BS ISO/IEC 27004:2016

BSI Standards Publication

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

bsi.

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 It supersedes BS ISO/IEC 27004:2009 which is withdrawn.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.

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

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)

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.

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

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.

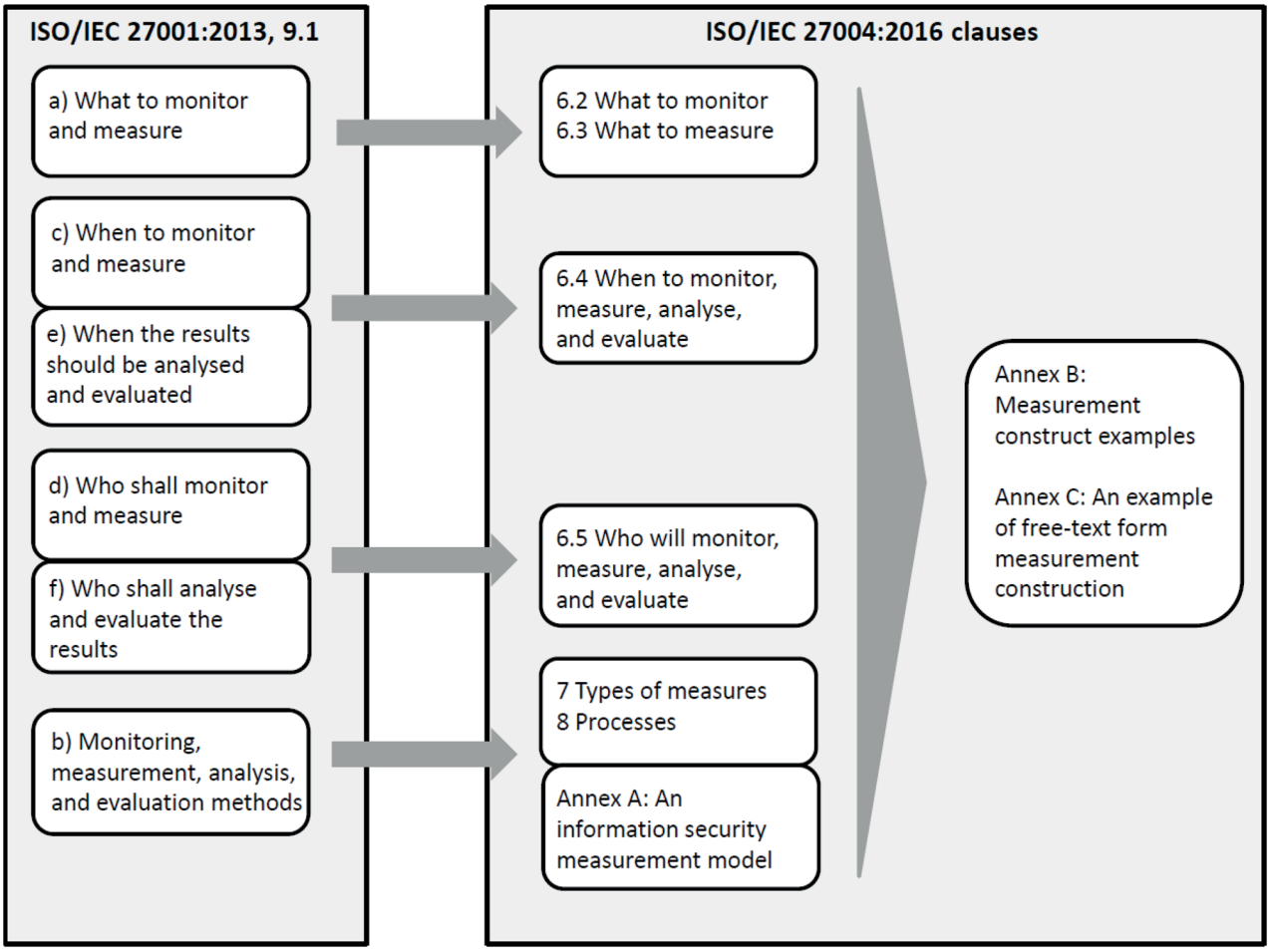

Figure 1 — Mapping to ISO/IEC 27001:2013, 9.1 requirements

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

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;

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.

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.

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.

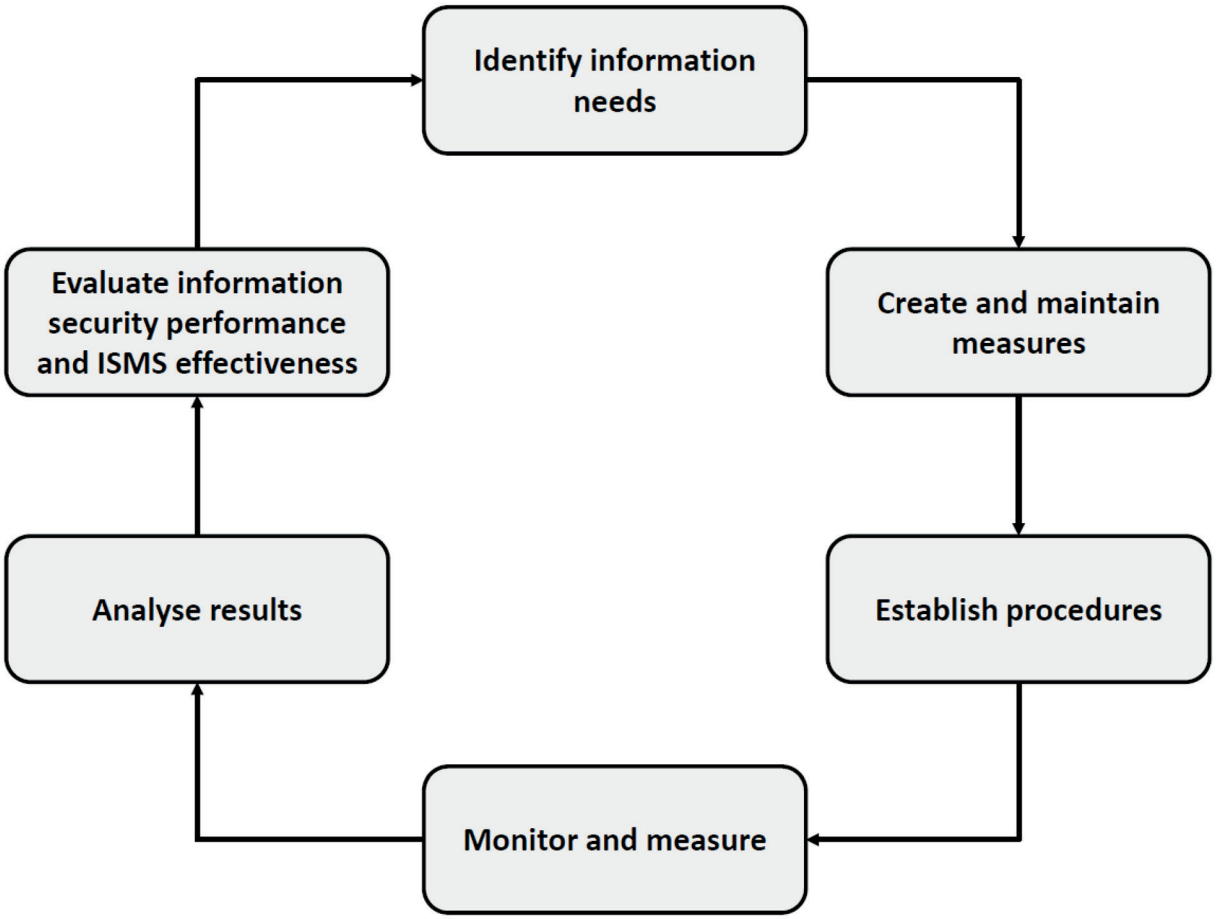

Figure 2 — Monitoring, measurement, analysis and evaluation processes

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;

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.

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.

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.

