7.3).

According to ISO/IEC 27001:2013, 9.1, it is likewise important to also measure the effectiveness of the management system (discussed next). To operate a suitable ISMS, organizations should measure performance and effectiveness at planned intervals.

7.3 Effectiveness measures

Effectiveness measures should be used to describe the effectiveness and impact that the realisations of the ISMS risk treatment plan and ISMS processes and controls have on the organization's information security objectives. These measures should be used to determine whether ISMS processes and information security controls are operating as intended and achieving their desired outcomes. Depending upon those objectives, effectiveness measures can be used to quantify, e.g.:

a) cost savings produced by the ISMS or through costs incurred from addressing information security incidents;

b) the degree of customer trust gained/maintained by the ISMS; and

c) the achievement of other information security objectives.

Effectiveness measures can be created by combining data obtained from automated monitoring and evaluation tools with manually-derived data about ISMS activity. This can require tracking a variety of measures across the organization in a manner that can be directly tied to the ISMS activities and information security events. To achieve this, an organization should have an established capability to:

d) evaluate the degree to which ISMS processes, controls, or groups of controls have been implemented through performance measures;

e) collect data from automated monitoring and evaluation tools;

f) manually collect data from ISMS activities;

g) normalize and analyse data originating from multiple automated and manual sources; and

h) interpret and report this data to decision makers.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

These effectiveness measures combine information about the realisation of the risk treatment plan with a variety of information about resources and can provide inputs to the risk management process. They can also provide the most direct insight into the value of information security to the organization and can be the ones that ought to be of most interest to top management.

Example 3

Exploitations of known vulnerabilities are known to cause a large portion of information security incidents. The greater the number of known vulnerabilities and the longer that they are not addressed (e.g. patched), the greater the probability of their exploitation by associated threats and the greater the related risk exposure. An effectiveness measure can help an organization determine its risk exposure caused by such vulnerabilities.

Example 4

A training course can have specific training objectives for each course module. An effectiveness measure can help the organization to determine the extent to which each trainee has understood each lesson and is able to apply their new knowledge and skills. These measures usually require multiple data points, such as: results of post-training tests; examination of incident data correlated with training topics; or analysis of help desk calls correlated with training topics.

8 Processes

8.1 General

Monitoring, measurement, analysis and evaluation (see Figure 2) consists of the following processes:

a) identify information needs;

b) create and maintain measures;

c) establish procedures;

d) monitor and measure;

e) analyse results; and

f) evaluate information security performance and ISMS effectiveness.

In addition, there is an ISMS management process that covers the review and improvement of the above processes, see 8.8.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

