ISO/IEC JTC 1/SC 27 **N4810**

ISO/IEC JTC 1/SC 27/WG 1 **N14810**

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: Text for Working Draft

TITLE: **Draft Text for ISO/IEC 3rd WD 27004, Information technology -- Security techniques -- Information security management measurements**

SOURCE: Project Editors (E. Kuiper, P. llaneza)

DATE: 2006-01-07

PROJECT: 27004

STATUS: In accordance with resolution 5 (ref. document SC27 N4825rev1) of the 31st SC 27 WG1 Plenary Meeting in Kuala Lumpur (Malaysia), Nov 7 - 11, 2005, this document is being circulated for **STUDY AND COMMENT.** The national bodies and liaison organizations of SC27 are requested to send their comments/contributions on this Working Draft directly to the SC27 Secretariat by 2006-04-07.

PLEASE NOTE: For comments please use THE SC27 TEMPLATE separately attached to this document.

ACTION ID: **COM**

DUE DATE: **2006-04-07**

DISTRIBUTION: P-, O- and L-Members
W. Fumy, SC27 Chairman
M. De Soete, SC27 Vice-Chair
T. Humphreys, K. Naemura, M. Ohlin, WG Conveners
A. Plate, SC27/WG1 Secretariat

MEDIUM: Livelink Server

NO. OF PAGES: 1 + 36 + 1 (Template)

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile:+ 49 30 2601-1723; e-mail: krystyna.passia@din.de
HTTP://www.ni.din.de/sc27

Information technology — Security techniques — Information security management — Measurements
WD 27004

0 Introduction

This International Standard is one of a number in the ISO/IEC 27000 series that address the specification of an information security management system (ISMS). This particular standard provides guidance and advice in support of the monitoring and measurement requirements for an ISMS as specified in ISO/IEC 27001.

This International Standard is also applicable to any organisation that has an information security management programme and that wishes to make measurements concerning information security management.

The use of this standard will allow organizations to answer the question how effective and efficient the information security management programme is and what degree of implementation and maturity has been achieved. Use of measurements will allow comparison of achieved information security outcomes over a period of time and between similar business areas in the organization as part of continuous improvement.

1 Scope

This International Standard provides guidance on the specification and use of measurement techniques for providing assurance as regards the effectiveness of information security management systems. It is intended to be applicable to a wide range of organisations with a correspondingly wide range of information security management systems.

This International Standard provides guidance for measurement procedures and techniques to determine the effectiveness of information security controls and information security processes applied in an ISMS.

The purpose of the Information security management measurements development and implementation process, defined in this Standard is to create a base for each organization to collect, analyse, and communicate data related to ISMS processes. This data is ultimately to be used to base ISMS-related decisions and to improve implementation of an ISMS.

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 27001:2005, Information technology - Security techniques - Information security management systems requirements

3 Terms and definitions

For the purposes of this Guide, the following terms and definitions apply.

3.1
attribute
Property or characteristic of an entity that can be distinguished quantitatively or qualitatively by human or automated means [ISO/IEC 15939:2002]

3.2
base measure
Measure defined in terms of an attribute and the method for quantifying it [ISO/IEC 15939:2002]
NOTE 1 A base measure is functionally independent of other measures.

3.3
business object
A business object is a business process, business unit, system or location.

3.4
derived measure
A measure that is defined as a function of two or more values of base measures [ISO/IEC 15939:2002]

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

3.6
effectiveness
a measure of how well the ISMS, a process, or a control achieves the information control objectives.

3.7
entity
an object that shall be characterised through the measurement of its attributes. [ISO/IEC 15939].
NOTE: The entity may be tangible or intangible.

3.8
form of measurement
set of operations, either a measurement method, a function of calculation, or an analytical model, aimed at determining the value of a measurement.

3.9
information security control
Standards or countermeasures prescribed for ISMS to protect confidentiality, availability, and integrity of the ISMS and its information.

3.10
information security indicator
An information security indicator is an extension adding measurement interpretation criteria.

EDITORS' NOTE:
UK suggestion: An indicator is a measure that provides an estimate or evaluation of specified attributes derived from a model with respect to defined information needs.

3.11
information security management system (ISMS)
that part of the overall management system, based on a business risk approach, that establishes, implements, operates, monitors, reviews, maintains and improve information security [ISO/IEC N4036].

NOTE: the management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

3.12
management
process planning, organising, directing, communicating and controlling activity

3.13
measure
variable to which a value is assigned as the result of measurement [ISO/IEC 15939:2002]

3.14
measurable concept
an abstract relationship between the attributes of one or more entities and a need for information

3.15
measurement
the action or set of actions that make it possible to obtain the value of a measurement for the attribute of an entity using a form of measurement

NOTE. Whenever in this Standard the terms “measurement” or “measurements” are used, the whole range indicators and measures is meant [i.e. base measures, derived measures and indicators] unless a specific type of document is referred to.

3.16
measurement function
algorithm or calculation performed to combine two or more base measures. [ISO/IEC 15939:2002]

3.17
measurement method
the logical sequence of operations expressed generically that make it possible to undertake the description of measurement. [ISO/IEC 15939:2002]

3.18
model
algorithm or calculation combining one or more base and/or derived measures with associated decision criteria [ISO/IEC 15939:2002]

3.19
scale
ordered set of values, continuous or discrete, or a set of categories to which the attribute is mapped [ISO/IEC 15939:2002]

3.20
control objectives
objectives of management that are used as the framework for developing and implementing controls (control procedures). [ISACA].

3.21
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

4 Measurements in the ISMS

This International Standard supports the requirements of the ISMS Plan – Do – Check – Act (PDCA) cycle. Measures are used mainly for the measurement of the of the “Do” components of an ISMS (Implement and operate the ISMS) as input to the “Check” (monitor and review) components of an ISMS, with the goal of providing a means for taking decisions at the “ACT” (maintain and improve the ISMS) stage, leading to continuous improvement of the ISMS cycle.