8.4 Establish procedures

To implement defined and prioritized measures the following steps should be taken:

a) interested parties who should be participating in the security measurement process should be made aware of measurement activities and the rationale behind it; and

b) data collection and analysis tools should be identified and, if needed, modified, to effectively and efficiently gather measures.

Organizations should establish procedures for data collection, analysis, and reporting of measures, for example by:

c) data collection, including secure data storage and verification. The procedures should define how data is collected, stored, verified and which context information is necessary for further processing. Data verification can be performed by applying such techniques as:

   1) ensuring a value lies within a range of possible values;

   2) checking against a list of expected values; and

   3) capturing contextual information, e.g., the time at which a datum was collected.

d) data analysis and reporting of analysis of measures. The procedures should specify the data analysis techniques and the frequency for reporting the resulting measures;

e) reporting methods and formats, which can include:

   1) scorecards to provide strategic information by integrating high-level performance indicators;

   NOTE These may be termed 'key performance indicators' (see the information security measurement model in Annex A).

   2) executive and operational dashboards focused on strategic objectives, rather than on specific controls and processes;

   3) reporting formats ranging from simple and static styles, such as a list of measures for a given time period, to more sophisticated cross-referencing reports with nested groupings, rolling summaries, and dynamic drill-through or linking. Reports can be more useful when there is a need to present interested parties with raw data in an easy-to-read format; and

   4) gauges to represent dynamic values including alerts, additional graphical elements and labelling of end-points.

8.5 Monitor and measure

Procedures for monitoring and measurement accomplished by either manual or automated means, and for storage and verification, should be defined. Data verification can be performed by qualifying the data collected against a checklist to ensure that the effects on the analysis of missing data are minimal and that the values are correct or within recognized bounds. For the purpose of analysing, sufficient data should be collected to ensure that the results of analysis are reliable.

Organizations should collect, analyse, evaluate and report measures to relevant interested parties with established periodicity. When any of the conditions stated in 8.3.1 occur, the organization should consider updating its monitoring, measurement, analysis, and evaluation processes.

Prior to publishing information in reports, dashboards, etc., the organization should determine how collected data and results can be shared, and with whom, as some information security-related data can be sensitive from a confidentiality perspective.

Moreover, there is benefit to having a process to check and evaluate the collection process to confirm that the right measures are being collected and in a manner such that they are repeatable, precise and consistent.

8.6 Analyse results

Collected data should be analysed in relation to the target for each individual measure. Guidance for performing statistical analysis can be found in ISO/TR 10017.

The data analysis results should be interpreted. The person analysing the results (communicator) should be able to draw some initial conclusions based on the results. However, since the communicator(s) might not be directly involved in the technical and management processes, such conclusions need to be reviewed by other interested parties. All interpretations should take into account the context of the measures.

Data analysis should identify gaps between the expected and actual measurement results of an implemented ISMS, controls or groups of controls. Identified gaps can point to needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

8.7 Evaluate information security performance and ISMS effectiveness

In accordance with 5.2, organizations should:

a) express their information needs in terms of the organization's questions concerning information security performance and ISMS effectiveness; and

b) express their measures in terms of those information needs.

It therefore follows that the analysis of the results of monitoring and measurement will provide data which can be used to satisfy the information needs (see Annex A). Evaluation is the process of interpreting that data to answer the organization's information security performance and ISMS effectiveness questions.

8.8 Review and improve monitoring, measurement, analysis and evaluation processes

Monitoring, measurement, analysis, and evaluation processes should continually improve with the needs of the ISMS. Continual improvement activities can include, among other things:

a) soliciting feedback from interested parties;

b) revising collection and analysis techniques, based on lessons learned and other feedback;

c) revising implementation procedures; and

d) information security benchmarking data.

8.9 Retain and communicate documented information

In order to fulfil the requirements of ISO/IEC 27001:2013, 9.1, it is only necessary for organizations to retain documented information as evidence of the organization's monitoring and measurements. Organizations are at liberty to decide what is appropriate. Organizations can, for example, document the process and the methods used to analyse and evaluate the results.

Reports that are used to communicate measurement results to relevant interested parties should be prepared using appropriate reporting formats. The conclusions of the analysis should be reviewed by relevant interested parties to ensure proper interpretation of the data. The results of data analysis should be documented for communication to interested parties.

The information communicator should determine how to communicate the information security measurement results, such as:

a) which measurement results should be reported internally and externally;

b) listings of measures corresponding to individual interested parties, and interested parties;

c) specific measurement results to be provided, and the type of presentation, tailored to the needs of each group; and

d) means for obtaining feedback from the interested parties to be used for evaluating the usefulness of measurement results and the effectiveness of information security measurement.

Annex A
(informative)

An information security measurement model

The measurement information model described in Figure A.1 is presented and explained in ISO/IEC 15939, and can be applied to ISMS. It describes how attributes of relevant entities can be quantified and converted to indicators that provide a basis for decision making. The model is a structure which starts with linking information needs to the relevant entities and attributes of concern. For example, the information need can be how well the employees are informed about the information security policy. Entities include processes, controls, documented information, systems, devices, personnel and resources. Examples of relevant entities in an ISMS are: risk management process, auditing process, information classification, management of access rights, information security policy, mobile device policy, back-end computer, administrator and employee.

The measurement information model helps to determine what the measurement planner needs to specify during monitoring, measurement, analysis, and evaluation.

ISO/IEC 27001:2013, 9.1 requires that organizations evaluate the information security performance and the effectiveness of the ISMS. This often involves the identification of indicators, and from these, according to the significance and importance of the indicators to the organization's purposes, key performance indicators (KPI – sometimes also referred to as 'key success indicators') can be identified.

To determine such indicators, an organization can establish base measures and derive a measure from them by using a measurement function that combines two or more base measures.

The measurement model in this Annex (using base measure, derived measure, performance indicator and measurement result) is an example of the approach to fulfil the ISMS requirements for measurement. There are other possible ways of looking at the process of measurement, analysis and evaluation.

