INTERNATIONAL STANDARD

ISO/IEC 27004

First edition
2009-12-15

Information technology — Security techniques — Information security management — Measurement

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Mesurage

Reference number
ISO/IEC 27004:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27004 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

0 Introduction

0.1 General

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls need to be changed or improved. It needs to be kept in mind that no measurement of controls can guarantee complete security.

The implementation of this approach constitutes an Information Security Measurement Programme. The Information Security Measurement Programme will assist management in identifying and evaluating non-compliant and ineffective ISMS processes and controls and prioritizing actions associated with improvement or changing these processes and/or controls. It may also assist the organization in demonstrating ISO/IEC 27001 compliance and provide additional evidence for management review and information security risk management processes.

This International Standard assumes that the starting point for the development of measures and measurement is a sound understanding of the information security risks that an organization faces, and that an organization's risk assessment activities have been performed correctly (i.e. based on ISO/IEC 27005), as required by ISO/IEC 27001. The Information Security Measurement Programme will encourage an organization to provide reliable information to relevant stakeholders concerning its information security risks and the status of the implemented ISMS to manage these risks.

Effectively implemented, the Information Security Measurement Programme would improve stakeholder confidence in measurement results, and enable the stakeholders to use these measures to effect continual improvement of information security and the ISMS.

The accumulated measurement results will allow comparison of progress in achieving information security objectives over a period of time as part of an organization's ISMS continual improvement process.

0.2 Management overview

ISO/IEC 27001 requires the organization to "undertake regular reviews of the effectiveness of the ISMS taking into account results from effectiveness measurement" and to "measure the effectiveness of controls to verify that security requirements have been met". ISO/IEC 27001 also requires the organization to "define how to measure the effectiveness of the selected controls or groups of controls and specify how these measures are to be used to assess control effectiveness to produce comparable and reproducible results".

The approach adopted by an organization to fulfil the measurement requirements specified in ISO/IEC 27001 will vary based on a number of significant factors, including the information security risks that the organization faces, its organizational size, resources available, and applicable legal, regulatory and contractual requirements. Careful selection and justification of the method used to fulfil the measurement requirements are important to ensure that excessive resources are not devoted to these activities of the ISMS to the detriment of others. Ideally, ongoing measurement activities are to be integrated into the regular operations of the organization with minimal additional resource requirements.

This International Standard gives recommendations concerning the following activities as a basis for an organization to fulfil measurement requirements specified in ISO/IEC 27001:

a) developing measures (i.e. base measures, derived measures and indicators);

b) implementing and operating an Information Security Measurement Programme;
c) collecting and analysing data;
d) developing measurement results;
e) communicating developed measurement results to the relevant stakeholders;
f) using measurement results as contributing factors to ISMS-related decisions;
g) using measurement results to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
h) facilitating continual improvement of the Information Security Measurement Programme.

One of the factors that will impact the organization's ability to achieve measurement is its size. Generally the size and complexity of the business in combination with the importance of information security affect the extent of measurement needed, both in terms of the numbers of measures to be selected and the frequency of collecting and analysing data. For SMEs (Small and Medium Enterprises) a less comprehensive information security measurement program will be sufficient, whereas large enterprises will implement and operate multiple Information Security Measurement Programmes.

A single Information Security Measurement Programme may be sufficient for small organizations, whereas for large enterprises the need may exist for multiple Information Security Measurement Programmes.

The guidance provided by this International Standard will result in the production of documentation that will contribute to demonstrating that control effectiveness is being measured and assessed.

Information technology — Security techniques — Information security management — Measurement

1 Scope

This International Standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

This International Standard is applicable to all types and sizes of organization.

NOTE This document uses the verbal forms for the expression of provisions (e.g. "shall", "shall not", "should", "should not", "may", "need not", "can" and "cannot") that are specified in the ISO/IEC Directives, Part 2, 2004, Annex H. See also ISO/IEC 27000:2009, Annex A.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000 and the following apply.

3.1
analytical model
algorithm or calculation combining one or more base and/or derived measures with associated decision criteria

[ISO/IEC 15939:2007]

3.2
attribute
property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

[ISO/IEC 15939:2007]

3.3
base measure
measure defined in terms of an attribute and the method for quantifying it

[ISO/IEC 15939:2007]

NOTE A base measure is functionally independent of other measures.

3.4
data
collection of values assigned to base measures, derived measures and/or indicators

[ISO/IEC 15939:2007]

3.5
decision criteria
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result

[ISO/IEC 15939:2007]

3.6
derived measure
measure that is defined as a function of two or more values of base measures

[ISO/IEC 15939:2007]

3.7
indicator
measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs

3.8
information need
insight necessary to manage objectives, goals, risks and problems

[ISO/IEC 15939:2007]

3.9
measure
variable to which a value is assigned as the result of measurement

[ISO/IEC 15939:2007]

NOTE The term “measures” is used to refer collectively to base measures, derived measures, and indicators.

EXAMPLE A comparison of a measured defect rate to planned defect rate along with an assessment of whether or not the difference indicates a problem.

3.10
measurement
process of obtaining information about the effectiveness of ISMS and controls using a measurement method, a measurement function, an analytical model, and decision criteria

3.11
measurement function
algorithm or calculation performed to combine two or more base measures

[ISO/IEC 15939:2007]

3.12
measurement method
logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale

[ISO/IEC 15939:2007]

NOTE The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

— subjective: quantification involving human judgment;
— objective: quantification based on numerical rules.

3.13
measurement results
one or more indicators and their associated interpretations that address an information need

3.14
object
item characterized through the measurement of its attributes

3.15
scale
ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped

[ISO/IEC 15939:2007]

NOTE The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined:

— nominal: the measurement values are categorical;
— ordinal: the measurement values are rankings;
— interval: the measurement values have equal distances corresponding to equal quantities of the attribute;
— ratio: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

3.16
unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity

[ISO/IEC 15939:2007]

3.17
validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

3.18
verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

[ISO 9000:2005]

NOTE This could also be called compliance testing.

4 Structure of this International Standard

This International Standard provides an explanation of measures and measurement activities needed to assess the effectiveness of ISMS requirements for the management of adequate and proportionate security controls as required in ISO/IEC 27001:2005, 4.2.

This International Standard is structured as follows:

- Overview on the Information Security Measurement Programme and the Information Security Measurement Model (Clause 5);
- Management responsibilities for information security measurements (Clause 6); and
- Measurement constructs and the processes (i.e. planning and developing, implementing and operating, and improving measurements: communicating measurement results) to be implemented in the Information Security Measurement Programme (Clauses 7-10).

In addition, Annex A provides an example template for the measurement construct of which the constituents are the elements of the Information Security Measurement Model (see Clause 7). Annex B provides the measurement construct examples for specific controls or processes of an ISMS, using the template provided in Annex A.

These examples are intended to help an organization on how to implement the Information Security Measurement and how to record measurement activities and outcomes from them.

5 Information security measurement overview

5.1 Objectives of information security measurement

The objectives of information security measurement in the context of an ISMS includes:

a) evaluating the effectiveness of the implemented controls or groups of controls (See “4.2.2 d)” in Figure 1);
b) evaluating the effectiveness of the implemented ISMS (See “4.2.3 b)” in Figure 1);
c) verifying the extent to which identified security requirements have been met (See “4.2.3 c)” in Figure 1);
d) facilitating performance improvement of information security in terms of the organization’s overall business risks;
e) providing input for management review to facilitate ISMS-related decision making and justify needed improvements of the implemented ISMS.

Figure 1 illustrates the cyclical input–output relationship of the measurement activities in relation to the Plan-Do-Check-Act (PDCA) cycle, specified in ISO/IEC 27001. Numbers in each figure represent relevant sub-clauses of ISO/IEC 27001:2005.

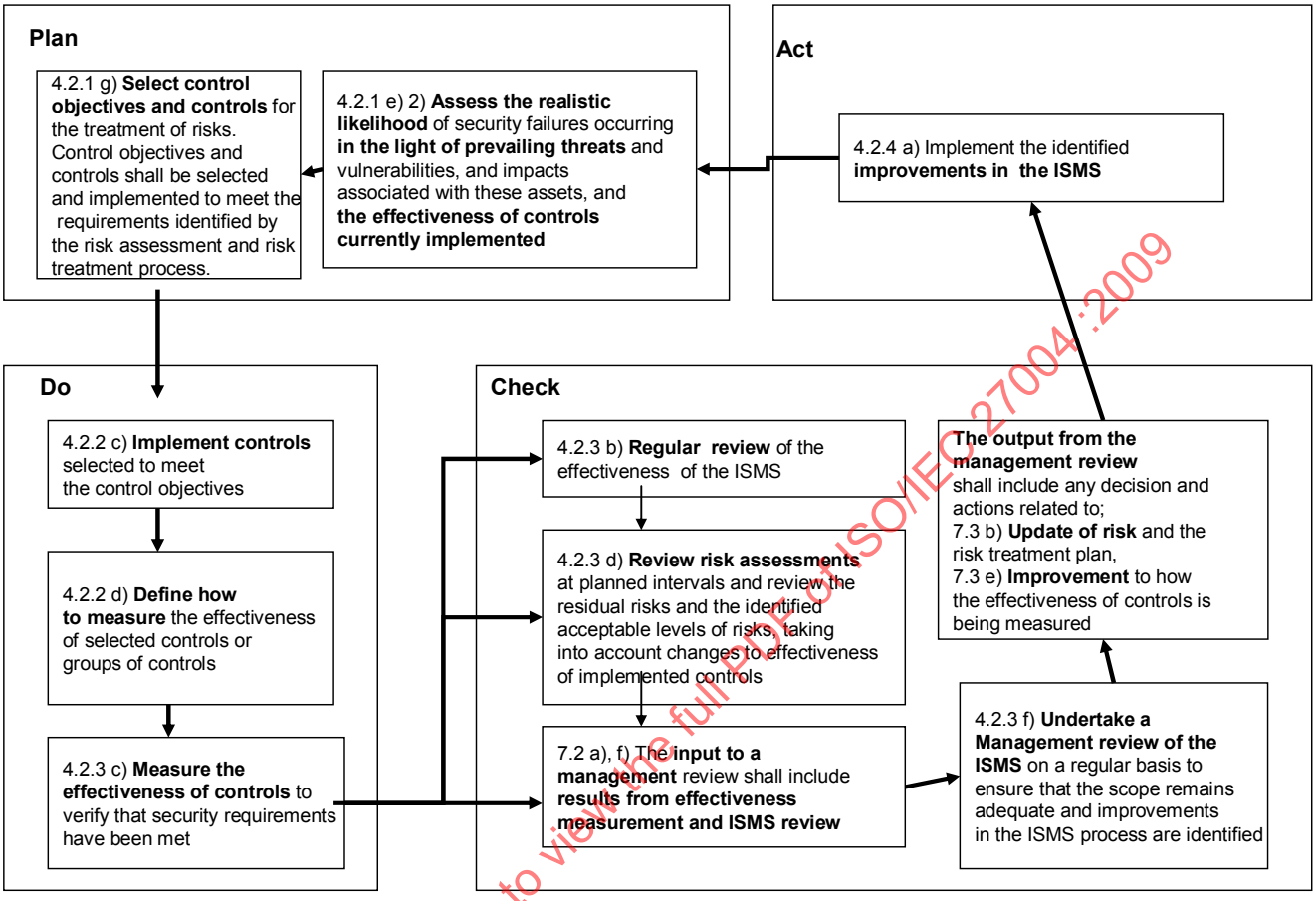


Figure 1 — Measurement inputs and outputs in ISMS PDCA cycle of information security management

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

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

5.2 Information Security Measurement Programme

An organization should establish and manage an Information Security Measurement Programme in order to achieve the established measurement objectives and adopt the PDCA model within the organization's overall measurement activities. An organization should also develop and implement measurement constructs in order to obtain repeatable, objective and useful results of measurement based on the Information Security Measurement Model (see 5.4).