Measurements should be integrated into the management cycle of the organization and used to effect improvement of security-related processes and outcomes within the project or organization.

The measurements themselves should be used for security-related decision making regarding improvement to or changes within the ISMS.

An organization should describe how ISMS and the measurements interact and interrelate. Guidelines should be developed to ensure this relationship is clarified and documented.

The objectives of the measurement process are:

- Evaluate security controls implementation effectiveness.
- Evaluate the information security management system effectiveness including continuous improvement.
- Provide security status to guide management review, facilitate security improvements, and provide input for security audits.
- Communicate value of security to the organization.
- Serve as an input into risk assessment and risk treatment plan

EDITORS' NOTE*: figure 1 to be agreed. Editors call for contributions.*
NB proposals received in KL.

Japanese proposal

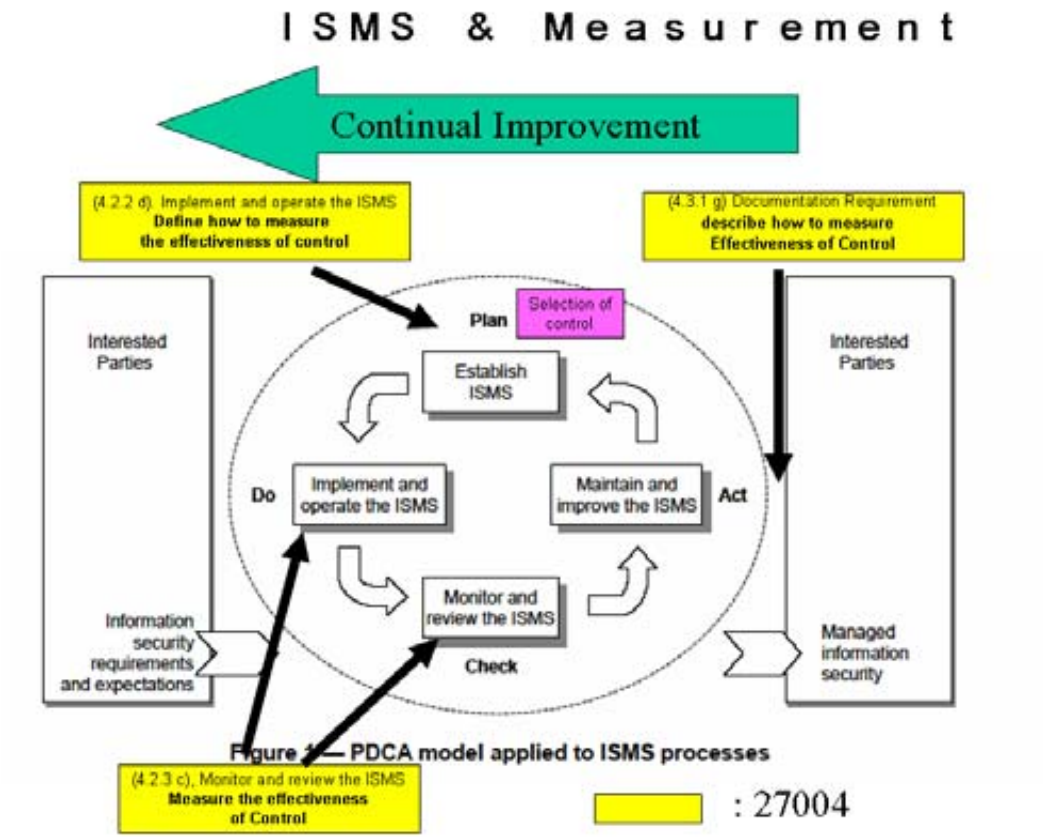
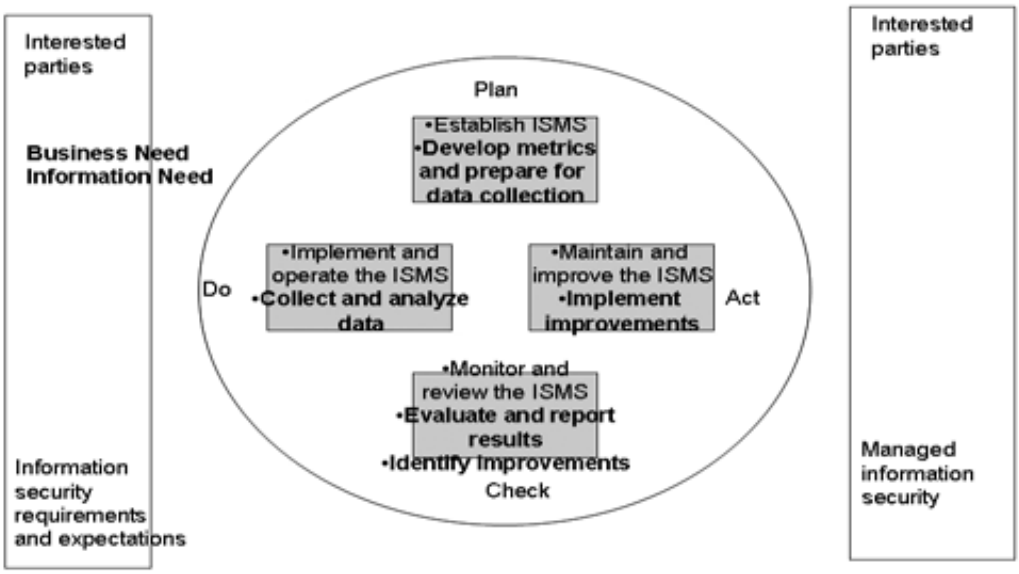