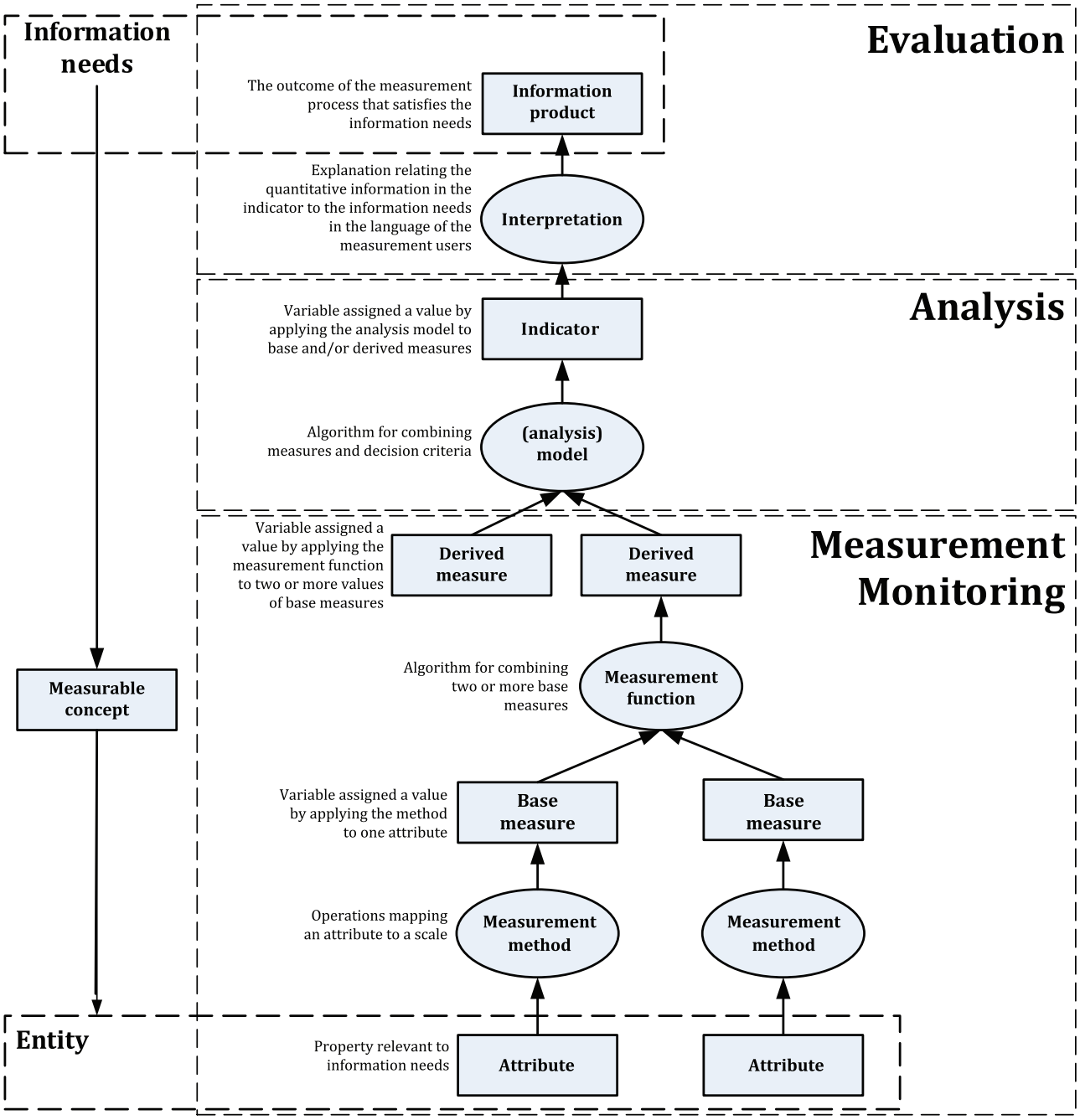

Figure A.1 — Key relationships in the measurement information model

Annex B
(informative)

Measurement construct examples

B.1 General

The examples in Annex B follow the principles set out in this document. The table below maps measurement construct examples to specific clauses or control objective numbers in ISO/IEC 27001:2013.

Related ISMS processes and controls (Clause or control number in ISO/IEC 27001:2013)	**Measurement construct example names**
5.1, 7.1	B.2 Resource allocation
7.5.2, A.5.1.2	B.3 Policy review
5.1, 9.3	B.4 Management commitment
8.2, 8.3	B.5 Risk exposure
9.2, A.18.2.1	B.6 Audit programme
10	B.7 Improvement actions
10	B.8 Security incidents cost
10, A.16.1.6	B.9 Learning form information security incidents
10.1	B.10 Corrective action implementation
A.7.2	B.11 ISMS training or ISMS awareness
A.7.2.2	B.12 Information security training
A.7.2.1, A.7.2.2	B.13 Information security awareness compliance
A.7.2.2	B.14 ISMS awareness campaigns effectiveness
A.7.2.2, A.9.3.1, A.16.1	B.15 Social engineering preparedness
A.9.3.1	B.16 Password quality – manual
A.9.3.1	B.17 Password quality – automated
A.9.2.5	B.18 Review of user access rights
A.11.1.2	B.19 Physical entry controls system evaluation
A.11.1.2	B.20 Physical entry controls effectiveness
A.11.2.4	B.21 Management of periodic maintenance
A.12.1.2	B.22 Change management
A.12.2.1	B.23 Protection against malicious code
A.12.2.1	B.24 Anti-malware
A.12.2.1, A.17.2.1	B.25 Total availability
A.12.2.1, A.13.1.3	B.26 Firewall rules
A.12.4.1	B.27 Log files review
A.12.6.1	B.28 Device configuration
A.12.6.1, A.18.2.3	B.29 Pentest and vulnerability assessment
A.12.6.1	B.30 Vulnerability landscape
A.15.1.2	B.31.1/B.31.2 Security in third party agreements

Related ISMS processes and controls (Clause or control number in ISO/IEC 27001:2013)	Measurement construct example names
A.16	B.32 Security incident management effectiveness
A.16.1	B.33 Security incidents trend
A 16.1.3	B.34 Security event reporting
A.18.2.1	B.35 ISMS review process
A.18.2.3	B.36 Vulnerability coverage

A cross reference of the relationship to clauses or control objective numbers in ISO/IEC 27001:2013 is included for each example. In addition, for two examples (B.20 and B.28) an additional information descriptor called "action" is included. This 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. Indeed, there is no single way to specify such measurement constructs and Annex C demonstrates an alternative free-form approach.

B.2 Resource allocation

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Quantify resources which are being allocated to information security with respect to original budgets
Measure	Breakdown of resources allocated to information security (internal personnel, contracted personnel, hardware, software, services) within annual budget
Formula/scoring	Allocated resources/used resources within a budgeted period of time
Target	1
Implementation evidence	Information security resource monitoring
Frequency	Yearly
Responsible parties	Information Owner: information security manager Information Collector: information security manager Information Customer: board of directors
Data source	Information security budget Information security effective expenditure Information security resources usage reports
Reporting format	Radar diagram with a resource category for each axis and the double indication of allocated and used resources

Relationship	ISO/IEC 27001:2013, 5.1: Leadership and commitment ISO/IEC 27001:2013, 7.1: Resources

B.3 Policy review

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate whether the policies for information security are reviewed at planned intervals or if significant changes occur
Measure	Percentage of policy reviewed
Formula/scoring	Number of information security policies that were reviewed in previous year/ Number of information security policies in place * 100
Target	Green: >80, Orange >=40%, Red <40%
Implementation evidence	Document history mentioning review of document or document list indicating date of last review
Frequency	Collect: after planned interval defined for reviews (e.g. yearly or after significant changes) Report: for each collection
Responsible parties	Information owner: Policy owner who has approved management responsibility for the development, review and evaluation of the policy Information collector: Internal auditor Measurement client: Chief information security officer
Data source	Review plan of policies, history section of a security policy, list of documents
Reporting format	Pie chart for current situation and line chart for compliance evolution representation

Relationship — ISO/IEC 27001:2013, A.5.1.2: Review of the policies for information security

ISO/IEC 27001:2013, 7.5.2: Creating and updating of documented information

B.4 Management commitment

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Assess management commitment and information security review activities regarding management review activities
Measure	a) Management review meetings completed to date b) Average participation rates in management review meetings to date
Formula/scoring	a) Divide [management review meetings performed] by [management review meetings scheduled] b) Compute mean and standard deviation of all participation rates to management review meetings
Target	Resulting ratio of indicator a) should fall between 0.7 and 1.1 to conclude the achievement of the control objective and no action. Even if it fails, it should be still over 0.5 to conclude the least achievement. With regard to indicator b), Computed confidence limits based on the standard deviation indicate the likelihood that an actual result close to the average participation rate will be achieved. Very wide confidence limits suggest a potentially large departure and the need for contingency planning to deal with this outcome.
Implementation evidence	1.1 Count management review meetings scheduled to date 1.2 Per management review meetings to date, count managers planned to attend and add a new entry with a default value for unplanned meetings performed in an ad hoc manner 2.1.1 Count planned management review meetings held to date 2.1.2 Count unplanned management review meetings held to date 2.1.3 Count rescheduled management review meetings held to date 2.2 For all management review meetings that were held, count the number of managers who attended
Frequency	Collect: Monthly Analysis: Quarterly Report: Quarterly Measurement revision: Review and update every 2 years Period of measurement: Applicable 2 years
Responsible parties	Information owner: Quality system manager (assuming combined management system of QMS and ISMS) Information collector: Quality manager; Information security manager Measurement client: Managers responsible for ISMS; Quality system manager
Data source	1. Information security management review plan/schedule 2. Management review minutes/records
Reporting format	Line chart depicting indicator with criteria over several data collection and reporting periods with the statement of measurement results. The number of data collection and reporting periods should be defined by the organization.