The Information Security Measurement Programme and the developed measurement construct should ensure that an organization effectively achieves objective and repeatable measurement and provides measurement results for relevant stakeholders to identify needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

An Information Security Measurement Programme should include the following processes:

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

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

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

5.3 Success factors

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

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

Once successfully implemented, an Information Security Measurement Programme can:

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

5.4 Information security measurement model

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

5.4.1 Overview

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

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

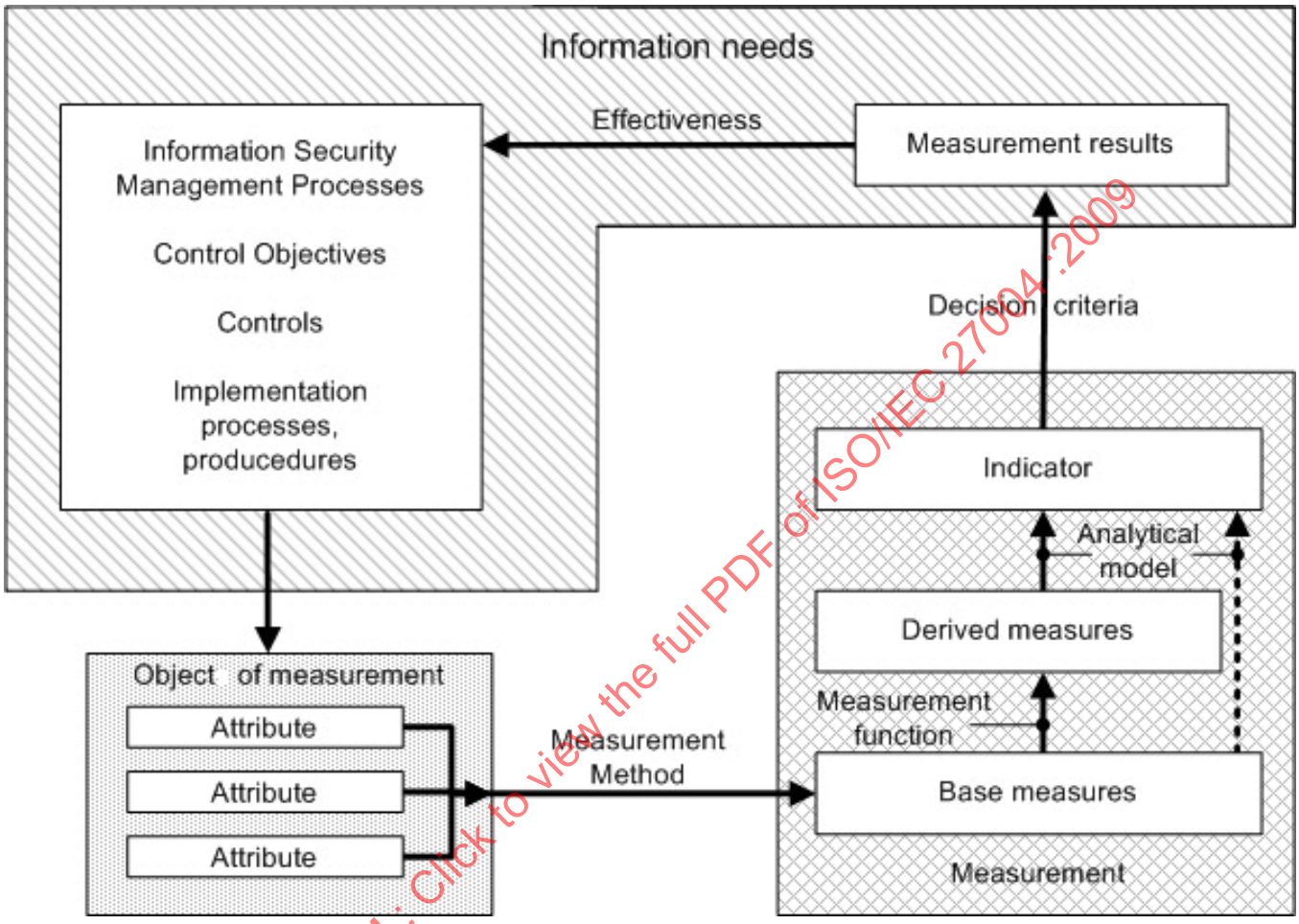


Figure 2 — Information security measurement model

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

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

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

5.4.2 Base measure and measurement method

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

A measurement method is a logical sequence of operations used in quantifying an attribute with respect to a specified scale. The operation may involve activities such as counting occurrences or observing the passage of time.

A measurement method can apply attributes to an object of measurement. Examples of an object of measurement include but are not limited to:

- Performance of controls implemented in the ISMS;
- Status of information assets protected by the controls;
- Performance of processes implemented in the ISMS;
- Behaviour of personnel who are responsible to the implemented ISMS;
- Activities of organizational units responsible for information security; and
- Extent of satisfaction of interested parties.

A measurement method may use measurement objects of measurement and attributes from a variety of sources, such as:

- Risk analysis and risk assessment results;
- Questionnaires and personal interviews;
- Internal and/or external audits reports;
- Records of events, such as logs, report statistics, and audit trails;
- Incident reports, particularly those that result in the occurrence of an impact;
- Test results, e.g. from penetration testing, social engineering, compliance tools, and security audit tools; or
- Records from the organization's information security related procedures and programmes, eg. information security awareness training results.

Tables 1-4 below present the application of the information security model for the following controls:

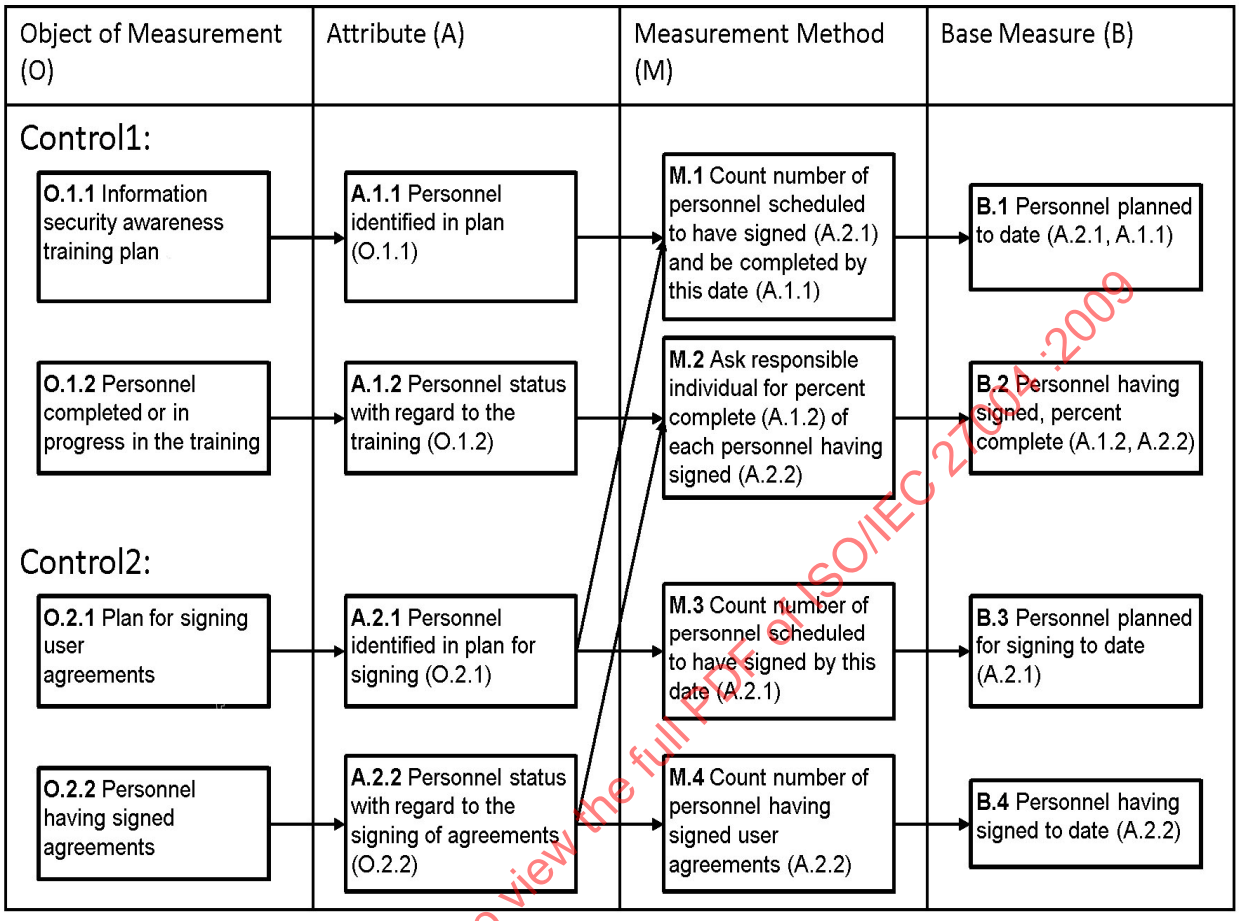
- "Control 2" refers to control A.8.2.1 Management responsibility of ISO/IEC 27001:2005 ("Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization"); being implemented as follows: "All personnel relevant to the ISMS must sign user agreements before being granted access to an information system";
- "Control 1" refers to control A.8.2.2 "Information security awareness, education and training" of ISO/IEC 27001:2005 ("All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function"); being implemented as follows: "All personnel relevant to the ISMS must receive information security awareness training before being granted access to an information system".

The corresponding measurement constructs are contained in B.1.

NOTE Table 1-4 consists of various columns (Table 1, four columns; Table 2-4, three columns) of which are assigned a letter designator. Each box within individual columns is assigned a number designator. The combinations of letter and number designators are used in subsequent boxes to refer to previous boxes. Arrows designate the data flows between individual elements of the information security measurement model within the specific example.

Table 1 includes an example of the relationships between object of measurement, attribute, measurement method and base measure for measuring the objects established for implemented controls described above.