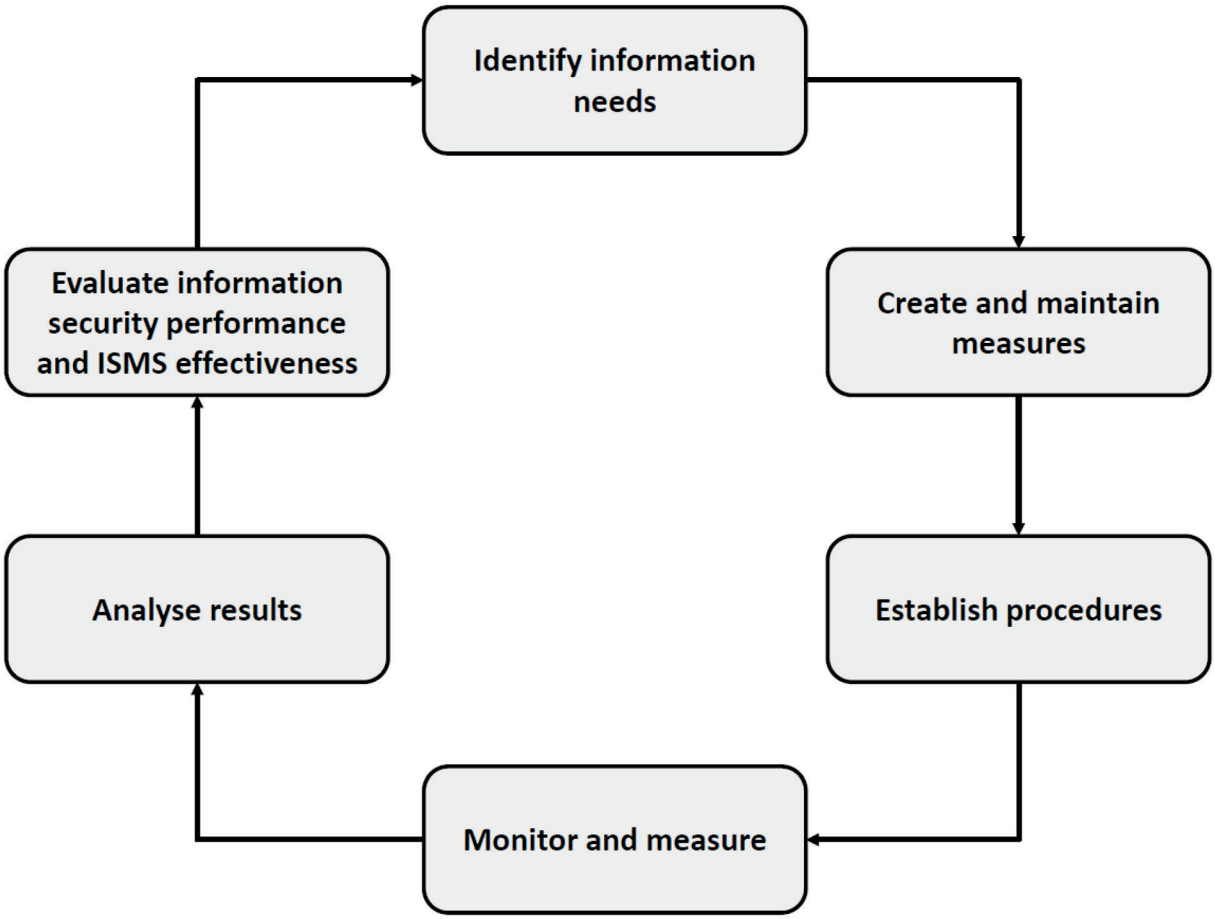

Figure 2 — Monitoring, measurement, analysis and evaluation processes

8.2 Identify information needs

The creation of measures should begin with identification of information needs, which can assist in the understanding of the operational characteristics and/or performance of any aspect of the ISMS, such as any of the following:

a) interested party needs;

b) the strategic direction of the organization;

c) information security policy and objectives; and

d) the risk treatment plan.

The following activities should be performed to identify relevant information needs:

e) examine the ISMS, its processes and other elements such as:

   1) information security policy and objectives, control objectives and controls;

   2) legal, regulatory, contractual and organizational requirements for information security; and

   3) the information security risk management process outcomes.

f) prioritize the identified information needs based on criteria, such as:

   1) risk treatment priorities;

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

2) capabilities and resources of an organization;

3) interested party needs;

4) the information security policy and objectives, and control objectives;

5) information required to meet organizational, legal, regulatory, and contractual obligations; and

6) the value of the information to be obtained in relation to the cost of measurement;

g) select a subset of information needs required to be addressed in measurement activities from the prioritized list; and

h) document and communicate the selected information needs to all relevant interested parties.

8.3 Create and maintain measures

8.3.1 General

Organizations should create measures once and thereafter review and systematically update these measures at planned intervals or when the ISMS's environment undergoes substantial changes. Such changes can include, among others:

a) the scope of the ISMS;

b) organizational structure;

c) interested parties including interested party roles, responsibilities and authorities;

d) business objectives and requirements;

e) legal and regulatory requirements;

f) achievement of desired and stable results for several subsequent cycles; and

g) introduction or disposition of information processing technologies and systems.

Creating or updating such measures can include, among others, the followings steps:

h) identify current security practices that can support information needs;

i) develop or update measures;

j) document measures and define implementation priority; and

k) keep management informed and engaged.

Updating measures is expected to take less time and effort than the initial creation.

8.3.2 Identify current security practices that can support information needs

Once an information need is identified, organizations should inventory existing measurement and security practices as a potential component of measurement. Existing measurement and security practices can include measurement associated with:

a) risk management;

b) project management;

c) compliance reporting; and

d) security policies.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

8.3.3 Develop or update measures

Measures should respond to the information need. They can rely on the current practices or they need new ones. Newly identified measures can also involve an adaptation of existing measures or measurement processes. In any case, the identified measures should be defined in sufficient detail to enable these measures to be implemented.