Figure 1 — PDCA model applied to ISMS processes

US/ISSEA Proposal



Spanish Proposal

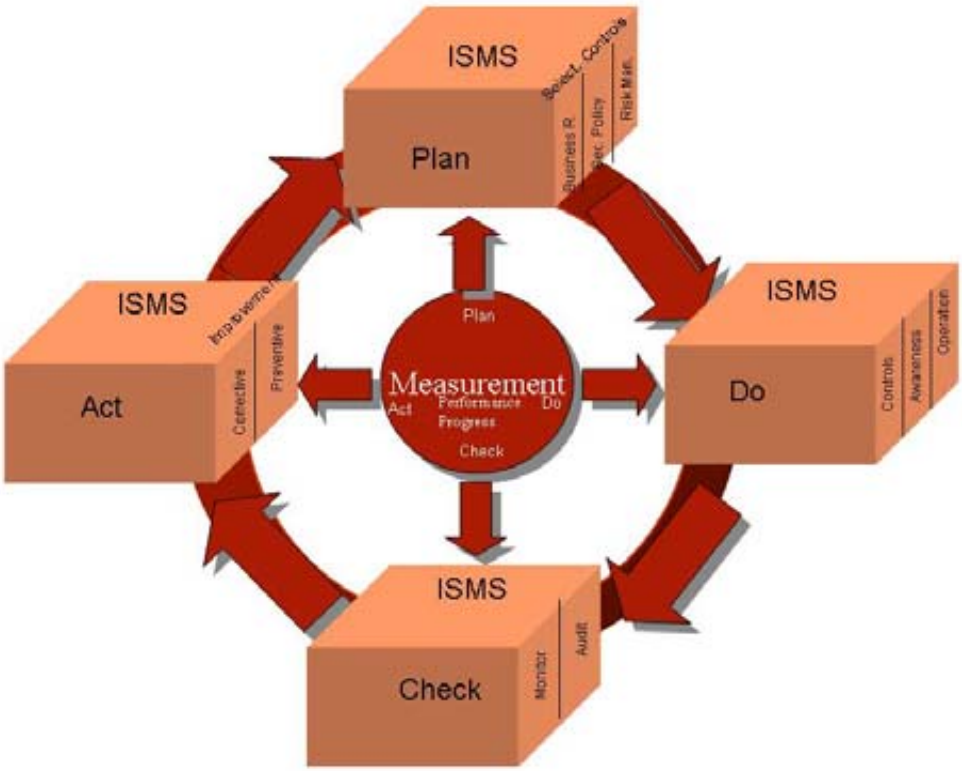


Figure 1. The organization should implement a PDCA circle to establish, implement, monitor, maintain and improve measurements.

5 Measurements Information Security Model

An organization, through the use of measurements, may identify the adequacy of in-place security controls, policies, and procedures and develop a programto measure Information Security performance.

Its goal is to explain the measurement development and implementation process and so assist in the creation of a measurements programme that can assist management when making decisions about the effectiveness of security controls. This measurement programme should be based upon Measurements information Security Model.

5.1 Model definition

The selection or definition of appropriate measurements to address an information need begins with a measurable concept: an idea of which measurable attributes are related to an information need and how they are related.

The measurement planner defines measurement constructs that link these attributes to a specified information need. The measurement information model helps to determine what the measurement planner needs to specify during measurement planning, performance, and evaluation.

The Measurements Information Security Model is a structure linking information needs to the relevant entities and attributes of concern. Entities include processes, products, projects, and resources.

The Measurements Information Security Model describes how the relevant attributes are quantified and converted to indicators that provide a basis for decision making.

An entity may have many attributes, only some of which may be of interest for measurement. The first step in defining a specific instantiation of the measurement information model is to select the attributes that are most relevant to the measurement user's information needs. A given attribute may be incorporated in multiple measurement constructs supporting different information needs.