Relationship — ISO/IEC 27001:2013, 9.3: Management review
ISO/IEC 27001:2013, 5.1: Leadership and commitment

B.5 Risk exposure

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Assess exposure of the organization to information security risks
Measure	a) High and medium risks beyond acceptable threshold b) Timely review of high and medium risks
Formula/scoring	a) Threshold for high and medium risks should be defined and responsible parties alerted if the threshold is breached b) Number of risks without status update
Target	1
Implementation evidence	Updated risk register
Frequency	Collect: minimum quarterly Report: each quarter
Responsible parties	Information owner: Security staff Information collector: Security staff
Data source	Information risk register
Reporting format	Trend of high risks Trend of accepted high and medium risks

Relationship — ISO/IEC 27001:2013, 8.2: Information security risk assessment
ISO/IEC 27001:2013, 8.3: Information Security Risk Treatment

B.6 Audit programme

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Completeness of the audit programme
Measure	Total number of audit performed compared with the total number of audits planned
Formula/scoring	(Total number of audits performed) / (Total number of audits planned) * 100.
Target	>95%
Implementation evidence	Audit programme and related reports monitoring
Frequency	Yearly
Responsible parties	Information owner: Audit manager Information collector: Audit manager Information customer: Top management
Data source	Audit programme and audit reports
Reporting format	Trend chart linking the ratio of completed audits against the programme for each sampled year

Relationship

ISO/IEC 27001:2013, 9.2: Internal audit

ISO/IEC 27001:2013, A.18.2.1: Independent review of information security

B.7 Improvement actions

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Verify the status of improvement actions and their management according with plans
Measure	Percentage of actions on time, costs and quality (i.e. requirements) against all planned actions The actions should be the ones planned (i.e. opened, stand-by and in progress) in the beginning of the timeframe
Formula/scoring	[(Actions on time, costs and quality) / (Number of actions)] * 100
Target	90%
Implementation evidence	Status monitoring of each action
Frequency	Quarterly
Responsible parties	Information Owner: project management office Information Collector: project management office Information Customer: information security manager
Data source	Relevant project plans
Reporting format	List of all relevant actions and their status (actual time, costs and quality forecast against the planned ones) with the percentage of actions on time, costs and quality against the relevant number of actions in the timeframe

Relationship ISO/IEC 27001:2013, Clause 10: Improvement

Note that this measure may be improved by weighting each action considering their criticality (e.g., actions that address high risks).

A list of all relevant actions should be together with the synthetic result, so that a high number of non-critical but within acceptable boundaries won't hide a low number of critical actions outside acceptable boundaries.

B.8 Security incident cost

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Considerations about costs arising from lack of information security
Measure	Sum of costs for each information security incident occurred in the sampling period
Formula/scoring	Sum (costs of each information security incident)
Target	Less than an acceptable threshold defined by the organization
Implementation evidence	Systematic gathering of costs for each information security incidents
Frequency	Quarterly
Responsible parties	Information owner: Computer security incident response team (CSIRT) Information collector: Information security manager Information customer: Top management
Data source	Incident reports
Reporting format	Column chart showing costs of information security incidents for this and previous sampling periods. It can be followed by a drill-down with: — average cost of each information security incident; — average cost of each information security incident for each information security incident category (categories should be previously defined).

Relationship ISO/IEC 27001:2013, Clause 10: Improvement

B.9 Learning from information security incidents

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Verify whether security incidents trigger actions for improving the current security situation
Measure	Number of security incidents that trigger information security improvement actions
Formula/scoring	Sum of security incidents that triggered actions/Sum of security incidents
Target	Value should be higher than the threshold defined by the organization
Implementation evidence	Action plan with link to security incidents
Frequency	Collect: Quarterly Report: Every semester
Responsible parties	Information owner: Computer security incident response team (CSIRT) Information collector: Information security manager Information customer: Information security manager
Data source	Incident reports
Reporting format	Column chart showing costs of information security incidents for this and previous sampling periods. It can be followed by a drill-down with: — average cost of each information security incident; — average cost of each information security incident for each information security incident category (categories should be previously defined).

Relationship ISO/IEC 27001:2013, Clause 10: Improvement

ISO/IEC 27001:2013, A.16.1.6: Learning from information security incidents

B.10 Corrective action implementation

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Assess performance of corrective action implementation
Measure	a) Status expressed as a ratio of corrective action not implemented b) Status expressed as a ratio of corrective action not implemented without reason c) Trend of statuses
Formula/scoring	a) Divide [Corrective action not implemented to date] by [Corrective actions planned to date] b) Divide [Corrective action not implemented without reason] by [Corrective actions planned to date] c) Compare Statuses with Previous statuses
Target	In order to conclude the achievement of the objective and no action, the ratios of indicator a) and b) should fall respectively between 0.4 and 0.0 and between 0.2 and 0.0, and Trend of indicator c) should have been declining for the last 2 reporting periods. The indicator c) should be presented in comparison with previous indicators so that the trend in corrective action implementation can be examined.
Implementation evidence	1. Count corrective actions planned to be implemented to date 2. Count corrective actions recorded as implemented by due date 3. Count corrective actions recorded as planned actions not taken with the reason
Frequency	Collect: Quarterly Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Applicable 1 year
Responsible parties	Information owner: Managers responsible for ISMS Information collector: Managers responsible for ISMS Measurement client: Managers responsible for ISMS; Information security manager
Data source	Corrective action reports
Reporting format	Stacked bar chart with the statement of measurement results including an executive summary of findings and possible management actions, that depicts total number of corrective actions, separated into implemented, not implemented without a legitimate reason, and not implemented with a legitimate reason.

Relationship ISO/IEC 27001:2013, 10.1: Nonconformity and corrective action

B.11 ISMS training or ISMS awareness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To measure how many employees received an ISMS related awareness training and establish control compliance with the organization's information security policy
Measure	Percentage of employees having participated to an ISMS awareness training
Formula/scoring	I1 = [Number of employees who received ISMS training/number of employees who have to receive ISMS training] * 100 I2 = [Number of employees who renewed their ISMS training in the last year / number of employee in scope] * 100
Target	Green: if I1>90 and I2>50% otherwise Yellow: if I1>60% and I2>30% otherwise Red Red – intervention is required, causation analysis must be conducted to determine reasons for non-compliance and poor performance Yellow – indicator should be watched closely for possible slippage to Red Green – no action is required
Implementation evidence	Participation lists of all awareness trainings; count of logs/registries with ISMS training field/row filler as "Received"
Frequency	Collect: Monthly, first working day of the month Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Annual
Responsible parties	Information owner: Training manager – Human resources Information collector: Training management – Human resource department Measurement client: Managers responsible for an ISMS, Chief information security officer
Data source	Employee database, training records, participation list of awareness trainings
Reporting format	Bar graph with bars colour-coded based on target. Short summary of what the measure means and possible management actions should be attached to the bar chart. OR Pie chart for current situation and line chart for compliance evolution representation.

Relationship ISO/IEC 27001:2013, A.7.2: Competence.

B.12 Information security training

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate compliance with annual information security awareness training requirement
Measure	Percentage of personnel who received annual information security awareness training
Formula/scoring	[Number of employees who received annual information security awareness training/number of employees who need to receive annual information security awareness training] * 100
Target	0-60% - Red; 60-90% - Yellow; 90-100% Green. For Yellow, if progress of at least 10% per quarter is not achieved, rating is automatically red. Red – intervention is required, causation analysis must be conducted to determine reasons for non-compliance and poor performance. Yellow – indicator should be watched closely for possible slippage to Red. Green – no action is required.
Implementation evidence	Count of logs/registries with annual information security awareness training field/row filler as "Received"
Frequency	Collect: Monthly, first working day of the month Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Annual
Responsible parties	Information owner: Information security officer and Training manager Information collector: Training management – Human resource department Measurement client: Managers responsible for an ISMS; Security management; Training management
Data source	Employee database, training records
Reporting format	Bar graph with bars colour-coded based on target. Short summary of what the measure means and possible management actions should be attached to the bar chart.

Relationship — ISO/IEC 27001:2013, A.7.2.2: Information security awareness, education and training.