Table 1 — Example of base measure and measurement method



5.4.3 Derived measure and measurement function

A derived measure is an aggregate of two or more base measures. A given base measure may serve as input for several derived measures.

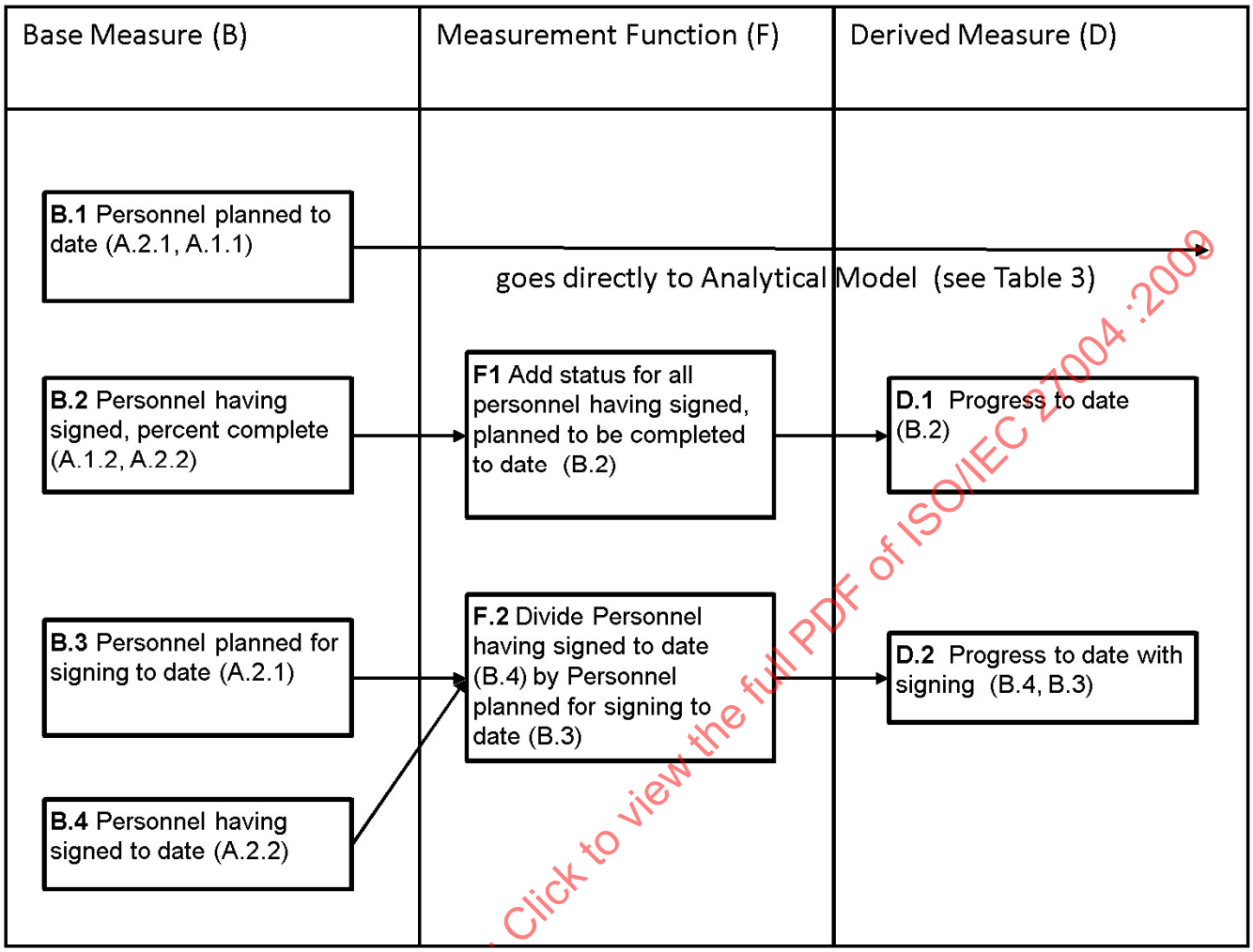
A measurement function is a calculation used to combine base measures together to create a derived measure.

The scale and unit of the derived measure depends on the scales and units of the base measures from which it is composed as well as how they are combined by the measurement function.

The measurement function may involve a variety of techniques, such as averaging base measures, applying weights to base measures, or assigning qualitative values to base measures. The measurement function may combine base measures using different scales, such as percentages and qualitative assessment results.

An example of the relationship of further elements of the information security measurement model application i.e. base measure, measurement function and derived measure is presented in Table 2.

Table 2 — Example of derived measure and measurement function

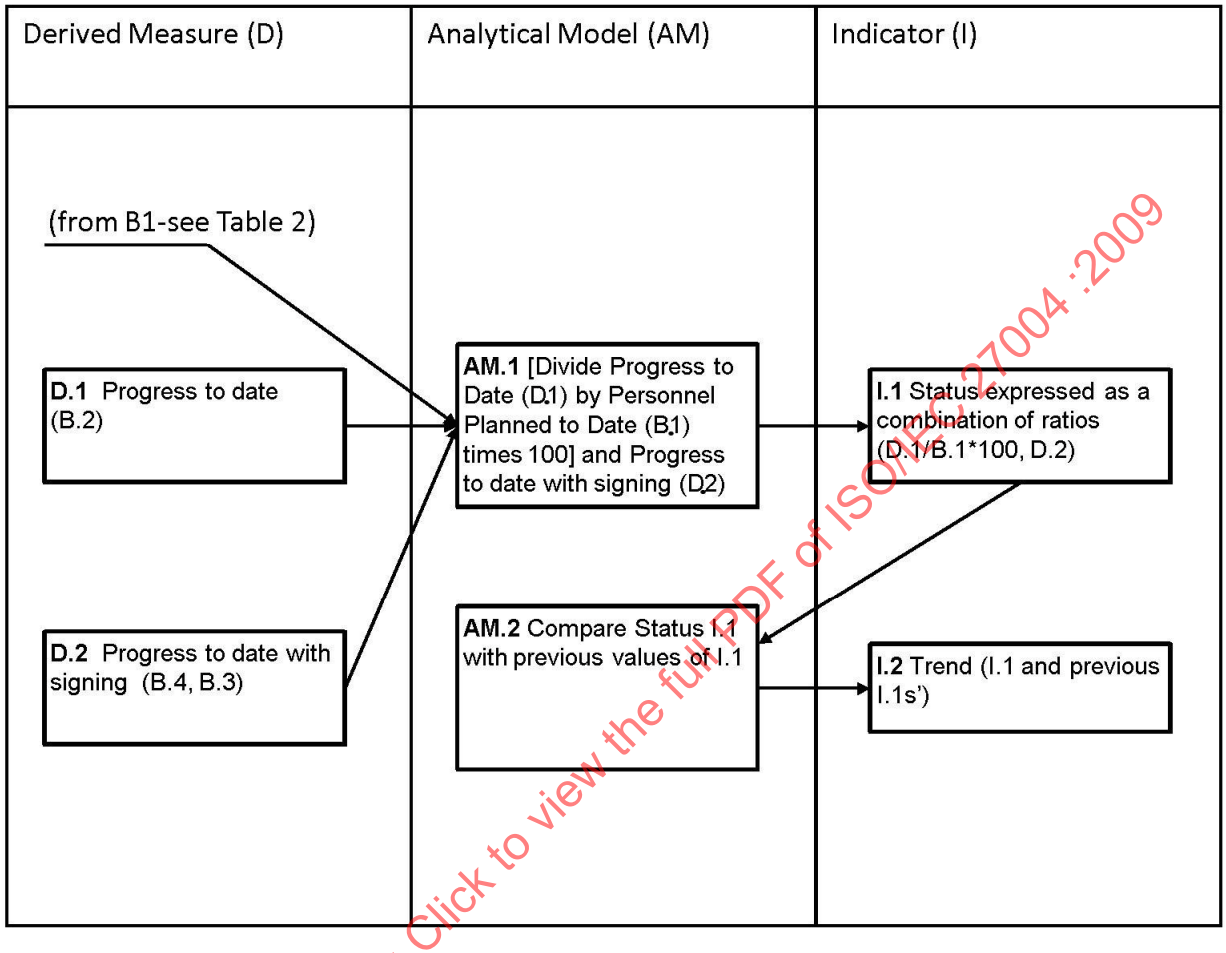


5.4.4 Indicators and analytical model

An indicator is a measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information need. Indicators are obtained by applying an analytical model to a base and/or a derived measure and combining them with decision criteria. The scale and measurement method affect the choice of analytical techniques used to produce indicators.

An example of the relationships between derived measures, analytical model and indicators for the information security measurement model application is presented in Table 3.

Table 3 — Example of indicator and analytical model



NOTE If an indicator is represented in a graphical form, it should be usable by visually impaired users or when monochrome copies are used. To make that possible the indicator description should include colors, shading, fonts or other visual methods

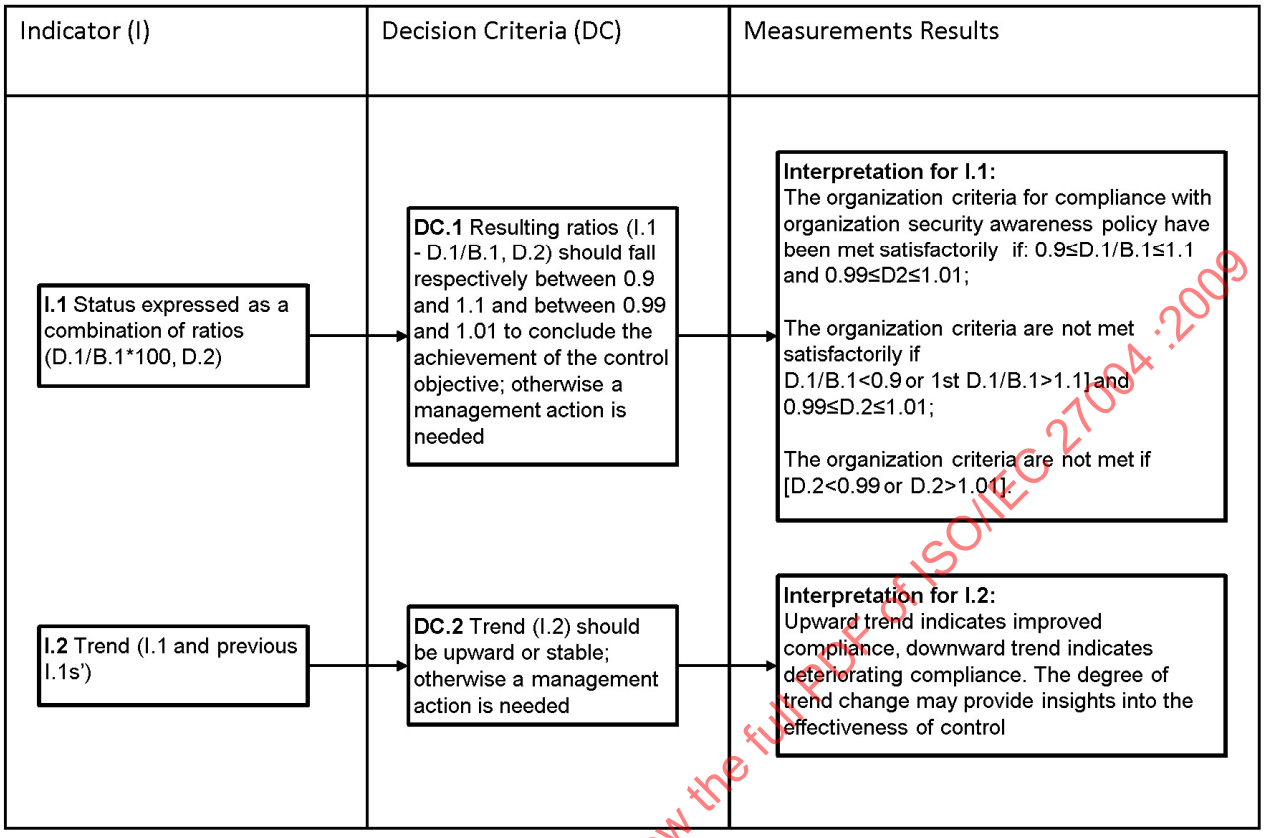
5.4.5 Measurement results and decision criteria