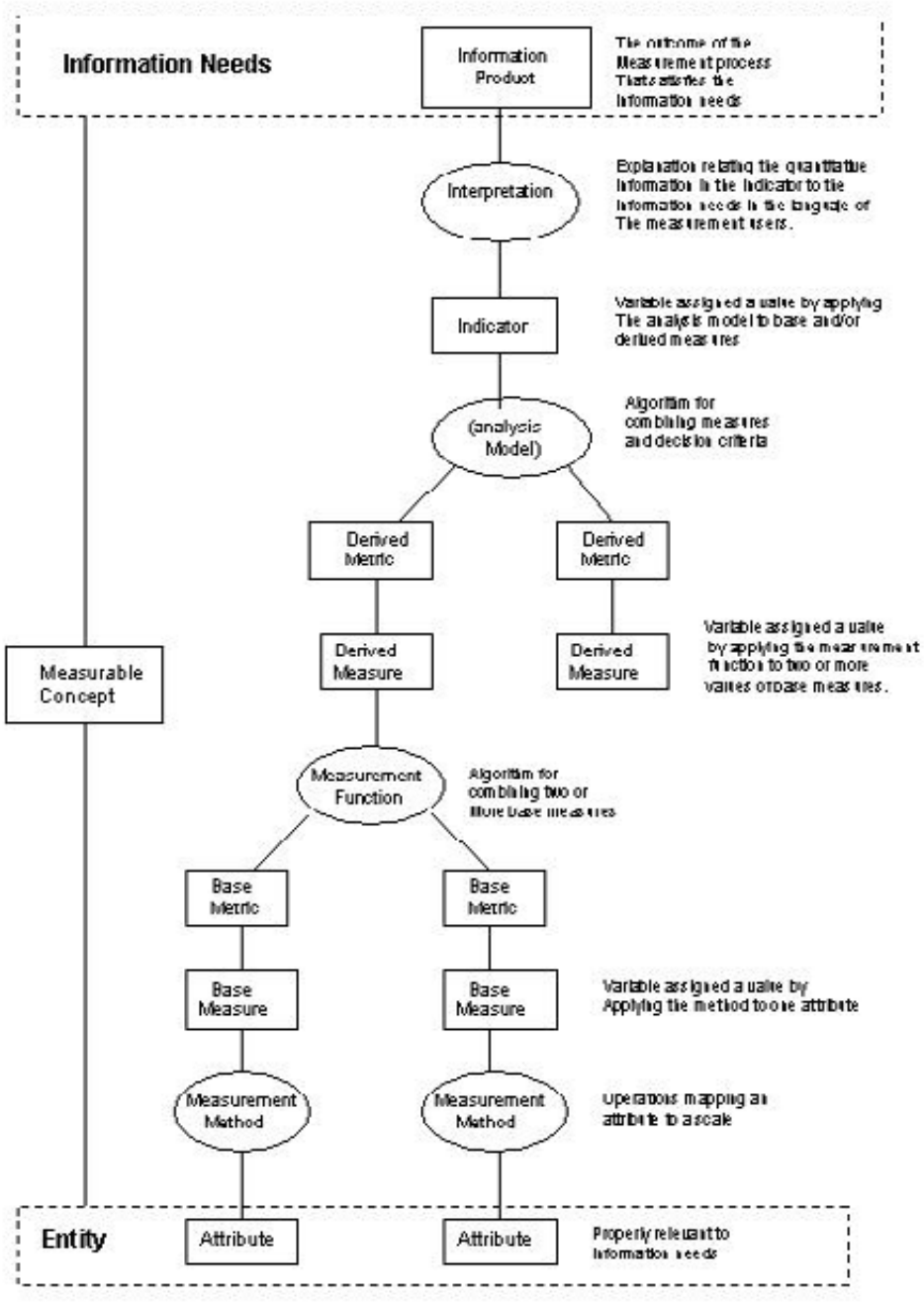


Figure A.1 –Key relationships in the Measurement Information Model

Figure 2 illustrates the relationships among the key components of the measurement information security model. The model defines three types of measures: base measures, derived measures, and indicators. The information content of measures increases as they become closer in the model to the information need. The individual components of the generic information model are described below.

5. 2 Identify the method

The method should describe how the attributes of the object under measurement (i.e., the data source) is measured.

Possible examples of data sources are:

- Internal or external audits, for example, to measure the degree of implementation of an ISM measurements
- Risk analyses, to measure an information system's risk levels
- The use of questionnaires
- The use of records, such as records of events
- Through a formally written, formulated procedure
- Through the automatic output of an information system, such as statistics and data yielded by an IDS, etc.

Provision of adequate data for the measurement should be defined and documented, including

- Definition of data and data sources available
- Responsible person(s) for data gathering
- Date/time of availability of data
- Location where to find data
- Interaction of management like
- Security requirements
- Reports for management
- Audit of the measurement by management

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

- Subjective: quantification involving human judgement
- Objective: quantification based on numerical rules such as counting. These rules may be implemented via human or automated means.

The measurement method operations may involve activities such as counting occurrences or observing the passage of time. The same measurement method may be applied to multiple attributes. However, each unique combination of an attribute and a method produces a different base measure. Possible examples of measurements methods are:

- Inquiry
- Observation
- Questionnaire
- Knowledge assessment
- Inspection
- Re-performance (re-execute, re-creating…)
- System queries
- Testing. The following testing techniques might help an organization to meet its needs
    - Tests of Design: how to determine if a control has been designed to achieve the control objective
    - Tests of Operating Effectiveness: does the control achieve the objective and operate correctly over a period of time
- Sampling: sampling Guidelines are necessary to define how to achieve a statistically valid sample. The following statistical techniques or families of techniques might help an organization to meet its needs:
    - descriptive statistics;
    - design of experiments;
    - hypothesis testing;
    - measurement analysis;
    - process capability analysis;
    - regression analysis;
    - reliability analysis;
    - sampling;
    - simulation;
    - statistical process control (SPC) charts;

- statistical tolerance;
- time series analysis.

Some measurement methods may be implemented in multiple ways. A measurement procedure describes the specific implementation of a measurement method within a given organisational context.

The measurement method maps the magnitude of the measured attribute to a value on a scale. A unit of measurement often is associated with a scale.

a) Type of scale

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

Nominal: the measurement values are categorical. For example, the classification of defects by their type does not imply order among the categories.

Ordinal: the measurement values are rankings. For example, the assignment of defects to a severity level is a ranking.

Interval: the measurement values have equal distances corresponding to equal quantities of the attribute. For example, cyclomatic complexity has the minimum value of one, but each increment represents an additional path. The value of zero is not possible.

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. For example, the size of a software component in terms of LOC is a ratio scale because the value of zero corresponds to no lines of code and each additional increment represents equal amounts of code.

The method of measurement usually affects the type of scale that can be used reliably with a given attribute. As an example of scale, subjective methods of measurement usually only support ordinal or nominal scales.

b) Unit of measurement

A 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. Only quantities expressed in the same units of measurement are directly comparable. Example of units includes the hour and the metre.

5.3 Identify the frequency

The intervals at which the measurements of the ISM measurements programme are to be obtained should be defined: weekly, monthly, quarterly, annually, etc.

This frequency should be established as a compromise between the need to avail of the information and the cost of obtaining it.

6 Definition and selection of ISM measurements

This section specifies how to develop ISM measurements for the purpose of quantifying effectiveness of ISMS, its processes, and controls. It covers the measurement of the effectiveness of sets of controls as well as of the effectiveness of the management systems that surround the controls. It is anticipated that an understanding and application of this section will result in an organization developing and implementing stakeholder-specific sets of measurements.

Information security measurements should be based on relevant stakeholders' information needs and organization's control objectives. Assuming that the control objectives address risk tolerance levels

and cost effectiveness, information security indicators should measure deviations from acceptable risk and cost levels. Information security measurements should be matched to control objectives to:

- Keep the impact of actual events consistent with risk tolerance; and
- Ensure that security management activities are cost effective.

Typically the objectives will not be directly measurable, so available information security indicators will have to be assessed and evaluated to determine measurements of achievement of those objectives.