B.13 Information security awareness compliance

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Assess status of compliance with organization security awareness policy among relevant personnel
Measure	1. Progress to date 2. Progress to date with signing
Formula/scoring	Derive the "progress to date" by adding status for all personnel having signed, planned to be completed to date Derive "progress to date with signing" by divide personnel having signed to date by personnel planned for signing to date a) [divide progress to date by (personnel planned to date times 100)] and progress to date with signing b) Compare status with previous statuses
Target	a) Resulting ratios should fall respectively between 0.9 and 1.1 and between 0.99 and 1.01 to conclude the achievement of the control objective and no action; and b) Trend should be upward or stable
Implementation evidence	1.1. Count number of personnel scheduled to have signed and completed the training to date 1.2. Ask responsible individual for percent of personnel who have completed the training and signed 2.1. Count number of personnel scheduled to have signed by this date 2.2. Count number of personnel having signed user agreements
Frequency	Collect: Monthly, first working day of the month Analysis: Quarterly Report: Quarterly Measurement Revision: Review annually Period of Measurement: Annual
Responsible parties	Information owner: Information security officer and Training manager Information collector: Training management; Human resource department Measurement client: Managers responsible for an ISMS; Security management. training management
Data source	1.1. Information security awareness training plan/schedule: Personnel identified in plan 1.2 Personnel who have completed or in progress in the training: Personnel status with regard to the training 2.1. Plan for signing user agreements/schedule: Personnel identified in plan for signing 2.2. Personnel having signed agreements: Personnel status with regard to the signing of agreements
Reporting format	Standard Font = Criteria have been met satisfactorily Italic Font = Criteria have been met unsatisfactorily Bold Font = Criteria have not been met

Relationship	ISO/IEC 27001:2013, A.7.2.2: Management responsibilities
	ISO/IEC 27001:2013, A.7.2.1: Information security awareness, education and training

B.14 ISMS awareness campaigns effectiveness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To measure if employees have understood content of awareness campaign
Measure	Percentage of employees passing a knowledge test before and after ISMS awareness campaign
Formula/scoring	Choose a given number of employees who were targeted by an awareness campaign and let them fill out a short knowledge test about topics of the awareness campaign Percentage of people passed the test
Target	Green: 90-100% of people passed the test, Orange: 60-90% of people passed the test, Red: <60% of people passed the test
Implementation evidence	Awareness campaign documents/information provided to employees; list of employees who followed awareness campaign; knowledge tests
Frequency	Collect: one month after awareness campaign Report: for each collection
Responsible parties	Information owner: Human resources Information collector: Human resources Measurement client: Information security manager
Data source	Employee database, awareness campaign information, knowledge test results
Reporting format	Pie chart for representing percentage of staff members passed the test situation and line chart for evolution representation if extra training has been organised for a specific topic

Relationship — ISO/IEC 27001:2013, A.7.2.2: Information security awareness, education and training

B.15 Social engineering preparedness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate whether staff is prepared to react properly in case of some social engineering attacks
Measure	Percentage of staff that react correctly to a test, e. g., who did not click on a link in a given test consisting in sending a phishing email to (a selected part of the) staff
Formula/scoring	a = Number of staff having clicked on the link/number of staff participating in the test b = 1-Number of staff having reported the dangerous email through appropriate channels c = Number of staff having followed the instruction given when clicking on the link, i.e. start revealing a password/number of staff participating d = An appropriate weighted sum of the above parameter, depending on the nature of the test
Target	d: 0-60: Red, 60-80: Yellow, 90-100: Green
Implementation evidence	Count of activity on a simulated command and control addressed by the link. Take care to respect personnel privacy aspects, and to anonymise data so that test participants do not have to fear negative consequences from this test.
Frequency	Collect: monthly to annually, depending on the criticality of social engineering attacks Report: for each collection
Responsible parties	Information owner: Chief information security officer Information collector: IT security officer trained to respect privacy aspects Measurement client: Risk owner
Data source	List of staff, or users of a given service; Awareness support, communication (email or intranet)
Reporting format	Test report indicating test details, measurements, analysis of results, and recommendation, based on target and agreed treatment

Relationship

ISO/IEC 27001:2013, A.16.1: Management of information security incidents and improvements

ISO/IEC 27001:2013, A.9.3.1: Use of secret authentication information

ISO/IEC 27001:2013, A.7.2.2: Information security awareness, education and training

B.16 Password quality – manual

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the quality of the passwords used by the Users to access the organization's IT systems
Measure	Total number of passwords that comply with organization's password quality policy a) Ratio of passwords which meet organization's password quality policy b) Trends of compliance status regarding password quality policy
Formula/scoring	Count number of passwords in user password database Determine the number of passwords which satisfy organization's password policy Σ of [Total number of passwords that comply with organization's password quality policy for each user] a) Ratio of passwords which meet organization's password quality policy b) Trends of compliance status regarding password quality policy c) Divide [Total number of passwords complied with organization's password quality policy] by [Number of registered passwords] d) Compare ratio with the previous ratio
Target	Control objective is achieved and no action required if the resulting ratio is above 0.9. If the resulting ratio is between 0.8 and 0.9 the control objective is not achieved, but positive trend indicates improvement. If the resulting ratio is below 0.8 immediate action should be taken.
Implementation evidence	1 Count number of passwords on user password database 2 Determine the number of passwords which satisfy organization's password policy Configuration file, password setting or configuration tool
Frequency	Collect: Depending on the criticality but minimum yearly Analysis: After each collection Report: After each analysis Measurement Revision: Yearly Period of Measurement: Yearly
Responsible parties	Information owner: System administrator Information collector: Security staff Measurement client: Managers responsible for an ISMS, Security manager
Data source	User password database; Individual passwords
Reporting format	Trend line that depicts the number of passwords compliant with organization's password quality policy, superimposed with trend lines produced during previous reporting periods.

Relationship ISO/IEC 27001:2013, A.9.3.1: Use of secret authentication information

B.17 Password quality – automated

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the quality of the passwords used by the Users to access the organization's IT systems
Measure	1 Total number of passwords 2 Total number of uncrackable passwords
Formula/scoring	1 Ratio of passwords crackable within 4 hours 2 Trend of the ratio 1 a) Divide [Number of uncrackable passwords] by [Total number of passwords] b) Compare ratio with the previous ratio
Target	Control objective is achieved and no action required if the resulting ratio is above 0.9. If the resulting ratio is between 0.8 and 0.9 the control objective is not achieved, but positive trend indicates improvement. If the resulting ratio is below 0.8 immediate action should be taken.
Implementation evidence	1 Run query on employee account records 2 Run password cracker on employee system account records using hybrid attack
Frequency	Collect: Weekly Analysis: Weekly Report: Weekly Measurement revision: Review and update every year Period of measurement: Applicable 3 years
Responsible parties	Information owner: System administrator Information collector: Security staff Measurement client: Managers responsible for an ISMS, Security manager
Data source	Employee system account database
Reporting format	Trend line that depicts password crackability for all records tested superimposed with lines produced during previous tests.

Relationship ISO/IEC 27001:2013, A.9.3.1: Use of secret authentication information

B.18 Review of user access rights

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Measure on how many systematic user access rights reviews are performed on critical systems
Measure	Percentage of critical systems where user access rights are periodically reviewed
Formula/scoring	[Number of information systems classified as critical where periodic access rights reviews are performed/Total number of information systems classified as critical] * 100
Target	Green: 90-100%, Orange: 70-90%, Red <70%
Implementation evidence	Proofs of reviews (e.g. email, ticket in ticketing system, formula proofing review completion)
Frequency	Collect: After any changes such as promotion, demotion or termination of employment Report: each semester
Responsible parties	Information owner: Risk owner Information collector: Chief information security officer Measurement client: Information security manager
Data source	Asset inventory, system used to track if reviews were performed, e.g., Ticketing system
Reporting format	Pie chart for current situation and line chart for compliance evolution representation