Measurement results are developed with interpreting applicable indicators based on defined decision criteria and should be considered in the context of the overall measurement objectives of assessing the ISMS effectiveness. Decision criteria is used to determine the need for action or further investigation, as well as to describe the level of confidence in measurement results. Decision criteria may be applied to a series of indicators, for example to conduct trend analysis based on indicators received at different point in time.

Targets provide detailed performance specifications, applicable to the organization or parts thereof, derived from the information security objectives such as the ISMS objectives and control objectives, and that need to be set and met in order to achieve those objectives.

An example of the relationship of final elements of the information security measurement model application (i.e. indicator, decision criteria and measurement results) is presented in Table 4.

Table 4 — Example of measurement results and analytical model



6 Management responsibilities

6.1 Overview

Management is responsible for establishing the Information Security Measurement Programme, involving relevant stakeholders (see 7.5.8) in the measurement activities, accepting measurement results as an input into management review and using measurement result in improvement activities within the ISMS.

To achieve this, management should:

a) Establish objectives for the Information Security Measurement Programme;
b) Establish a policy for the Information Security Measurement Programme;
c) Establish roles and responsibilities for the Information Security Measurement Programme;
d) Provide adequate resources to perform measurement including personnel, funding, tools and infrastructure;
e) Ensure that the objectives of the Information Security Measurement Programme are achieved;
f) Ensure that tools and equipment used to collect data are maintained properly;
g) Establish the purpose of measurement for each measurement construct;
h) Ensure that measurement provides sufficient information to relevant stakeholders with regard to effectiveness of the ISMS and needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and
i) Ensure that measurement provides sufficient information to relevant stakeholders with regard to effectiveness of controls or group of controls and needs for improving the implemented controls.

Through the appropriate assignment of measurement roles and responsibilities, management should ensure measurement results are not influenced by information owners (see 7.5.8). This may be achieved through segregation of duties or, if this is not possible, through the use of detailed documentation that allows

independent checks.

6.2 Resource management

Management should assign and provide resources to support essential activities of measurement, such as data collection, analysis, storage, reporting, and distribution. Resource allocations should include the assignment of:

a) Individuals with responsibility for all aspects of Information Security Measurement Programme;
b) Appropriate financial support; and
c) Appropriate infrastructure support, such as physical infrastructure and tools used to perform the measurement process.

NOTE Clause 5.2.1 of ISO/IEC 27001:2005 specifies requirement on the provision of resources for implementation and operation of an ISMS.

6.3 Measurement training, awareness, and competence

Management should ensure that:

a) The stakeholders (see 7.5.8) are trained adequately for achieving their roles and responsibilities in the implemented Information Security Measurement Programme, and appropriately qualified to perform their roles and responsibilities; and
b) The stakeholders understand that their duties include making suggestions for improvements in the implemented Information Security Measurement Programme.

7 Measures and measurement development

7.1 Overview

This clause provides guidance on how to develop measures and measurement for the purpose of assessing the effectiveness of the implemented ISMS and controls or group of controls, and identifying organisation-specific sets of measurement constructs. Activities needed to develop measures and measurement should be established and documented, including the following:

a) Defining the measurement scope (see 7.2);
b) Identifying an information need (see 7.3);
c) Selecting the object of measurement and its attributes (see 7.4) ;
d) Developing measurement constructs (see 7.5);
e) Applying measurement constructs (see 7.6);
f) Establishing data collection and analysis processes and tools (see 7.7), and
g) Establishing measurement implementation approach and documentation (see 7.8).

When establishing these activities, the organization should take into account financial, human, and infrastructure (physical and tools) resources.

7.2 Definition of measurement scope

Depending on an organization's capabilities and resources, the initial scope of an organization's measurement activities will be limited to such elements as specific controls, information assets protected by specific controls, specific activities for information security that are given highest priority by management. Over time, the scope of measurement activities will be widened to address further elements of the implemented ISMS and controls or group of controls, taking into account stakeholders' priorities.

Relevant stakeholders should be identified and should participate in defining the measurement scope. The relevant stakeholders may be internal or external to the organizational units, such as project managers, information system managers, or information security decision makers. Specific measurement results addressing the effectiveness of individual controls or group of controls should be defined and communicated to relevant stakeholders.

The organization may consider limiting the number of measurement results to be reported to decision-makers within a given time period to ensure their ability to effect improvement of the ISMS based on the reported measurement results. An excessive number of reported measurement results will impact the ability of the decision-maker to focus efforts and prioritize future improvement activities. Measurement results should be prioritized based on the importance of corresponding information needs and associated ISMS objectives.

NOTE The measurement scope is related to the scope of the ISMS established in accordance with 4.2.1 a) of ISO/IEC 27001:2005.

7.3 Identification of information need

Each measurement construct should correspond to, at least, one information need. An example of the information need, describing in starting point as the purpose of measurement and ending with relevant decision criteria is presented in Annex A.

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

a) Examine the ISMS and its processes, such as:
   1) ISMS policy and objectives, control objectives and controls;
   2) Legal, regulatory, contractual and organizational requirements for information security;
   3) The information security risk management process outcomes as described in ISO/IEC 27001.

b) Prioritize the identified information needs based on criteria, such as:
   1) Risk treatment priorities;
   2) An organization's capabilities and resources;
   3) Stakeholders' interests;
   4) The information security policy;
   5) Information required to meet legal, regulatory, and contractual requirements;
   6) The value of the information in relation to the cost of measurement;

c) Select a subset of information required to be addressed in measurement activities from the prioritized list; and

d) Document and communicate the selected information needs to all relevant stakeholders.

All relevant measures applied to an implemented ISMS, controls or groups of controls should be implemented based on the selected information needs.

7.4 Object and attribute selection

An object of measurement and its attributes should be identified in the overall context and scope of an ISMS. It should be noted that an object of measurement can have several applicable attributes.

The object and its attributes to be used by measurement should be selected based on the priority of a corresponding information needs.

The values to be assigned to a relevant base measure are obtained by applying an appropriate measurement method to the selected attributes. This selection should also ensure that:

- Relevant base measure and an appropriate measurement method can be identified; and
- Meaningful measurement results can be developed based on the obtained values and developed measures.

Characteristics of selected attributes determine which type of a measurement method needs to be used to obtain values to be assigned to base measures (e.g. qualitative or quantitative).

The selected object and attributes should be documented, along with the rationale for the selection.

Data describing the object of measurement and corresponding attributes should be used as the values to be assigned to base measures. Examples of objects of measurement include but are not limited to:

- Products and services;
- Processes;

- Applicable assets such as facilities, applications, and information systems as identified in ISO/IEC 27001:2005 (Inventory of assets, A.7.1.1);
- Business units;
- Geographic locations; and
- Third party services.

Attributes should be reviewed to ensure that:
a) Appropriate attributes have been selected for measurement; and
b) Data collection has been defined to ensure a sufficient number of attributes is present to allow for effective measurement.

Only attributes that are relevant to the corresponding base measure should be selected. Although the selection of attributes should take into consideration the degree of difficulty in obtaining the attributes to measure, it should not be made solely upon data being easily obtainable or the attribute being easy to measure.

7.5 Measurement construct development

7.5.1 Overview

This sub-clause (7.5) addresses measurement construct development from 7.5.2 (measure selection) to 7.5.8 (stakeholders).

7.5.2 Measure selection

Measures that could potentially satisfy the selected information need should be identified. The identified measures should be defined in sufficient detail to allow for selection of measures to be implemented. Newly identified measures may involve an adaptation of an existing measure.

NOTE Identification of base measures is closely related with identification of objects of measurement and their attributes.

The identified measures that could potentially satisfy the selected information need should be selected. Context information necessary to interpret or normalize measures also should be considered.

NOTE Many different combinations of measures (i.e. base measures, derived measures, and indicators) may be selected to address a specific information need.

The selected measures should reflect the priority of the information needs. Further example criteria that may be used for the selection of measures include:

- Ease of data collection;
- Availability of human resources to collect and manage data;
- Availability of appropriate tools;
- Number of potentially relevant indicators supported by the base measure;
- Ease of interpretation;
- Number of users of developed measurement results;
- Evidence as to the measure's fitness for purpose or information need; and
- Costs of collecting, managing, and analysing the data.

7.5.3 Measurement method

For each individual base measure a measurement method should be defined. This measurement method is used to quantify an object of measurement through transforming the attributes into the value to be assigned to the base measure.

A measurement method may be subjective or objective. Subjective methods rely on quantification involving human judgment, while objective methods use quantification based on numerical rules such as counting which may be implemented via human or automated means.

The measurement method quantifies the attributes as values by applying an appropriate scale. Each scale uses units of measurement. Only quantities expressed in the same unit of measurement are directly comparable.

For each measurement method, verification process should be established and documented. This verification should ensure a level of confidence in the value that is to be obtained by applying a measurement method to an attribute of object of measurement and assigned to a base measure. Where necessary to ascertain valid value, tools used to obtain attributes should be standardized and verified at specified intervals.

The precision of the measurement method should be taken into account and the associated deviation or variance should be recorded.

A measurement method should be consistent over time so that the values assigned to a base measure taken at different times are comparable and that the values assigned to a derived measure and an indicator are also comparable.

7.5.4 Measurement function

For each individual derived measure a measurement function should be defined which is applied to two or more values assigned to base measures. This measurement function is used to transform the values assigned to one or more base measures into the value to be assigned to a derived measure. In some cases, a base measure may contribute directly to the analytical model in addition to a derived measure.