Where information security activities include specific risk management processes, e.g. if there is an established process for accrediting Information Security systems (including services) before connection to the Information Security infrastructure, the proportion of recently accredited systems in the organisation could be taken as a information security measurement. Other categories of information security measurement may include the number of malicious code incidents that have affected the system, the availability of key information systems, the number of breaches of physical security, the proportion of correctly licensed software, proportion of lost assets etc against set targets.

While information control objectives and stakeholder information needs may cover a variety of topics, specific information security measurements may be required to address the following requirements

- Corporate governance
- Legislative and regulatory compliance
- Organisational management and operations
- Certification of information security management systems, operational Information Security environments
- Customers and other stakeholders
- Improvement of information security implementation and effectiveness
- Process improvement

In some cases, the stakeholders will be concerned with the absolute value of an information security measurement. For example, senior management of an organisation may be interested in the aggregate planned acceptable risk (risk tolerance) or the total cost of a security management programme. In other cases, relative measurements may be valuable (e.g, comparison with industry standards and benchmarks; comparison with best practice; comparison with previous results; comparison across different divisions within an organisation; comparison with competitors; or comparing information security expenditure with Information Security expenditure).

The ISM measurements steps guiding the establishment and operation of a programme of measures are: the definition process, the development of the applicable measurements, the implementation of the measurements programme and the revision of the measurements.

The ISM measurements programme establishes the ensemble of selected ISM measurements that are appropriate for an organization at a given moment and its implementation. Organizations must limit the number of measurements they use within the same time period to ensure organization's ability to effect change, based on the collected information. Excessive number of ISM measures may result in organization's inability to focus its efforts on its priorities

It is important to consider the convenience of following an incremental model, that is, to start an ISM measurement programme with a limited scope and then to increase it when obtaining results and then to refine methods and procedures.

Lastly, the ISM measurements must be revised following the later steps developed in "ISM measurements validation" for verifying that

- They continue to supply the organization with valid information.
- The sources and other aspects related with their attributes are correct.
- The benefits against the required effort maintain a profitable rate.

As a consequence of this analysis, the measurement may be maintained, eliminated, substituted or modified.

6.1 Types of ISM measurements

The ISM measurements should focus on checking the information security status. The status is a direct or an indirect result of the information security management system. The measurement shall generate an input for improvement of the management system itself as well as the protection of information within the organization.

ISM measurements relate directly to the management system processes (e.g. Are audits done?, does manual comply with standard?, are resolution of outstanding issues up to date?... etc) and to the performance of information security controls (e.g. training coverage, volumes of incidents by type, correctness of implementations -access tables, and other types of protective means)

This standard defines two categories of information security measurements, as follows:

- Performance measurements: effectiveness
- Progress measurements: changes in protection of information

6.1.1. ISM performance measurements

In designing each information security control, it is necessary to establish measurements to evaluate the effectiveness and cost of the control once it is implemented. It must be possible to verify that a given control complies with the control objectives for which it was designed and to establish its degree of performance in fulfilling its function.

In the selection of ISM measurements and of the information that they yield, it is likewise relevant to know that security controls are meeting their objectives by determine how well they contribute to security requirements derived from:

- The assessment and management of detected risks
- The set of legal, statutory, regulatory and contractual requirements
- The principles and guidelines of the organisation for processing information.
- The scope of technical and organizational resources involved to protect the information security align with objectives

ISM Measurements should then be applied accordingly from the derived need of measurements in order to provide the necessary information security performance indicators

Example of measurements for a subset of ISO/IEC 27001 controls are illustrated in Annex B. In general, for most of the ISO/IEC 27001 controls, effectiveness measurements can be set as the measurements of policy lapse or inconsistent deployment captured during internal ISMS audit, periodic review, sample check or regular monitoring.

6.1.2. ISM progress measurements

The management of information security implies development. The development could be seen as:

a. Progress of information security performance, e.g. changes of indicator values
b. Progress of the ability of the information security process to handle changes in the organisation's environment (external, internal). This may be development in the maturity of information security controls or in the incorporation of new projects or initiatives in support of the principal security plan (or its equivalent).

The organisation has to use the ISM Measurements that will provide its position relative to an achievable target goal in its path towards solidity in its policies and procedures or in the deployment of any new security project or initiative.

6.2. The ISM Measurement in the Plan Phase

This continuous cycle requires, initially, a planning phase where the ISM measurements generic premises are established, a selection of information security measures chosen, their categorisation, definition and specification (name, objective, owner, etc.) defined, the identification of the sources, the assignment of resources and documentation established. This planning phase guarantees that the environment and context of the measurements process has been correctly established.

An organisation should base its planning of ISM Measurement (including the selection of information security measurements and information security indicators) on the following performance criteria:

- The requirements of interested parties;
- The full range of its activities, products and services;
- The organisational structure;
- The overall business strategy, goals and objectives ;
- The information security policy;
- The information needed to meet its legal and other requirements;
- The costs and benefits of the ISM measurements implemented;

Planning of ISM measurement should include identification of financial, human, and infrastructure (physical and tools) resources. It is management's responsibility to provide these resources to ensure proper implementation of information security measurement.

Depending on its capabilities and resources, the initial scope of an organisation's ISM measurements may be limited to those elements of its activities, products and services given highest priority by management. Over time, the initial scope of ISM measurements can be widened to address elements of an organisation's activities, products and services that have not been previously addressed.

The identification of an organisation's information security aspects is an important input in planning ISM measurements. This information typically is developed in the context of a risk management process. Examples of risk assessment methodologies are discussed in ISO/IEC 27005 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security). An organisation with ISMS in place should assess its ISM performance against its information security policy, objectives, targets and other information security performance criteria.