Relationship ISO/IEC 27001:2013, A.9.2.5: Review of user access rights

B.19 Physical entry controls system evaluation

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To show the existence, extent and quality of the system used for access control
Measure	Strength of physical entry controls system
Formula/scoring	Scale from 0-5 **0** There is **no access control system** **1** There is an access system where **PIN code** (one factor system) is used for entry control **2** There is an access control **card** system where pass card (one factor system) is used for entry control **3** There is an access card system where **pass card and PIN code** is used for entry control **4** Previous + **log functionality** activated **5** Previous + PIN code is replaced by **biometric authentication** (fingerprint, voice recognition, retina scan etc.)
Target	Value 3= satisfactory
Implementation evidence	Qualitative assessment where each subset grade is a part of the grade above. Control the type of entry control system and inspect the following aspects: — Access control card system existence — PIN code usage — Log functionality — Biometric authentication
Frequency	Collect: Yearly Analysis: Yearly Report: Yearly Measurement revision: 12 months Period of measurement: Applicable 12 months
Responsible parties	Information owner: Facility manager Information collector: Internal auditor/external auditor Measurement client: Management committee
Data source	Identity management records
Reporting format	Graphs

Relationship ISO/IEC 27001:2013, A.11.1.2: Physical entry controls

B.20 Physical entry controls effectiveness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	1. Ensure an environment of comprehensive security and accountability for personnel, facilities, and products 2. Integrate physical and information security protection mechanisms to ensure appropriate protection of the organization's information resources
Measure	Number of unauthorized entry into facilities containing information systems (subset of physical security incidents)
Formula/scoring	Current number of physical security incidents allowing unauthorized entry into facilities containing information systems/previous value (Note that these measures need to take into account organization-specific context such as the total number of physical security incidents)
Target	Below 1.0
Implementation evidence	Systematic analysis of physical security incident reports and access control logs
Frequency	Quarterly for data gathering and reporting
Responsible parties	Information owner: Physical security officer Information collector: Computer security incident response team (CSIRT) Information customer: Chief information officer, Chief information security officer
Data source	Physical security incident reports Physical access control logs
Reporting format	Plot showing trend of unauthorized entry into facilities containing information systems for the most recent sampling periods

Relationship ISO/IEC 27001:2013, A.11.1.2: Physical entry controls

Action Review and improve physical security controls applied to information systems.

B.21 Management of periodic maintenance

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate timeliness of maintenance activities in relation to schedule
Measure	Maintenance delay per completed maintenance event
Formula/scoring	For each completed event, subtract [Date of actual maintenance] from [Date of scheduled maintenance]
Target	1. Organization-specific, for example, if average delay is consistently showing at over 3 days, the causes need to be examined 2. Ratio of completed maintenance events should be greater than 0.9 3. Trend should be stable or close to 0 4. Trend should be stable or upwards
Implementation evidence	1 Dates of scheduled maintenance 2 Dates of completed maintenance 3 Total number of planned maintenance events 4 Total number of completed maintenance events
Frequency	Collect: quarterly Report: annually
Responsible Parties	Information owner: System administrator Information collector: Security staff Measurement client: Security manager, IT manager
Data source	1 Plan/schedule of system maintenances 2 Records of system maintenances
Format	Line chart that depicts the average deviation of maintenance delay, superimposed with lines produced during previous reporting periods and the numbers of systems within the scope An explanation of findings and recommendation for potential management action

Relationship ISO/IEC 27001:2013, A.11.2.4: Equipment maintenance

B.22 Change management

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Evaluate whether change management best practice as well hardening policy are respected
Measure	Percentage of new installed systems that were respected change management best practice and hardening policy
Formula/scoring	Number of newly installed applications or systems where evidences of respecting the change management best practices are available/number of newly installed applications
Target	All systems must follow the change management guidelines
Implementation evidence	Ticketing system, e-mails, reports, checklist used for configuration
Frequency	Collect: Every semester Report: Yearly to management, each semester to Information security manager
Responsible parties	Information owner: Risk owner Information collector: Risk owner Measurement client: Information security manager
Data source	Ticketing system, e-mails, reports, checklist used for configuration, configuration review tool report
Reporting format	Pie chart for current situation and line chart for compliance evolution representation

Relationship ISO/IEC 27001:2013, A.12.1.2: Change management

B.23 Protection against malicious code

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the effectiveness of the protection system against malicious software attacks
Measure	Trend of detected attacks that were not blocked over multiple reporting periods
Formula/scoring	Number of security incidents caused by malicious software/number of detected and blocked attacks caused by malicious software
Target	Trend line should remain under specified reference, resulting in a downward or constant trend
Implementation evidence	1 Count number of security incidents caused by malicious software in the incident reports 2 Count number of records of blocked attacks
Frequency	Collect: Daily Analysis: Monthly Report: Monthly Measurement Revision: Review annually Period of Measurement: Applicable 1 year
Responsible parties	Information owner Information collector Measurement client
Data source	1 Incident reports 2 Logs of countermeasure software for malicious software
Reporting format	Trend line that depicts ratio of malicious software detection and prevention with lines produced during previous reporting periods

Relationship ISO/IEC 27001:2013, A.12.2.1: Controls against malware

NOTE Organizations adopting this measure should consider the following issues that may lead to an incorrect analysis of such measure:

— “number of detected and blocked attacks caused by malicious software” can be very high; thus such measure can result in very small ratios;

— if in one period there is an increase of spreading of a specific virus, an organization may experience an increase of malware attacks and incidents; in this case the ratio remains the same, even if the increase of incidents can raise concern.

B.24 Anti-malware

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Number of malware affected systems which do not have an updated anti-malware solution
Measure	Percentage of malware affected systems connected to the organization's network with obsolete (e.g. more than one week) antimalware signatures
Formula/scoring	(Number of obsolete antivirus) / (Total workstation)
Target	0 or a small value decided by the organization
Implementation evidence	Monitoring of antivirus activities in each malware affected system
Frequency	Daily
Responsible parties	Information owner: IT operations Information collector: IT operations Information customer: Chief information security officer
Data source	Monitoring tools Antimalware console
Reporting format	Numbers per system classes (workstations, servers, o/s)

Relationship ISO/IEC 27001:2013, A.12.2.1: Controls against malware

B.25 Total availability

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Availability of IT services for each service, compared with the defined maximum downtime
Measure	For each IT service the end-to-end availability is compared with the maximum availability (i.e., excluding the previously defined downtime windows)
Formula/scoring	(Total availability)/(Maximum availability excluding downtime windows)
Target	Service availability target
Implementation evidence	Monitoring of end-to-end availability of each IT service
Frequency	Monthly
Responsible parties	Information owner: IT operations Information collector: IT quality Information customer: Chief information officer
Data source	Monitoring tools
Reporting format	For each service, two lines: 1. line linking the actual availability (percentage) of each sampled period 2. line (for comparison purposes) showing the availability target

Relationship ISO/IEC 27001:2013, A.17.2.1: Availability of information processing facilities

B.26 Firewall rules

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Evaluate current firewall performance
Measure	Unused firewall rules on border firewalls
Formula/scoring	Count of border firewall rules which have been used 0 times in the last sampling period
Target	0
Implementation evidence	Records of usage counters on each firewall rules
Frequency	Bi-annual or yearly
Responsible parties	Information owner: network manager/information security manager Information collector: network analyst/security analyst Information customer: network manager/information security manager
Data source	Firewall management console, firewall review report
Reporting format	Count or list of unused firewall rules to be marked for review and possible deletion

Relationship ISO/IEC 27001:2013, A.13.1.3: Segregation in networks

B.27 Log files review

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the status of compliance of the regular review of critical system log files
Measure	Percentage of audit log files reviewed when required per time period
Formula/scoring	[# of log files reviewed within specified time period/total # of log files]*100
Target	Result below 20% should be examined for causes of underperformance
Implementation evidence	Add up total number of log files listed in the review log list
Frequency	Collect: Monthly (depending on the criticality, it could go to daily or real-time) Analysis: Monthly (depending on the criticality, it could go to daily or real-time) Report: Quarterly Measurement Revision: Review and update every 2 years Period of Measurement: Applicable 2 years
Responsible parties	Information owner: Security manager Information collector: Security staff Measurement client: Managers responsible for an ISMS, Security manager
Data source	System; individual log files; evidence of the log review
Reporting format	Line chart that depicts the trend with a summary of findings and any suggested management actions

Relationship ISO/IEC 27001:2013, A.12.4.1: Event logging

B.28 Device configuration

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Validate that our devices are continually securely configured according to policy
Measure	Percentage of devices (by type) configured according to policy
Formula/scoring	[Number of devices configured correctly/total # devices] * 100 (total number of devices is organization-specific and may include any and all of the following: devices registered in configuration management database, devices found but not registered in configuration management database, devices running a specific operating system/version, mobile devices, etc.)
Target	100%
Implementation evidence	Based on automated scanning: authoritative device inventory; authoritative software inventory; configuration scanning results
Frequency	Scan every 3 days; report immediately
Responsible Parties	Information owner: Network management Information collector: Network management Information customer: Chief information officer
Data source	Configuration control board; inventory database; scanning tools
Reporting format	Line chart for trends, vulnerable hosts by name
Action	Disconnect unapproved devices from the network; patch non-compliant devices; review and revise as necessary configuration management guidelines; etc.