A measurement function (e.g. a calculation) may involve a variety of techniques, such as averaging all values assigned to base measures, applying weights to values assigned to base measures, or assigning qualitative values to values assigned to base measures before aggregating them into the value to be assigned to a derived measure. The measurement function may combine values assigned to base measures using different scales, such as percentages and qualitative assessment results.

7.5.5 Analytical model

For each indicator, an analytical model should be defined for the purpose of transforming one or more values assigned to a base and/or a derived measure into the value to be assigned to the indicator.

The analytical model combines relevant measures in a way that produces an output that is meaningful to stakeholders.

Decision criteria that are applied to an indicator should also be considered when defining the analytical model.

Sometimes an analytical model may be as simple as transforming a single value assigned to a derived measure into the value to be assigned to an indicator.

7.5.6 Indicators

The values to be assigned to indicators will be produced by aggregating values assigned to the derived measure and interpreting these values based on the decision criteria. For each indicator that will be reported to the client a format for indicator's presentation as a part of reporting formats (see 7.7) should be defined.

Formats for indicator's presentation will visually depict the measures and provide a verbal explanation of the indicators. Formats for indicator's presentation should be customized to meet the information need of the client.

7.5.7 Decision criteria

Decision criteria corresponding to each indicator should be defined and documented based on information security objectives, to provide actionable guidance for stakeholders. This guidance should address the expectations for progress and the thresholds for initiating improvement actions based on the indicator.

Decision criteria establish a target by which success (see 5.3) is measured and provide guidance on interpreting the indicator in relation to its proximity to the target.

Targets need to be set for each item regarding performance of ISMS processes and controls, achievement of objectives, and for effectiveness of the ISMS to be evaluated.

Management may decide not to set targets for indicators until the initial data is collected. Once the corrective actions based on the initial data are identified, appropriate decision criteria and implementation milestones can be defined that are realistic for a specific ISMS. If decision criteria cannot be established at that point, management should evaluate whether the object of measurement and corresponding measures are providing expected value for the organization.

Establishment of decision criteria can be facilitated if historic data that pertains to developed or selected measures is available. Trends observed in the past will provide insight into ranges of performance that have existed previously and guide the creation of realistic decision criteria. Decision criteria may be calculated or based on a conceptual understanding of expected behaviour. Decision criteria may be derived from historical data, plans, and heuristics, or computed as statistical control limits or statistical confidence limits.

7.5.8 Stakeholders

For each base and/or derived measure appropriate stakeholders should be identified and documented. Stakeholders may include the following:

a) Client for measurement: the management or other interested parties requesting or requiring information about the effectiveness of an ISMS, controls or group of controls;
b) Reviewer for measurement: the person or organizational unit that validates that the developed measurement constructs are appropriate for assessing the effectiveness of an ISMS, controls or group of controls;
c) Information owner: the person or organizational unit that owns the information about an object of measurement and attributes and is responsible for the measurement;
d) Information collector: the person or organizational unit responsible for collecting, recording and storing the data; and
e) Information communicator: the person or organizational unit responsible for analysing data and communicating measurement results.

7.6 Measurement construct

As a minimum, the measurement construct specification should include the following information:

a) Purpose of measurement;
b) Control objective to be achieved by controls, and specific controls, group of controls and ISMS process to be measured;
c) Object of measurement;
d) Data to be collected and used;
e) Processes for data collection and analysis;
f) Process for reporting of measurement results, including reporting formats;
g) Roles and responsibilities of relevant stakeholders; and
h) A cycle for reviewing the measurement to ensure their usefulness in relation to an information need.

Annex A provides a generic measurement construct example that incorporates a) to h). Annex B provides measurement construct examples applied to measuring ISMS processes and controls.

7.7 Data collection, analysis and reporting

Procedures for data collection and analysis, and processes for reporting of developed measurement results should be established. Supporting tools, measurement equipment and technologies should also be established, if required. These procedures, tools, measurement equipment and technologies will address the following activities:

a) Data collection, including data storage and verification (see 8.3). The procedures should identify how data are to be collected by using measurement method, measurement function and analytical model,

as well as how and where they will be stored together with any context information necessary to understand and verify the data. Data verification can be performed by inspecting the data against a checklist which is constructed to verify that missing data are minimal, and that the value to be assigned to each measure is valid.

NOTE: Verification of values to be assigned to base measures is closely related with verification of measurement method (see 7.5.3).

b) Data analysis and reporting of developed measurement results. The procedures should specify the data analysis techniques (see 9.2), and the frequency, format and methods for reporting the measurement results. The range of tools that may be needed to perform the data analysis should be identified.

Examples of reporting formats include:

- Scorecards to provide strategic information by integrating high level indicators;
- Executive and operational dashboards less focused on strategic objectives and more tied to the effectiveness of specific controls and processes;
- Reports, from simple and static in nature, such as a list of measures for a given time period, to more sophisticated cross-tab reports with nested grouping, rolling summaries, and dynamic drill-through or linking. Reports are best used when the user needs to look at raw data in an easy-to-read format; and
- Gauges to represent a dynamic values including alerts, additional graphical elements and labelling of endpoints.

7.8 Measurement implementation and documentation

The overall approach to measurement should be documented in an implementation plan. The implementation plan should include the following information as a minimum:
a) Information Security Measurement Programme implementation for the organization;
b) Measurement specification as follows:
   1) Organization's generic measurement construct;
   2) Organization's individual measurement constructs; and
   3) Definition of the range and procedures for data collection and data analysis;
c) Calendar plan to perform measurement activities;
d) Records created through performing measurement activities, including collected data and analysis records; and
e) Reporting formats for measurement results to be reported to management/stakeholders (see ISO/IEC 27001:2005 Clause 7 "Management review").

8 Measurement operation

8.1 Overview

Operation of information security measurement involves activities that are essential for ensuring that the developed measurement results provide accurate information with regard to effectiveness of an implemented ISMS, controls or group of controls and needs for appropriate improvement actions.

This activity includes the following:
a) Integrating measurement procedures into the overall operation of the ISMS.
b) Collecting, storing and verifying data.

8.2 Procedure integration

The Information Security Measurement Programme should be fully integrated into and used by the ISMS. The measurement procedures should be coordinated with the operation of the ISMS including:
a) Definition and documentation of roles, authority and responsibility, regarding development, implementation, and maintenance of information security measurement;

b) Collection of data, and, where needed, modifying current operation of the ISMS to accommodate data generation and collection activities;
c) Communication of the changes in data collection activities to relevant stakeholders;
d) Maintenance of information collectors' competency and understanding of the required types of data, data collection tools, and data collection procedures;
e) Development of policies and procedures defining the use of measurement within the organization, dissemination of the measurement information, auditing and review of the Information Security Measurement Programme;
f) Integration of data analysis and reporting into the relevant processes to ensure their regular performance;
g) Monitoring, reviewing and evaluating measurement results;
h) Establishment of a process for phasing measures out and adding new measures to ensure that they evolve with the organization; and
i) Establishment of a process for determining the useful life of historical data for trend analysis.

8.3 Data collection, storage and verification

Data collection, storage and verification activities include the following:

a) Collecting required data within regular intervals using a designated measurement method;
b) Documenting the data collection, including:
   1) date, time, and location of data collection;
   2) information collector;
   3) information owner;
   4) any issues that occurred during data collection that may be useful;
   5) information for data verification and measurement validation; and
c) Verifying collected data against measures selection criteria and measurement constructs validation criteria.

The collected data and any necessary context information should be consolidated and stored in a recording format conducive to data analysis.

9 Data analysis and measurement results reporting

9.1 Overview

Collected data should be analysed to develop measurement results and developed measurement results should be communicated.

This activity includes the following:

a) Analysing data and developing measurement results; and
b) Communicating measurement results to relevant stakeholders.

9.2 Analyse data and develop measurement results

Collected data should be analysed and interpreted in terms of the decision criteria. The data may be aggregated, transformed, or re-coded prior to analysis. During this task, data should be processed to produce the indicators. A number of analysis techniques can be applied. The depth of the analysis should be determined by the nature of the data and the information need.

NOTE Guidance for performing statistical analysis may be found ISO/TR 10017 (Guidance on statistical techniques for ISO 9001).

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 stakeholders. 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 will point to needs for improving the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures.

Those indicators that demonstrate non-compliance or poor performance should be identified and may be classified as follows:

a) Risk treatment plan failure to implement or sufficiently implement, operate, and manage controls or ISMS processes (e.g., controls and ISMS processes can be bypassed by threats);
b) Risk assessment failure:
    1) Controls or ISMS processes are ineffective because they are insufficient to either counter estimated threats (e.g. because likelihood of threats was underestimated); or counter new threats;
    2) Controls or ISMS processes are not implemented, because of overlooked threats.

Reports that are used to communicate measurement results to relevant stakeholders should be prepared using appropriate reporting formats (see 7.7) in accordance with the Information Security Measurement Programme implementation plan.

The conclusions of the analysis should be reviewed by relevant stakeholders to ensure proper interpretation of the data. The results of data analysis should be documented for communication to stakeholders.

9.3 Communicate measurement results

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

- Which measurement results are to be reported internally and externally;
- Listings of measures corresponding to individual stakeholders, and interested parties;
- Specific measurement results to be provided, and the type of presentation, tailored to the needs of each group; and
- Means for obtaining feedback from the stakeholders to be used for evaluating the usefulness of measurement results and the effectiveness of Information Security Measurement Programme.

Measurement results should be communicated to a variety of internal stakeholders including but not limited to:

- Clients for measurement (see 7.5.8);
- Information owners (see 7.5.8);
- Personnel in charge of the information security risk management, especially where failures of risk assessment are identified; and
- Personnel who are responsible to the identified areas in need of improvement.

The organization may be requested in some cases to distribute reports of measurement results to external parties, including regulatory authorities, shareholders, customers, and suppliers. It is recommended that reports on measurement results to be distributed externally only contain data appropriate for external release and are approved by management and relevant stakeholders before being released.

10 Information Security Measurement Programme Evaluation and Improvement

10.1 Overview

The organization should evaluate at planned intervals the following:

a) Effectiveness of the implemented Information Security Measurement Programme to ensure that it:
    1) Produces measurement results in an effective manner;
    2) Is executed as planned;
    3) Addresses changes in the implemented ISMS and/or controls;
    4) Addresses changes in the environment (e.g., requirements, legislation, or technology); and
b) Usefulness of developed measurement results to ensure that they satisfy relevant information needs.

Management should specify the frequency of such evaluation, plan periodic revisions and establish the mechanisms for making such revisions possible (see clause 7.2 of ISO/IEC 27001:2005).

The relevant activities should be as follows:

1) To identify evaluation criteria for the Information Security Measurement Programme (see 10.2);
2) To monitor, review, and evaluate measurement (see 10.3); and
3) To implement improvements (see 10.4).

10.2 Evaluation criteria identification for the Information Security Measurement Programme

The organization should define criteria for evaluating effectiveness of the Information Security Measurement Programme as well as usefulness of developed measurement results. The criteria should be defined at the beginning of Information Security Measurement Programme implementation, taking into account the context of the technical and business objectives of the organization.