6.2.1. ISM Measurements validation criteria

A valid ISM Measurement should comply with the following criteria:

a) Strategic: Aligned to the Information Security strategy, and therefore aligned to mission requirements.
b) Quantitative: Numerical and empirical data rather than opinions.
c) Reasonable: The value of data collected should not exceed the cost of collection.
d) Verifiable: Third-party reviewers should be able to assess data and concur with result.
e) Trendable: Data should be meaningful over time to assess the impact of changes.
f) Useful: Results should support mission or financial decision-making.
g) Indivisible: Data should be collected at the most discrete, unanalyzed level possible.
h) Well-defined: Document characteristics like frequency, formula, evidence, and indicators.

6.2.2. Selection of ISM measurements

To select appropriate information security measures organizations should take the following steps:

a) Define an ISM measurements programme in terms of the characteristics of the business, the organisation, its location, assets and technology that takes into account business and legal or regulatory requirements, and contractual security obligations and has been approved by management.
b) Select control objectives and controls of the ISMS to be included in the ISM measurements programme.
c) Define the information security indicators for selected controls.

The information security indicator objectives and ISM measurements and the reasons for their selection should be documented in the Statement of Applicability.

6.2.3. Identifying the object under measurement

A detailed description of the object and a precise delimitation is needed. It is recommended that the number of interfaces on these objects is strictly limited.

An adequate size of business objects must be chosen. If business units are too big, results can be too vague. If they are too small, effort is considerably higher.

It should be identified and defined what it is desired to measure exactly. This definition shall include the following points the domain (scope) of the object under measurement and the attributes of the object that it is desired to measure.

Examples:

- Degree of risk (attribute) associated to an information system (object)
- Degree of implementation (attribute) of ISM measurements that an information system (object) must fulfil
- The evaluation level (attribute) of the security system of a product (object)
- The degree of implementation and effectiveness (attributes) of an Information Security Management System (object)
- The maturity level (attribute) of the processes (object) of an organization

6.2.4 Identifying the criteria

The criteria by which the object under measurement is to be measured shall be identified.

ISM measurements will result in a value that will represent a security attribute of the object, selected from a possible set of partially ordered values according to a measurement process

Example: the value average by means of mathematical expression: If we have a big dispersion, the average is not a significant value, e.g. the absolute value of the number of internal notifications of a bad software operation cannot give us a suitable information (are 2 notifications better than 20?) or ratios that can indicate controls that are beneficial but irrelevant.

The criteria by which the object under measurement is to be measured should be identified, in the same way as a yardstick is used to measure the length of an object.

ISM measurements will result in a value that will represent a security attribute of the object, selected from a possible set of partially ordered values according to a measurement process.

6.2.5. Identifying, selecting an documenting ISM measurements

There should be identified and selected the ISM measurement that satisfies the selected information needs. The Model described in Clause 5 can be used.

The selected measurements should reflect the priority of the information needs.

Selected measurements should be documented. An example of Format is described in Annex A:

a) Name: name, abbreviation and numerical code
b) Purpose
c) Type of purpose.
d) Scope or Domain
e) Measurement method
f) Scale
g) Roles (Person in charge)
h) Data gathering Method (the method of data collection).
i) Life cycle.
j) Criteria
k) Fields of Indicator (Decisions criteria) :
    1 Effects impact.

2 Causes of deviation: Positive values and targets.
3 Graphic indicator.

6.2.6. Document the implementation measures plan

Organizations should document their plan for implementing and using information security measurements in an Implementation Plan. The Implementation Plan should:

a) List the measurements to be collected and used, including specification (e.g., purpose, frequency, owners)
b) Define the steps for collection and analysis of measurements data
c) Identify reporting formats for each measurement
d) Define a cycle for refreshing the measurements to ensure their currency in relation to the ISMS.

7 Operation of ISM Measurements (ISMS do phase)

ISM Measurements must be fully integrated into and used by the ISMS, including:

a) Definition and documentation of roles and responsibilities regarding development, implementation, and maintenance of information security measurements within the context of ISMS
b) Policies and procedures defining the use of measurements within the organization, dissemination of the measurements information, auditing and review of the measurements process
c) Process for monitoring the measurements to evaluate their use
d) Process for phasing measurements out and adding new measurements to ensure that measurements evolve with the organization.

7.1. Define data collection, analysis, and reporting procedures

This activity consists of the following tasks:

a) Procedures for data collection, including storage and verification should be defined: The procedures should specify how data are to be collected, as well as how and where they will be stored. Data verification may be accomplished through an audit.
b) Procedures for data analysis and reporting of ISM measurements should be defined: The procedures should specify the data analysis method(s), the frequency and format and methods for reporting the information products. The range of tools that would be needed to perform the data analysis should be identified

7.2. Review, approve, and provide resources for measurement tasks

The Do phase is the one that establishes the ensemble of selected ISM Measurements that result in adequate coverage for an organization at a given moment.

In this phase the results of measurement programme should be reviewed and approved. The results of measurement planning include the data collection procedures, storage, analysis and reporting procedures, evaluation criteria, schedules and responsibilities. Measurement planning should take into consideration improvements and updates proposed from previous measurement cycles.

Resources should be made available for implementing the planned measurement tasks. Management should agreed to ISM measurement planning and allocate appropriate financial and infrastructure resources.

Available supporting technologies should be evaluated and appropriate ones selected. Supporting technology may consist of, for example, automated tools and training courses. The types of automated tools that may be needed include graphical presentation tools, data analysis tools, and databases.

The selected supporting technologies should be acquired and deployed. If the supporting technologies concern the infrastructure for data management, then access rights to the data should be implemented in accordance with organisational security policies.

8 Improvement of ISM measurements (ISMS check & act phases)

The phases Check and Act facilitate the amelioration and reinforcement of all the ISM measurements processes and allow the analysis of the information, making available a help in the decision making with the end of attacking the causes. The ISM measurements must be evaluated, adjusted to the detected needs and assuring their evolution for covering the new needs of the variations over the initial positions at the start.