Examples of data that can be collected to support security measures include:

a) output of various logs and scans;

b) statistics on training and other human resource activities;

c) relevant surveys and questionnaires;

d) incident statistics;

e) results of internal audits;

f) results of business continuity/disaster recovery exercises; and

g) reports from management reviews.

These and other potential sources of data, which can be of either of internal or external origin, should be examined and types of available data identified.

The selected measures should support the priority of the information needs and can consider:

h) ease of data collection;

i) availability of human resources to collect and manage data;

j) availability of appropriate tools;

k) number of potentially relevant performance indicators supported by the measure;

l) ease of interpretation;

m) number of users of developed measurement results;

n) evidence showing the measure's fitness for purpose or information need; and

o) costs of collecting, managing, and analysing the data.

Organizations should document each measure in a form that ties the measure to the relevant information need (or needs) and provides sufficient information about the characteristics describing the measure and how to collect, analyse, and report it. Suggested information descriptors are provided in Table 1.

The examples in Annex B use Table 1 as a template. Two examples have an additional information descriptor (called "action"), which defines the action to be taken in the event that the target is not met. Organizations may include this information descriptor if they consider it useful. There is no single way to specify such measurement constructs and Annex C demonstrates an alternative free-form approach.

It should be noted that different measures may need to be provided to meet the needs of different measurement clients (see Table 1), which can be internal or external. For example, measures for addressing top management information needs can differ from those for system administrator consumption (e.g. either interested party can have a specific range or focus, or granularity).

Each measure should correspond to, at least, one information need, while a single information need might require several measures.

Organizations should take care when using subjective measures as measures formed by combining two or more subjective measures can adversely affect the final result.

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016

Table 1 — Example security measure descriptors

Information descriptor	Meaning or purpose
Measure ID	Specific identifier.
Information need	Over-arching need for understanding to which the measure contributes.
Measure	Statement of measurement, generally described using a word such as "percentage", "number", "frequency" and "average".
Formula/scoring	How the measure should be evaluated, calculated or scored.
Target	Desired result of the measurement, e.g., a milestone or a statistical measure or a set of thresholds. Note that ongoing monitoring can be required to ensure continued attainment of the target.
Implementation evidence	Evidence that validates that the measurement is performed, helps identify possible causes of poor results, and provides input to the process. Data to provide input into the formula.
Frequency	How frequently the data should be collected and reported. There can be a reason for having multiple frequencies.
Responsible parties	The person responsible for gathering and processing the measure. At the least, an Information Owner, Information Collector and Measurement Client should be identified.
Data source	Potential data sources can be databases, tracking tools, other parts of, the organization, external organizations, or specific individual roles.
Reporting format	How the measure should be collected and reported, e.g., as text, numerically, graphically (pie chart, line chart, bar graph etc.), as part of a 'dashboard' or another form of presentation.

It is very important to define measures in such way as to collect data once and use it for multiple purposes. Ideally, the same data should support a variety of measures that can respond to different interested parties' information needs. Note also that what is easiest to measure need not be most meaningful or most relevant.

Targets should state the desired end states for specific measures with respect to the ISMS processes and controls, the achievement of information security objectives, and for the effectiveness of the ISMS to be evaluated.

Establishment of targets can be facilitated if historic data that pertains to developed or selected measures is available. Trends observed in the past can in some cases provide insight into ranges of performance that have existed previously and guide the creation of realistic targets. However, organizations should be cautioned that without due consideration, setting targets based upon what was previously achieved or previous performance can also perpetuate a status quo or even impede continual improvement.

8.3.4 Document measures and prioritize for implementation

Following definition of the required measures, their compilation should be documented and prioritized for implementation based on the priority of each information need and feasibility of obtaining the data. Performance measures should be implemented first to ensure that ISMS processes and controls have been implemented. Once performance measures are producing targeted values, effectiveness measures can be implemented as well. See also 6.4 for guidance on when to perform monitoring and related activities.

8.3.5 Keep management informed and engaged

Management on different organizational levels needs to be involved in developing and implementing measures, so that the measures reflect management's needs. Furthermore, management should receive regular updates in appropriate formats and styles, to ensure that it remains informed concerning the security measurement activities throughout the process of measures development, implementation and application.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27004:2016