The most likely criteria when organizations should evaluate and improve implemented Information Security Measurement Programme are:

- Changes in business objectives of the organization;
- Changes to legal or regulatory requirements and contractual obligations on information security;
- Changes in organization's requirements on information security;
- Changes in information security risks to the organization;
- Increased availability of more refined or suitable data and/or methods to collect data for measurement purposes; and
- Changes to the object of measurement and/or its attributes;

The following criteria may be applied to evaluate the developed measurement results:

a) Measurement results are:
   1) Easy to understand;
   2) Communicated in a timely manner; and
   3) Objective, comparable and reproducible.
b) Established processes for developing measurement results are:
   1) Well defined;
   2) Easy to operate; and
   3) Followed properly.
c) Measurement results are useful for improving information security.
d) Measurement results address corresponding information needs.

10.3 Monitor, review, and evaluate the Information Security Measurement Programme

The organization should monitor, review and evaluate its Information Security Measurement Programme against the established criteria (see 10.2).

The organization should identify potential needs for improvements of the Information Security Measurement Programme, including:

a) Revising or removing adopted measurement constructs that are no longer appropriate; and
b) Re-allocating resources to support the Information Security Measurement Programme.

The organization should also identify potential needs for improvements of the implemented ISMS, including its scope, policies, objectives, controls, processes and procedures; and document management decisions to allow for comparison and trend analysis during subsequent reviews.

The results of this evaluation and the identified potential needs for improvements should be communicated to relevant stakeholders to allow decision-making regarding necessary improvements.

The organization should ensure that feedback is sought from stakeholders on the results of this evaluation and the identified potential needs for improvements. The organization should understand that the feedback is one of inputs regarding effectiveness of the Information Security Measurement Programme.

10.4 Implement improvements

The organization should ensure that relevant stakeholders identify needed improvements of the Information Security Measurement Programme (see clause 7.3 e) of ISO/IEC 27001:2005). The identified improvements should be approved by management. The approved plans should be documented and communicated to appropriate stakeholders.

The organization should ensure that the approved improvements of the Information Security Measurement Programme are implemented as planned.

The organization may apply project management techniques to accomplish the improvements.

Annex A
(informative)

Template for an information security measurement construct

Annex A provides an example template for an information security measurement construct that includes all components identified in 7.5 as described in 5.4. Organizations may modify the template according to their requirements.

Measurement Construct Identification	
Measurement Construct Name	Measurement Name
Numerical Identifier	Unique organization-specific numerical identifier.
Purpose of Measurement Construct	Describes the reasons for introducing the measurement.
Control/process Objective	Control/process objective under measurement (planned or implemented).
Control (1)/process (1)	Control/process under measurement.
Control (2)/process (2)	Optional: further controls/processes within the grouping included in the same measure, if applicable (planned or implemented).
Object of Measurement and Attributes	
Object of Measurement	Object (entity) that is characterised through the measurement of its attributes. An object may include processes, plans, projects, resources, and systems, or system components.
Attribute	Property or characteristic of an object of measurement that can be distinguished quantitatively or qualitatively by human or automated means.
Base Measure Specification (for each base measure [1...n])	
Base Measure	A base measure is defined in terms of an attribute and the specified measurement method for quantifying it (e.g., number of trained personnel, number of sites, cumulative cost to date). As data is collected, a value is assigned to a base measure.
Measurement Method	Logical sequence of operations used in quantifying an attribute with respect to a specified scale.
Type of Measurement Method	Depending on the nature of the operations used to quantify an attribute, two types of method may be distinguished: - Subjective: quantification involving human judgment. - Objective: quantification based on numerical rules such as counting.
Scale	Ordered set of values or categories to which the base measure's attribute is mapped.
Type of Scale	Depending on the nature of the relationship between values on the scale, four types of scale are commonly defined: Nominal, Ordinal, Interval and Ratio.
Unit of Measurement	Particular quantity, defined and adopted by convention, with which any other quantity of the same kind can be compared to express the ratio of the two quantities as a number.
Derived Measure Specification	
Derived Measure	A measure that is derived as a function of two or more base measures.
Measurement Function	Algorithm or calculation performed to combine two or more base measures. The scale and unit of the derived measure depend on the scales and units of the base measures from which it is composed of as well as how they are combined by the function.

Indicator Specification	
Indicator	Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to a defined information need. Indicators are the basis for analysis and decision making.
Analytical Model	Algorithm or calculation combining one or more base and/or derived measures with associated decision criteria. It is based on an understanding of, or assumptions about, the expected relationship between the base and/or the derived measure and/or their behaviour over time. An analytical model produces estimates or evaluations relevant to a defined information need.
Decision Criteria Specification	
Decision Criteria	Thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result. Decision criteria help to interpret the results of measurement.
Measurement Results	
Indicator Interpretation	A description of how the sample indicator (see sample figure in indicator description) should be interpreted.
Reporting Formats	Reporting formats should be identified and documented. Describe the observations that the organization or owner of the information may want on record. Reporting formats will visually depict the measures and provide a verbal explanation of the indicators. Reporting formats should be customized to the information customer.
Stakeholders	
Client for measurement	Management or other interested parties requesting or requiring information about the effectiveness of an ISMS, controls or group of controls.
Reviewer for measurement	Person or organizational unit that validates that the developed measurement constructs are appropriate for assessing the effectiveness of an ISMS, controls or group of controls;
Information Owner	Person or organizational unit that owns the information about an object of measurement and attributes and is responsible for the measurement.
Information Collector	Person or organizational unit responsible for collecting, recording and storing the data.
Information Communicator	Person or organizational unit responsible for analysing data and communicating measurement results.
Frequency/Period	
Frequency of Data Collection	How often data is collected.
Frequency of Data Analysis	How often data is analyzed
Frequency of Reporting Measurement Results	How often measurement results are reported (this may be less frequent than data collection).
Measurement Revision	Date of measurement revision (expiry or renovation of measurement validity).
Period of Measurement	Defines the period being measured.

Annex B
(informative)

Measurement construct examples

The following clauses provide examples of measurement constructs. These examples are meant to demonstrate how to apply this International Standard using the template provided in Annex A.

Table of contents

Related Processes and Controls (Clause in ISO/IEC 27001:2005 or control number in Annex A)	**Related measurement construct examples** (reference in this Annex)	**Measurement construct example names**
Clause 4.2.2 h)	B.4.1	Information Security Incident Management Effectiveness
Clause 5.2.2 d)	B.1.1	ISMS-trained personnel
Clause 8.2	B.4.2	Corrective Action Implementation
Control A.6.1.8	B.3	ISMS Review Process
Control A.6.1.1 and A.6.1.2	B.5	Management Commitment
Control A.6.2.3	B.10	Security in Third Party Agreements
Control A.8.2. and A.8.2.2	B.1.2	Information Security Training
Control A.8.2. and A.8.2.2	B.1.3	Information Security Awareness Compliance
Control A.9.1.2	B.7	Physical Entry Controls
Control A.9.2.4	B.9	Management of Periodic Maintenance
Control A.10.4.1	B.6	Protection Against Malicious Code
Control A.10.10.1 and A.10.10.2	B.8	Log Files Review
Control A.11.3.1	B.2.1	Password Quality - manual
Control A.11.3.1	B.2.2	Password Quality - automated

B.1 ISMS Training

B.1.1 ISMS-trained personnel.

Measurement Construct Identification	
Measurement Construct Name	ISMS-trained personnel.
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	To establish control compliance with the organization's information security policy.
Control/process Objective	Clause 5.2.2 [27001:2005]. Training, awareness and competence.
Control (1)/process (1)	Clause 5.2.2.d [27001:2005]. Training, awareness and competence. The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by: d) maintaining records of education, training, skills, experience and qualifications.
Control (2)/process (2)	Optional: further controls within the grouping included in the same measure, if applicable (planned or implemented).
Object of Measurement and Attributes	
Object of Measurement	Employee database.
Attribute	Training records.
Base Measure Specification (1)	
Base Measure	Number of employees who received ISMS training according to ISMS annual training plan. Number of employees who have to receive ISMS training.
Measurement Method	Count of logs/registries with ISMS training field/row filler as "Received".
Type of Measurement Method	Objective
Scale	Numeric
Type of Scale	Ratio
Unit of Measurement	Employee
Derived Measure Specification	
Derived Measure	Percent of ISMS-trained personnel.
Measurement Function	Number of employees who received ISMS training/number of employees who have to receive ISMS training * 100.
Indicator Specification	
Indicator	Use of colour-coding with colour-identifiers. Bar graph depicting compliance over several reporting periods in relation to the thresholds (red, yellow, green) defined by the Analytical Model. The number of reporting periods to be used in the chart should be defined by the organization.
Analytical Model	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.
Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Organization-specific.
Reporting Formats	Bar graph with bars colour-coded based on decision criteria. Short summary of what the measure means and possible management actions should be attached to the bar chart.

Stakeholders	
Client for measurement	Managers responsible for an ISMS.
Reviewer for measurement	Managers responsible for an ISMS
Information Owner	Training Manager – Human Resources.
Information Collector	Training Management – Human Resource Department.
Information Communicator	Managers responsible for an ISMS.
Frequency/Period	
Frequency of Data Collection	Monthly, first working day of the month.
Frequency of Data Analysis	Quarterly
Frequency of Reporting Measurement Results	Quarterly
Measurement Revision	Review annually
Period of Measurement	Annual

B.1.2 Information Security Training

Measurement Construct Identification	
Measurement Construct Name	Information Security Training
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	To evaluate compliance with annual information security awareness Training requirement.
Control/process Objective	A.8.2 During employment Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
Control (1)/process (1)	A. 8.2.2. [27001:2005]. Information security awareness, education and training. All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.
Object of Measurement and Attributes	
Object of Measurement	Employee database.
Attribute	Training records.
Base Measure Specification (1)	
Base Measure	Number of employees who received annual information security awareness training. Number of employees who need to receive annual information security awareness training.
Measurement Method	Count of logs/registries with annual information security awareness training field/row filler as “Received”.
Type of Measurement Method	Objective
Scale	Numeric
Type of Scale	Ratio
Unit of Measurement	Employee
Derived Measure Specification	
Derived Measure	Percentage of personnel who received annual information security awareness training.
Measurement Function	Number of employees who received annual information security awareness training/number of employees who need to receive annual information security awareness training * 100.
Indicator Specification	
Indicator	Bar graph depicting compliance over several reporting periods in relation to the thresholds (red, yellow, green, with colour identifiers) defined by the Analytical Model. The number of reporting periods to be used in the chart should be defined by the organization.
Analytical Model	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.
Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Organization specific