The organisations should identify the frequency of these phases, plan the time periods planned for the periodical revisions and establish the mechanisms for making possible the reactive or automatic revisions facing deviations over the initial or environmental conditions.

The following points should be followed:

8.1 Define criteria for evaluating the information and the measurement process

1. Criteria for evaluating information should be defined (Information analysis).
    a. The measurement analyst(s) should be able to draw some initial conclusions based on the results. However, since the analyst(s) may not be directly involved in the technical and management processes, such conclusions need to be reviewed by other stakeholders as well.
    b. All interpretations should take into account the context of the measurements.
    c. The data analysis results, measures, and interpretations should conform to the ISM Measurement Programme.

2. Criteria for evaluating the measurement process should be defined (ISM measurements validation). ISM measurements validation verifies that the measurements established are useful and cost-effective. In order to achieve this, the utility of the results achieved and the cost to obtain them should be compared with the objectives for which the ISM measurements were developed as initially projected. The result of the validation should yield a clear idea about the ideal character of the chosen ISM measurements or about their modification or substitution. Criteria to validate an ISM measurements Programme are:
    a. An ISM measurements Programme is valid when it gives relevant information for the Organization that can be acted upon.
    b. An ISM measurements Programme is useful when action/s or measure/s triggered off by the result are carried out.
    c. An ISM measurements Programme is efficient when cost to obtain it is not higher than the benefit obtained by the action/s or measure/s triggered off.
    d. An ISM measurements Programme is valid, if sources and the rest of aspects, linked with its attributes, are correct.

8.2 Monitor and maintain the measurement.

Measurements should be revised when organisational change occurs. To assure that measurement results reflect the actual security status, it is important to check whether underlying data is still valid. Thus it should regularly be checked for example whether there are changes in the inventory of hardware or software or changes in the context of the organization.

8.3 Review ISM measurements at planned intervals.

Review is necessary to check whether ISM Measurements are executed as planned. Organizations should evaluate the ISM measurement efforts after the initial implementation, after significant changes within the programme or in a set of used measurements, and at least annually.
The purpose of these evaluations is to asses results of the measurement and evaluate the adequacy and appropriateness of each measurement.

External evaluations are also recommended to provide an independent third party assessment of the programme. Organizations should determine appropriate timing of the external evaluations to ensure that they do not heavily interfere with programme operations.

Management should conduct review of all used measurements at least annually, after the initial implementation, and when significant changes occur in the underlying system or the set of corresponding business objectives. Final results (not drafts) should be assessed. The purpose of such review is to ensure that:

1. The measurements are appropriately revised when business objectives change
2. Measurements that are no longer useful are phased out and appropriate new measurements are phased in
3. Adequate resources are allocated to support ISM measurement.
4. Management decisions should be documented to allow for comparisons and trend analysis during the subsequent reviews.

8.4 Implement modifications

ISM measurement should be modified if significant changes occur within the organization or its business or operating environment. While many conditions may precipitate this need, the following is the most likely conditions when organizations must re-evaluate and modify current ISM measurement:

Changes in business objectives
Changes in threats and vulnerabilities environment
Availability of more refined or suitable data for measurement increases

Management should ensure that the modifications are implemented as planned. Organizations should apply project management techniques and document planned and accomplished improvements.

8.5. Communicate results of the measurement

Measurements should be distributed to internal stakeholders, including head of organization, managers, security officers, and other interested parties. Reporting structure, specific measurements to be provided, and the type of presentation should be tailored to the needs of each group.

On the one hand, the members of the organization must have access to the information that the ISM measurements supply (accordingly to their need to know and to the authorisation that they have). On the other hand, they must be aware of the importance of the information security indicators within the management framework. Appropriate and timely communication supplies the information from the people responsible for decision making processes, to the experts within the entities that are being measured and to those responsible for evaluating the correctness of the information security indicators or their use within the entities being measured.

Those responsible for the active use of ISM measurements, together with those responsible for the communications of the information security measurement, must ensure that there exist the definition, establishment and maintenance of the objective public list for the information security measurement, as well as of the processes and procedures of its communication, awareness and training.

It is necessary to implement communication, awareness and training programs

- The information products should be documented. Example form for reporting ISM measurements are provided in Annex A.
- The information products should be communicated to the measurement users. The information products should be made available to the data providers, and other stakeholders.

Measurements should also be distributed to external stakeholders, including regulatory bodies, shareholders, customers, and suppliers. External reports should be not as detailed as internal reports and only appropriate data should be reported. External reports should be reviewed by management and other appropriate parties within the organization before being released. External auditing of results may facilitate establishment of trust in the quality and correctness of data by external

stakeholders. It is important to properly communicate changes in security environment and posture which can be facilitated through ISM measures reporting.

Feedback should be provided to the stakeholders, as well as being sought from the stakeholders. This ensures useful input for evaluating the information products and the measurement process.

9 Management commitment

Management should establish and sustain measurement commitment. In implementing a measurement process in compliance with this International Standard, the Management should:

a) Accept the requirements for measurement. This activity consists of the following tasks:
    1. Define the objective and boundaries of the ISM Measurements in terms of the characteristics of the business, the organization, its location, assets, technology, and including details of and justification for any exclusion from the scope. This may be a single security control, a process, a system, a functional area, the whole enterprise, a single site, or a multi-site organisation. Information needs for measurement should be identified. Information needs originate from the technical and management processes and are based on:
        - goals,
        - constraints,
        - risks, and
        - organization problems
    2. The information needs may be derived from the business information security, organisational, regulatory (such as legal or governmental), control objectives and controls for the treatment of risks, and/or project objectives. The identified information needs should be:
        - Prioritised.
        - Selected, and
        - Documented and communicated.

b) Management and staff commitment to measurement should be established: The organization should demonstrate its commitment through, for example, a measurement policy for the organization, allocation of responsibility and duties, training, and the allocation of budget and other resources.

c) Commitment should be communicated to the organization: This can be achieved, for example, through organisational announcements or internal corporate web.