Relationship ISO/IEC 27001:2013, A.12.16.1: Management of technical vulnerabilities

B.29 Pentest and vulnerability assessment

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate whether information systems handling sensitive data (confidentiality, integrity) are vulnerable to malicious attacks
Measure	Percentage of critical information systems where a penetration test or vulnerability assessment has been executed since their last major release
Formula/scoring	[Number of information systems quantified as critical and where a penetration test or vulnerability assessment has been done since their last major release/ Number of information systems quantified as critical] * 100, e.g. Green: 100%, Orange >=75%, Red <75%
Target	Orange (Green would be too perfect)
Implementation evidence	Reports of penetration tests or vulnerability assessments performed on information systems compared to number of information systems classified as critical in the asset inventory
Frequency	Collect: yearly Report: for each collection
Responsible parties	Information owner: Risk owner Information collector: Experts with the know-how to conduct penetration tests or execute vulnerability assessments Measurement client: Chief information security officer
Data source	Asset inventory, penetration test reports
Reporting format	Pie chart for current situation and line chart for compliance evolution representation

Relationship

ISO/IEC 27001:2013, A.12.6.1: Management of technical vulnerabilities

ISO/IEC 27001:2013, A.18.2.3: Technical compliance review

B.30 Vulnerability landscape

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Evaluate the vulnerability level of the organization's information systems
Measure	Weight of open (unpatched) vulnerabilities
Formula/scoring	Open vulnerability severity value (e.g. CVSS) * number of affected systems
Target	To be defined accordingly to the organization's risk appetite
Implementation evidence	Analysis on vulnerability assessment activities
Frequency	Monthly or quarterly
Responsible parties	Information owner: information security analysts or contracted third parties Information collector: information security analysts Information customer: information security manager
Data source	Vulnerability assessment reports Vulnerability assessment tools
Reporting format	Aggregated score values for homogeneous or sensitive systems (external/internal networks, Unix systems, etc.)

Relationship ISO/IEC 27001:2013, A.12.6.1: Management of technical vulnerabilities

B.31 Security in third party agreements – A

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate the degree to which security is addressed in third party agreements
Measure	Average percent of relevant security requirements addressed in third party agreements
Formula/scoring	[Sum of (for each agreement (number of required requirements - number of addressed requirements))/number of agreements] * 100
Target	100%
Implementation evidence	Supplier database, supplier agreement records
Frequency	Collect: quarterly Report: semi-annually
Responsible Parties	Information owner: Contract office Information collector: Security staff Measurement client: Security manager, Business managers
Data source	Supplier database, supplier agreement records
Format	Line chart depicting a trend over multiple reporting periods; short summary of findings and possible management actions

Relationship ISO/IEC 27001:2013, A.15.1.2: Addressing security within supplier agreements

NOTE This assumes that all security requirements are equal, whereas in practice this is not usually the case. An average can therefore hide significant variations and thereby present a false sense of security. Likewise, the requirements that an organization places on its suppliers, and its suppliers' ability to meet them, are likely to differ. This implies that suppliers should not all be measured in the same way. The supplier database should ideally include a security rating or category to ensure more accurate and meaningful measurement.

B.32 Security in third party agreements – B

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To evaluate the degree to which security is addressed in third party agreements of personal information processing
Measure	Average percent of relevant security requirements addressed in third party agreements
Formula/scoring	Identify number of security requirements that have to be addressed in each agreement per policy (availability, ratio, response time, help desk level, maintenance level etc.) Sum of (for each agreement (number of required requirements - number of addressed requirements))/number of agreements 1 Average ratio of difference of standard requirements to addressed requirements: Sum of (for each agreement ([Security requirements addressed total] – [Standard security requirements total.]))/[Number of third party agreements] 2 Trend of the ratio: Compare with previous indicator 1
Target	1 Indicator 1 should be greater than 0.9 2 Indicator 2 should be stable or upward
Implementation evidence	Identify number of security requirements that have to be addressed in each agreement per policy
Frequency	Collect: Monthly Analysis: Quarterly Report: Quarterly Measurement revision: 2 years Period of measurement: Applicable 2 years
Responsible parties	Information owner: Contract office Information collector: Security staff Measurement client: Managers responsible for an ISMS, Security manager
Data source	Third party agreements
Reporting format	Line chart depicting a trend over multiple reporting periods. Short summary of findings and possible management actions.

Relationship ISO/IEC 27001:2013, A.15.1.2: Addressing security within supplier agreements

B.33 Information security incident management effectiveness

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Assess the effectiveness of Information security incident management
Measure	Incidents not resolved in target timeframe
Formula/scoring	a) Define security incident categories and target time frames in which security incidents should be resolved for each security incident category b) Define indicator thresholds for security incidents exceeding category given target timeframes c) Compare the number of incidents which resolving time exceeds the category target time frames and compare their count with the indicator thresholds
Target	Incidents exceeding category target time frames within defined green threshold
Implementation evidence	Target indicators get reported monthly
Frequency	Collect: Monthly Analysis: Monthly Report: Monthly Measurement revision: Six months Period of measurement: Monthly
Responsible parties	Information owner: Managers responsible for an ISMS Information collector: Incident management manager Measurement client: ISMS management committee; Managers responsible for an ISMS; Security management; Incident management
Data source	ISMS; individual incident; incident report; incident management tool
Reporting format	Monthly target indicator values in table and trend diagram format

Relationship ISO/IEC 27001:2013, A.16: Information security incident management

B.34 Security incidents trend

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	1. Trend of information security incidents 2. Trend of categories of information security incidents
Measure	1. Number of information security incidents in a defined timeframe (e.g., month) 2. Number of information security incidents of a specific category in a defined timeframe (e.g., month)
Formula/scoring	Compare average measure value for the last two timeframes with the average measurement value of the last 6 timeframes Define threshold values for trend indicators, e.g., <1.0 equals Green 1.00 – 1.30 equals Yellow >1.3 equals Red 1. Perform analysis for all incidents 2. Perform analysis for each specific category
Target	Green
Implementation evidence	Indicator values are reported monthly
Frequency	Monthly
Responsible parties	Information owner: Computer security incident response team (CSIRT) Information collector: Computer security incident response team (CSIRT) Information customer: Chief information officer, Chief information security officer
Data source	Information security incident reports
Reporting format	Table with indicator values Trend diagram

Relationship — ISO/IEC 27001:2013, A.16.1: Management of information security incidents and improvements

B.35 Security event reporting

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Measure whether security events are reported and formally treated.
Measure	Sum of security events reported to the Computer security incident response team (CSIRT) in relation to the size of the organization
Formula/scoring	Sum of security events that have been reported and formally treated to CSIRT/ Number of security roles defined by the organization
Target	At least one security event per security role per year
Implementation evidence	Ticketing system used for treating security events
Frequency	Collect: Yearly Report: Yearly
Responsible parties	Information owner: Computer security incident response team (CSIRT) Information collector: Information security manager Information customer: Information security manager, top management
Data source	Incident reports
Reporting format	Trend line showing the evolution of reported events over last periods

Relationship ISO/IEC 27001:2013, A.16.1.3: Reporting information security weaknesses