Reporting Formats	Bar graph with bars colour-coded based on decision criteria. Short summary of what the measure means and possible management actions should be attached to the bar chart.
Stakeholders	
Client for measurement	Managers responsible for an ISMS. Security Management. Training Management.
Reviewer for measurement	Security Manager.
Information Owner	Information Security Officer and Training Manager.
Information Collector	Training Management – Human Resource Department.
Information Communicator	Managers responsible for an ISMS.
Frequency/Period	
Frequency of Data Collection	Monthly, first working day of the month.
Frequency of Data Analysis	Quarterly.
Frequency of Reporting Measurement Results	Quarterly.
Measurement Revision	Review annually
Period of Measurement	Annual

B.1.3 Information Security Awareness Compliance

Measurement Construct Identification	
Measurement Construct Name	Information security awareness policy compliance
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	Assess status of compliance with organization security awareness policy among relevant personnel
Control/process Objective	A.8.2 During employment To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
Control (1)/process (1)	A.8.2.2 All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function. (Implementation) All personnel relevant to the ISMS must receive information security awareness training before being granted access to an information system. The training includes ……
Control (2)/process (2)	A.8.2.1 Management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. (Implementation) All personnel relevant to the ISMS must sign user agreements before being granted access to an information system.
Object of Measurement and Attributes	
Object of Measurement	1.1. Information security awareness training plan/schedule 1.2 Personnel who have completed or in progress in the training. 2.1. Plan for signing user agreements/schedule 2.2. Personnel having signed agreements
Attribute	1.1. Personnel identified in plan 1.2. Personnel status with regard to the training 2.1. Personnel identified in plan for signing 2.2. Personnel status with regard to the signing of agreements
Base Measure Specification	
Base Measure	1.1.Number of personnel planned to date 1.2. Number of personnel who signed 2.1. Number of personnel planned for signing to date 2.2. Number of personnel having signed to date
Measurement Method	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
Type of Measurement Method	1.1. Objective 1.2. Subjective 2.1. Objective 2.2. Objective
Scale	1.1. Integers from zero to infinity 1.2. Integers from zero to one hundred 2.1. Integers from zero to infinity 2.2. Integers from zero to infinity
Type of Scale	1.1. Ordinal 1.2. Ratio 2.1. Ordinal 2.2. Ordinal

Unit of Measurement	1.1. Personnel 1.2. Percentage 2.1. Personnel 2.2. Personnel
Derived Measure Specification	
Derived Measure	1. Progress to date 2. Progress to date with signing
Measurement Function	1. Add status for all personnel having signed, planned to be completed to date 2. Divide Personnel having signed to date by Personnel planned for signing to date
Indicator Specification	
Indicator	a) Status expressed as a combination of ratios and; b) Trend
Analytical Model	a) [Divide Progress to Date by (Personnel Planned to Date times 100)] and Progress to date with signing b) Compare Status with Previous Statuses'
Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Interpretation for the indicator a) should be as follows: - The organization criteria for compliance with organization security awareness policy have been met satisfactorily at 0.9≤1st ratio≤1.1 and 0.99≤2nd ratio≤1.01; corresponding to standard font; - The organization criteria have been met unsatisfactorily at [1st ratio<0.9 or 1st ratio>1.1] and 0.99≤2nd ratio≤1.01; corresponding to italic; - The organization criteria are not met at [2nd ratio<0.99 or 2nd ratio>1.01]; corresponding to bold. Interpretation for the indicator b) should be as follows: - Upward trend indicates improved compliance, downward trend indicates deteriorating compliance. The degree of trend change may provide insights into the effectiveness of control implementation. Sharp changes in either direction indicate that control implementation requires close examination to determine the cause. Negative trends may require management intervention. Positive trends should be examined to identify potential best practices.
Reporting Formats	Standard Font = Criteria have been met satisfactorily Italic Font = Criteria have been met unsatisfactorily Bold Font = Criteria have not been met
Stakeholders	
Client for measurement	Managers responsible for an ISMS. Security Management. Training Management.
Reviewer for measurement	Security Manager.
Information Owner	Information Security Officer and Training Manager.
Information Collector	Training Management – Human Resource Department.
Information Communicator	Managers responsible for an ISMS.
Frequency/Period	
Frequency of Data Collection	Monthly, first working day of the month.
Frequency of Data Analysis	Quarterly.
Frequency of Reporting Measurement Results	Quarterly.

Measurement Revision	Review annually
Period of Measurement	Annual

B.2 Password Policies

B.2.1 Password Quality – manual

Measurement Construct Identification	
Measurement Construct Name	Password quality.
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	To assess the quality of the passwords used by the Users to access the organization's IT systems
Control/process Objective	To prevent user from selecting insecure passwords.
Control (1)/process (1)	A.11.3.1 Users shall be required to follow good security practices in the selection and use of passwords. Implementation. All users must select robust password for every system which: 1) length is more than 8; 2) are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc; 3) do not consist of words included in dictionaries; 4) are free of consecutive identical, all-numeric or all-alphabetic characters. All user accounts and passwords for the organization's IT systems must be controlled by the employee system.
Object of Measurement and Attributes	
Object of Measurement	User password database.
Attribute	Individual passwords.
Base Measure Specification	
Base Measure	1 Number of registered passwords. 2 Number of passwords which satisfy organization's password quality policy for each user.
Measurement Method	1 Count number of passwords on user password database. 2 Ask each user about number of passwords which satisfy organization's password policy.
Type of Measurement Method	1 Objective 2 Subjective
Scale	1 integers from zero to infinity 2 integers from zero to infinity
Type of Scale	1 Ordinal 2 Ordinal
Unit of Measurement	1 Passwords 2 Passwords
Derived Measure Specification	
Derived Measure	Total number of passwords that comply with organization's password quality policy.
Measurement Function	Σ of [Total number of passwords that comply with organization's password quality policy for each user].
Indicator Specification	
Indicator	a) Ratio of passwords which are met to organization's password quality policy. b) Trends of compliance status regarding password quality policy.
Analytical Model	a) Divide [Total number of passwords complied with organization's password quality policy] by [Number of registered passwords]. b) Compare ratio with the previous ratio.

Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Interpretation for the indicator a) should be as follows: • The organization criteria for compliance with organizational password policy are met satisfactorily at the ratios>0.9. • The organization criteria for compliance with organizational password policy are met unsatisfactorily at [0.8≤the ratio≤0.9]. • The organization criteria for compliance with organizational password policy are not met at the ratio<0.8. Interpretation of Indicators b) should be as follows : • Upward trend indicates improved compliance, downward trend indicate deteriorating compliance. • The degree of trend change may provide insights into the effectiveness of implemented controls. • Negative trend may require further controls such as awareness, or technical means to force for selection of robust passwords or changing passwords periodically. • Positive trends should be examined to estimate necessary terms to meet password policy from current ratio. The effect/impact of the criteria not being met is increased risk of confidentiality breaches. Potential causes of deviation include lack of security awareness, technical implementation deficiencies, and lack of time for implementing on all IT systems.
Reporting Formats	Trend line that depicts the number of passwords compliant with organization's password quality policy, superimposed with trend lines produced during previous reporting periods.
Stakeholders	
Client for measurement	Managers responsible for an ISMS, Security Manager.
Reviewer for measurement	Security Management.
Information Owner	System Administrator.
Information Collector	Security Staff.
Information Communicator	Security Staff.
Frequency/Period	
Frequency of Data Collection	Yearly.
Frequency of Data Analysis	Yearly.
Frequency of Reporting Measurement Results	Yearly.
Measurement Revision	Review and update every years.
Period of Measurement	Annually.

B.2.2 Password Quality – automated

Measurement Construct Identification	
Measurement Construct Name	Password quality.
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	To assess the quality of the passwords used by the Users to access the organization's IT systems
Control/process Objective	To prevent user from selecting insecure passwords.
Control (1)/process (1)	A.11.3.1 Users shall be required to follow good security practices in the selection and use of passwords. Implementation: All users must select robust password for every system which: 1) length is more than 8; 2) are not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc; 3) do not consist of words included in dictionaries; 4) are free of consecutive identical, all-numeric or all-alphabetic characters. All user accounts and passwords for the organization's IT systems must be controlled by the employee system. Robustness of password must be examined by using a password cracking software.
Object of Measurement and Attributes	
Object of Measurement	Employee system account database.
Attribute	Individual passwords stored in employee system account records.
Base Measure Specification	
Base Measure	1Total number of passwords 2 Total number of uncrackable passwords
Measurement Method	1 Run query on employee account records. 2 Run password cracker on employee system account records using hybrid attack.
Type of Measurement Method	1 Objective 2 Objective
Scale	1 integers from zero to infinity 2 integers from zero to infinity
Type of Scale	1 Ordinal 2 Ordinal
Unit of Measurement	1 Passwords 2 Passwords
Derived Measure Specification	
Derived Measure	None
Measurement Function	None
Indicator Specification	
Indicator	1 Ratio of passwords crackable within 4 hours. 2 Trend of the ratio 1.
Analytical Model	a) Divide [Number of uncrackable passwords] by [Total number of passwords]. b) Compare ratio with the previous ratio.

Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Interpretation for the indicator 1 should be as follows: • The organization criteria for compliance with organizational password policy are met satisfactorily at the ratios>0.9. • The organization criteria for compliance with organizational password policy are met unsatisfactorily at [0.8≤the ratio≤0.9]. • The organization criteria for compliance with organizational password policy are not met at the ratio<0.8. Interpretation of Indicators b) should be as follows : • Upward trend indicates improved compliance, downward trend indicate deteriorating compliance. • The degree of trend change may provide insights into the effectiveness of implemented controls. • Negative trend may require further controls such as awareness, or technical means to force for selection of robust passwords or changing passwords periodically. • Positive trends should be examined to estimate necessary terms to meet password policy from current ratio. The effect/impact of the criteria not being met is increased risk of password compromise that may lead to unauthorized system access. Potential causes of deviation include lack of security awareness, technical implementation deficiencies, and lack of time for implementing on all IT systems.
Reporting Formats	Trend line that depicts password crackability for all records tested superimposed with lines produced during previous tests.
Stakeholders	
Client for measurement	Managers responsible for an ISMS, Security Manager.
Reviewer for measurement	Security Management
Information Owner	System Administrator.
Information Collector	Security Staff.
Information Communicator	Security Staff.
Frequency/Period	
Frequency of Data Collection	Weekly.
Frequency of Data Analysis	Weekly.
Frequency of Reporting Measurement Results	Weekly.
Measurement Revision	Review and update every year.
Period of Measurement	Applicable 3 years.

B.3 ISMS Review Process

Measurement Construct Identification	
Measurement Construct Name	ISMS Review Process
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	To assess the degree of accomplishment of independent review of information security
Control/process Objective	To manage information security within the organization
Control (1)/process (1)	A.6.1.8 The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) shall be reviewed independently at planned intervals, or when significant changes to the security implementation occur. (Implementation) The organization's approach to managing information security and its implementation is reviewed by a third party security consultant quarterly.
Object of Measurement and Attributes	
Object of Measurement	1. Reports of third party reviews. 2. Plans of third party reviews.
Attribute	1. Reported third party reviews 2. Planned third party reviews
Base Measure Specification	
Base Measure	1 Number of conducted reviews by third party. 2Total number of planned third party reviews.
Measurement Method	1 Count number of report of conducted regular reviews by third party. 2. Count total number of planned third party reviews.
Type of Measurement Method	1 Objective 2 Objective
Scale	1 integers from zero to infinity 2 integers from zero to infinity
Type of Scale	1 Ordinal 2 Ordinal
Unit of Measurement	1 Review 2 Review
Derived Measure Specification	
Derived Measure	None
Measurement Function	None
Indicator Specification	
Indicator	Progress ratio of accomplished independent reviews.
Analytical Model	Divide [Number of conducted reviews by third party] by [Total number of planned third party reviews].
Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	

Indicator Interpretation	Interpretation for the indicator should be as follows: The organizational criteria for managing information security within the organization thorough third party review have been met satisfactorily at 0.8≤ the ratio≤1.1. The organizational criteria have been met unsatisfactorily at [0.6≤the ratio<0.8 or the ratio>1.1]. Monitoring is required to ensure appropriate progress is made. The organizational criteria are not met at [0≤ the ratio<0.6]. Immediate intervention is required to ensure appropriate progress is made. If at the end of second quarter the indicator a) is unsatisfactory, a corrective action is needed and should be communicated to management responsible for the ISMS. If at the end of year the indicator a) is unsatisfactory, senior management have to be informed and asked for their support. The effect/impact of the criteria not being met is ineffective management review process. Potential causes of deviation include low budget, incorrect planning, and lack of critical personnel/management commitment.
Reporting Formats	Bar graph depicting compliance over several reporting periods in relation to the thresholds defined by the decision criteria.
Stakeholders	
Client for measurement	Managers responsible for an ISMS, Quality System Manager
Reviewer for measurement	Managers responsible for an ISMS.
Information Owner	Managers responsible for an ISMS.
Information Collector	Internal Audit. Quality Manager
Information Communicator	Internal Audit. Quality Manager. Managers responsible for an ISMS
Frequency/Period	
Frequency of Data Collection	Quarterly
Frequency of Data Analysis	Quarterly
Frequency of Reporting Measurement Results	Quarterly
Measurement Revision	Review and update every 2 years.
Period of Measurement	Applicable 2 years.

B.4 ISMS Continual Improvement

B.4.1 Information Security Incident Management Effectiveness

Measurement Construct Identification	
Measurement Construct Name	Information security incident management effectiveness.
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	Assess the effectiveness of Information security incident management.
Control/process Objective	To enable prompt detection of security events and response to security incidents.
Control (1)/process (1)	Clause 4.2.2 h) [27001:2005].
Object of Measurement and Attributes	
Object of Measurement	ISMS.
Attribute	Individual incident.
Base Measure Specification	
Base Measure	Pre-determined threshold number.
Measurement Method	Count occurrences of information security incidents reported by the date.
Type of Measurement Method	Objective.
Scale	Numeric.
Type of Scale	Ordinal.
Unit of Measurement	Incident.
Derived Measure Specification	
Derived Measure	Incidents exceeding threshold.
Measurement Function	Comparison of number of total incidents with the threshold.
Indicator Specification	
Indicator	Line chart that depicts the constant horizontal line illustrating the threshold number(s) against the total number of incidents over several reporting periods.
Analytical Model	Red when total number of incidents exceeds the threshold (goes over the line); yellow when total number of incidents is within 10% of the threshold; green when total number of incidents is below the threshold by 10% or more.
Decision Criteria Specification	
Decision Criteria	Red – immediate investigation into causes of increase in number of incidents is required. Yellow – numbers need to be closely monitored and investigation should be started if numbers are not improving. Green – no action is required.
Measurement Results	
Indicator Interpretation	If red is observed in two reporting cycles, a review of the incident management procedures is required to correct existing procedures or to identify additional procedures. If the trend is not reversed during the next two reporting periods corrective action is required, such as proposing an extension to the ISMS scope.
Reporting Formats	Line chart.
Stakeholders	
Client for measurement	ISMS Management Committee. Managers responsible for an ISMS. Security Management. Incident Management.
Reviewer for measurement	Managers responsible for an ISMS.
Information Owner	Managers responsible for an ISMS.
Information Collector	Incident Management Manager.

Information Communicator	ISMS Management Committee.
Frequency/Period	
Frequency of Data Collection	Monthly
Frequency of Data Analysis	Monthly
Frequency of Reporting Measurement Results	Monthly
Measurement Revision	Six months
Period of Measurement	Monthly

B.4.2 Corrective Action Implementation

Measurement Construct Identification	
Measurement Construct Name	Corrective action implementation
Numerical Identifier	Organization-specific identifier
Purpose of Measurement Construct	Assess performance of corrective action implementation.
Control/process Objective	Clause 8.2 [27001:2005]. Corrective action. The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence.
Control (1)/process (1)	The documented procedure for corrective action shall define requirements for: a) identifying nonconformities; b) determining the causes of nonconformities; c) evaluating the need for actions to ensure that nonconformities do not recur; d) determining and implementing the corrective action needed; e) recording results of action taken (see 4.3.3); and f) reviewing of corrective action taken. (implemented) …….. The organization determines the corrective actions required, and issues the corrective action report documenting information regarding non-conformity, its cause, and the due date for the corrective action to be taken. Upon receiving the report, the manager responsible for the area where the non-conformity is detected is required to ensure that actions are taken without undue delay to eliminate detected non-conformities and their causes. If corrective action is not implemented as required, the cause of non-implementation has to be identified, as well as alternatives to the original corrective action that would be determined to be appropriate. The actions taken with the corresponding date and results should be documented. If the corrective action is not implemented as planned the reason and the alternative action have to be documented. The report should be provided to Information Security Manager.
Object of Measurement and Attributes	
Object of Measurement	Corrective action reports.
Attribute	Corrective action due date in report. Date of corrective action taken in report record. Reason for delaying and not taking the action.
Base Measure Specification	
Base Measure	1. Number of corrective actions planned to date. 2. Number of corrective actions implemented as planned to date. 3. Number of corrective actions not implemented with reason, to date.
Measurement Method	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.
Type of Measurement Method	1 – 3 Objective
Scale	1 – 3 integers from zero to infinity

Type of Scale	1 – 3 Ordinal
Unit of Measurement	1 – 3 Corrective action
Derived Measure Specification	
Derived Measure	a) Corrective action not implemented to date b) Corrective action not implemented without legitimate reason
Measurement Function	a) Subtract [Corrective actions taken as planned to date] from [Corrective actions planned to date] b) Subtract [Corrective action not implemented to date] from [Corrective actions not taken as planned with reason, to date]
Indicator Specification	
Indicator	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
Analytical Model	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'
Decision Criteria Specification	
Decision Criteria	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.
Measurement Results	
Indicator Interpretation	Interpretation for the indicator a) and b) should be as follows: Planned corrective actions must be implemented unless the organization's priorities have changed that would result in the need to implement different corrective actions or redirection of resources allocated to corrective action implementation. If over 40% of corrective actions are not implemented regardless of the reason, management action is required. If over 20% of corrective actions are not implemented without a good reason, management action is required. Corrective actions that were not implemented should be examined to identify reasons for non-implementation. Depending on the overall percentage not implemented and reasons for non implementation, further action may be required. Interpretation for the indicator c) should be as follows: A trend in corrective action implementation should be examined for any overall deterioration in performance or for significant improvement in performance. If percentage of implemented corrective action has been steadily declining for the last 2 reporting periods, management action is required regardless of the breakdown in the reasons for non-compliance. The effects/impact of criteria not being met is potential lack of continual ISMS improvement. The potential causes may include lack of resources, incorrect planning, and lack of critical personnel and management commitment.
Reporting Formats	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.

Stakeholders	
Client for measurement	Managers responsible for ISMS. Information Security Manager.
Reviewer for measurement	Managers responsible for ISMS.
Information Owner	Managers responsible for ISMS.
Information Collector	Managers responsible for ISMS.
Information Communicator	Managers responsible for ISMS.
Frequency/Period	
Frequency of Data Collection	Quarterly.
Frequency of Data Analysis	Quarterly.
Frequency of Reporting Measurement Results	Quarterly.
Measurement Revision	Review annually.
Period of Measurement	Applicable 1 year.

B.5 Management Commitment

Measurement Construct Identification	
Measurement Construct Name	Frequency of management review
Numerical Identifier	Organization-specific.
Purpose of Measurement Construct	Assess management commitment and information security review activities regarding management review activities.
Control/process Objective	A.6.1 To manage information security within the organization (planned). To manage information security within the organization through regularly performing management reviews.
Control (1)/process (1)	A.6.1.1 Management commitment to information security Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security (implemented). The organization must have management review meeting monthly to support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgement of information security. ISMS management review should be combined with QMS management review.
Control (2)/process (2)	A.6.1.2 Information security co-ordination Information security activities shall be co-ordinated by representatives from different parts of the organization with relevant roles and job functions. (implemented). Representatives of different departments who hold relevant roles and responsibilities should coordinate and participate in management review.
Object of Measurement and Attributes	
Object of Measurement	1. Information security management review plan/schedule. 2. Management review minutes records
Attribute	1.1 Management review meetings dates scheduled in the plan 1.2 Managers scheduled to attend management review meetings 2.1 Management review meetings dates recorded in meeting minutes 2.2 Managers recorded as having attended management review meetings
Base Measure Specification	
Base Measure	1.1 Number of management review meetings planned to date 1.2 Number of managers scheduled to attend management review meetings 2.1.1 Number of planned management review meetings held to date 2.1.2 Number of unplanned management review meetings held to date 2.1.3 Number of rescheduled management review meetings held to date 2.3 Number of managers who attended management review meetings to date

Measurement Method	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.
Type of Measurement Method	1.1 Objective 1.2 Objective or subjective 2.1.1 Objective 2.1.2 Objective 2.1.3 Objective 2.2 Objective
Scale	1.1 integers from zero to infinity 1.2 integers from zero to infinity 2.1.1 integers from zero to infinity 2.1.2 integers from zero to infinity 2.1.3 integers from zero to infinity 2.2 integers from zero to infinity
Type of Scale	1.1 Ordinal 1.2 Ordinal 2.1.1 Ordinal 2.1.2 Ordinal 2.1.3 Ordinal 2.2 Ordinal
Unit of Measurement	1.1 Meeting 1.2 Personnel 2.1.1 Meeting 2.1.2 Meeting 2.1.3 Meeting 2.2 Personnel
Derived Measure Specification	
Derived Measure	a) Number of management review meetings held to date b) Participation rates in management review meetings held to date
Measurement Function	a) Add [number of planned management review meetings to date] and [number of unplanned management review meetings to date] and [number of rescheduled management review meetings to date] b) For each management review meeting divide [number of managers who attended management review meeting] by [number of managers scheduled to attend management review meeting]
Indicator Specification	
Indicator	a) Management review meetings completed to date b) Average participation rates in management review meetings to date
Analytical Model	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.
Decision Criteria Specification	
Decision Criteria	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.