B.36 ISMS review process

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	To assess the degree of accomplishment of independent review of information security
Measure	Progress ratio of accomplished independent reviews
Formula/scoring	Divide [Number of conducted reviews by third party] by [Total number of planned third party reviews]
Target	Resulting ratio of indicator should fall primarily between 0.8 and 1.1 to conclude the achievement of the control objective and no action. And it should be over 0.6 if it fails to meet the primary condition.
Implementation evidence	1 Count number of report of conducted regular reviews by third party 2. Count total number of planned third party reviews
Frequency	Collect: Quarterly Analysis: Quarterly Report: Quarterly Measurement Revision: Review and update every 2 years Period of Measurement: Applicable 2 years
Responsible parties	Information owner: Managers responsible for an ISMS Information collector: Internal audit; Quality manager Measurement client: Managers responsible for an ISMS, Quality system manager
Data source	1. Reports of third party reviews 2. Plans of third party reviews
Reporting format	Bar graph depicting compliance over several reporting periods in relation to the thresholds defined by target

Relationship ISO/IEC 27001:2013, A.18.2.1: Independent review of information security

B.37 Vulnerability coverage

Information descriptor	Meaning or purpose
Measure ID	Organization-defined
Information need	Evaluate the current visibility on organization's systems vulnerabilities
Measure	Ratio of systems which have been object of vulnerability assessment/penetration testing activities
Formula/scoring	Number of systems object of a vulnerability assessment in the last quarter or of a penetration test in the last year / total systems
Target	1
Implementation evidence	Analysis on vulnerability assessment and penetration testing activities
Frequency	Quarterly
Responsible parties	Information owner: information security analysts or contracted third parties Information collector: information security analysts Information customer: information security manager
Data source	Vulnerability assessment reports Vulnerability assessment tools Penetration test reports
Reporting format	Aggregate pie chart and homogeneous or sensitive systems arrays-wide pie chart showing the obtained ratios

Relationship ISO/IEC 27001:2013, A.18.2.3: Technical compliance review

Annex C
(informative)

An example of free-text form measurement construction

C.1 'Training effectiveness' – effectiveness measurement construct

In this example a 'free text' approach is taken to determine whether formalized training is a better way to convey information security objectives than just making the policy available online.

Assume all members of staff (S1) are required to read the online version of the organization's information security policy as a part of their terms of employment (contract).

At any time, S2 = total number of staff who have acknowledged reading the policy online (i.e. they have gone online and at least scrolled-through to the end of the text).

S3 = number of employees who have attended specific information security policy awareness training. (S3 will always be a sub-set of S2, since the course will require their prior online reading of the policy).

All staff who have at least read the policy are required to take an online test, including those who have attended the formal training.

$S4_P$ = number of staff who have taken the test after only reading the intranet policy and who achieve the pass mark.

$S4_F$ = number of people who have taken the test after only reading the intranet policy and who fail to achieve the pass mark.

$S5_P$ = number of people who have taken the same test after attending the formal training and who achieve the pass mark.

$S5_F$ = number of people who have taken the same test after attending the training and who fail to achieve the pass mark.

E1=S1 - S2, the number of staff yet to have any exposure to the information security policy.

E2= $S4_P$ / ($S4_P$ + $S4_F$), i.e. the proportion of staff who have only read the policy and who have a good comprehension of it (that being determined by the pass threshold).

E3= S5P / (S5P + S5F), as above, for S5, but for those staff who have attended the formal training.

E4 = E3/E2, i.e. the effectiveness ratio of training versus plain self-instruction.

S1 - S2 is also a useful measure, indicating how many staff members have yet to read the online policy. This can have a threshold which triggers something an alert when either (or both) of a proportion of total numbers of staff is exceeded, but can also accommodate a duration within which the online policy must be read, in that there has to be a practical period of time from when an employee begins and their initial introductory actions are to be completed.

One can imagine that over time, as the information security awareness and culture advance, the threshold might be raised as trends are identified, as can analysis of questions failed, which might lead to more effective expression of the policy, or the setting of more realistic goals.

Bibliography

[1] ISO/TR 10017, *Guidance on statistical techniques for ISO 9001:2000*

[2] ISO/IEC 15939, *Systems and software engineering – Measurement process*

[3] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[4] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[5] NIST Special Publication 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

ICS 03.100.70; 35.030

Price based on 58 pages

This page deliberately left blank

British Standards Institution (BSI)

BSI is the national body responsible for preparing British Standards and other standards-related publications, information and services.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

About us

We bring together business, industry, government, consumers, innovators and others to shape their combined experience and expertise into standards -based solutions.

The knowledge embodied in our standards has been carefully assembled in a dependable format and refined through our open consultation process. Organizations of all sizes and across all sectors choose standards to help them achieve their goals.

Information on standards

We can provide you with the knowledge that your organization needs to succeed. Find out more about British Standards by visiting our website at bsigroup.com/standards or contacting our Customer Services team or Knowledge Centre.

Buying standards

You can buy and download PDF versions of BSI publications, including British and adopted European and international standards, through our website at bsigroup.com/shop, where hard copies can also be purchased.

If you need international and foreign standards from other Standards Development Organizations, hard copies can be ordered from our Customer Services team.

Copyright in BSI publications

All the content in BSI publications, including British Standards, is the property of and copyrighted by BSI or some person or entity that owns copyright in the information used (such as the international standardization bodies) and has formally licensed such information to BSI for commercial publication and use.

Save for the provisions below, you may not transfer, share or disseminate any portion of the standard to any other person. You may not adapt, distribute, commercially exploit, or publicly display the standard or any portion thereof in any manner whatsoever without BSI's prior written consent.

Storing and using standards

Standards purchased in soft copy format:

- A British Standard purchased in soft copy format is licensed to a sole named user for personal or internal company use only.
- The standard may be stored on more than 1 device provided that it is accessible by the sole named user only and that only 1 copy is accessed at any one time.
- A single paper copy may be printed for personal or internal company use only.

Standards purchased in hard copy format:

- A British Standard purchased in hard copy format is for personal or internal company use only.
- It may not be further reproduced – in any format – to create an additional copy. This includes scanning of the document.

If you need more than 1 copy of the document, or if you wish to share the document on an internal network, you can save money by choosing a subscription product (see 'Subscriptions').

Reproducing extracts

For permission to reproduce content from BSI publications contact the BSI Copyright & Licensing team.

Subscriptions

Our range of subscription services are designed to make using standards easier for you. For further information on our subscription products go to bsigroup.com/subscriptions.

With **British Standards Online (BSOL)** you'll have instant access to over 55,000 British and adopted European and international standards from your desktop. It's available 24/7 and is refreshed daily so you'll always be up to date.

You can keep in touch with standards developments and receive substantial discounts on the purchase price of standards, both in single copy and subscription format, by becoming a **BSI Subscribing Member**.

PLUS is an updating service exclusive to BSI Subscribing Members. You will automatically receive the latest hard copy of your standards when they're revised or replaced.

To find out more about becoming a BSI Subscribing Member and the benefits of membership, please visit bsigroup.com/shop.

With a **Multi-User Network Licence (MUNL)** you are able to host standards publications on your intranet. Licences can cover as few or as many users as you wish. With updates supplied as soon as they're available, you can be sure your documentation is current. For further information, email subscriptions@bsigroup.com.

Revisions

Our British Standards and other publications are updated by amendment or revision.

We continually improve the quality of our products and services to benefit your business. If you find an inaccuracy or ambiguity within a British Standard or other BSI publication please inform the Knowledge Centre.

Useful Contacts

Customer Services
Tel: +44 345 086 9001
Email (orders): orders@bsigroup.com
Email (enquiries): cservices@bsigroup.com

Subscriptions
Tel: +44 345 086 9001
Email: subscriptions@bsigroup.com

Knowledge Centre
Tel: +44 20 8996 7004
Email: knowledgecentre@bsigroup.com

Copyright & Licensing
Tel: +44 20 8996 7070
Email: copyright@bsigroup.com

BSI Group Headquarters

389 Chiswick High Road London W4 4AL UK

bsi.