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISM Measurements Programme by:

a) establishing an ISM Measurements Programme;
b) ensuring that ISM Measurements Plan is implemented;
c) establishing roles and responsibilities for ISM Measurements Programme;
d) communicating to internal and external stakeholders the ISM Measurements Programme and the indicator achievement.
e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISM Measurements Programme;
f) ensuring that internal ISM Measurements Programme audits as a part of the ISMS audits are conducted; and
g) conducting management reviews of the ISM Measurements Programme as a part of the ISMS

9.1 Resource management

Management should assign and provide resources to support ISM measurements, including individuals responsible for all aspects of ISM measurement and appropriate financial and infrastructure support for supporting essential functions of the ISM measurement, such as data collection, analysis, storage, reporting, and distribution.

9.1.1 Provision of resources

The organization shall determine and provide the resources needed to:

a) to support ISM measurement collection, analysis, reporting, and information distribution, including process changes, automated tools, databases, or data storage
b) establish, implement, operate, monitor, review, maintain and improve an ISM Measurements Programme as a part of the ISMS;
c) ensure that ISM Measurements Programme support the business requirements;
d) identify and address legal and regulatory requirements and contractual security obligations;
e) maintain adequate security by correct application of all implemented measurements;
f) carry out reviews when necessary, and to react appropriately to the results of these reviews; and
g) where required, improve the effectiveness of the ISM Measurements Programme;

9.2.2 Training, awareness and competence

The Management should assign the following roles and responsibilities for executing and using ISM measures:

a) the owner of the measurement
b) the person or organizational unit responsible for requesting the ISM measurement
c) the person or organizational unit responsible for collecting and storing the information attributes of an entity's object of measurement.
d) The person or organizational unit responsible for communicating the ISM measurement importance and results throughout the organization to ensure its acceptance and use
e) The person or organizational unit responsible for evaluating ISM measurement to verify that it is providing adequate measurement of corresponding security controls.
f) the persons to whom the ISM measurement information is addressed. It's important to involve all of them in the definition and implementation of the ISM measurements programme and attempt to achieve everybody's consensus.

It will be necessary to establish authorisations, certifications or accreditations for personnel carrying out the measurement or design of the ISM measurements programme for a certain object, the criteria for their technical training, and their requirements in terms of independence, if any.

Management may want to establish ISM measurements for the entire enterprise to assess effectiveness of security training or the measurement processes themselves. In that case, the organization itself becomes the object under measurement.

Management should also identify the beneficiaries/recipients of the information produced by the ISM measurements. Support of these individuals is key to the success of the ISM measurement.

Examples of beneficiaries include

- The users of the security products
- The persons in charge of information systems
- The persons in charge of information security

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISM Measurements Programme are competent to perform the required tasks by:

a) determining the necessary competencies for personnel performing work affecting the ISM Measurements;
b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;
c) evaluating the effectiveness of the actions taken; and
d) maintaining records of education, training, skills, experience and qualifications.

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their ISM Measurements Programme and how they contribute to the achievement of the ISMS objectives.

Bibliography

ISO/IEC 27002:2005, Information technology – Security Techniques - Code of Practice for Information Security Management

ISO/IEC 15939:2002 Software engineering — Software measurement process

NIST Special Publication 800-55, Security Measurements Guide for Information Technology Systems, July 2003

ISO/IEC 27000: 200?? Information Security Management – Principles [including concepts and models] and Vocabulary

ISO/IECE 27005:200? Information security risk management

ISO/TR 10017, Guidance on statistical techniques for ISO 9001:2000

ISO 9001:2000, Quality management systems - Requirements.

ISO/IEC TR 17792, A framework for security evaluation and testing of bio indicator technology (assuming that it is completed before this proposed standard is completed).

ISO/IEC 18028-2, Information technology – Security techniques - IT Network security – Part 2: Network security architecture (Joint text with ITU-T Recommendation X.805)

ITU-T Recommendation X.805 - Security architecture for systems providing end-to-end communications.

ITU-T Recommendation X.1051 - Information Security Management System - Requirements for Telecommunications (ISMS-T)

Annex A
(Informative)

Formats of Information Security Metric

A.1 Format for information security indicators

Measurement	Metric name.	
Value.	Defines the quantity measured as percentage, number, frequency, coefficient, difference, or in other similar terms.	
Abbreviation.	Expresses the label or abbreviation that will identify the metric.	
Numerical code.	Identifies the metric through a code, making simpler reference to it possible.	
Subject.	Classifies the control metric (implementation, effectiveness,	
Purpose of Indicator.	Defines the purpose of the indicator.	
Target public of the indicator.	Defines the target public to which the metric information is addressed.	
Measurement Method.	Defines the method used in measurement, the calculation function or the analysis model.	
Scale.	Defines the metric scale (Nominal, Ordinal, Interval, Ratio).	
Data-gathering Procedure.	Defines the data-gathering method used in the metric (In the case of indirect metrics, the data-gathering methods used in the basic metrics)	
Persons in Charge (AGENTS)	**Information owner.**	Person owning this metric (active).
	Petitioner.	Person or organizational unit responsible for requiring the metric (in the case of basic metrics), or in the case of indirect metrics, the basic metrics comprising it.
	Input.	Person or organizational unit responsible for gathering, recording and storing the information about the attributes of the entities being subjected to measurement.
	Communication.	Person or organizational unit responsible for disseminating the metrics.
	Revision.	Person or organizational unit responsible for using the metric evaluation criteria in order to verify that it is appropriate for the measurement of the security control.
Life cycle.	**Frequency of obtention.**	Defines the time period for data-gathering.
	Periodicity of input.	Defines the periodicity with which data is recorded.
	Obtention date.	Date the data was obtained (day of the week, month, year, ...)
	Metric valid up to.	Date of expiry or renovation of metric validity.
Criteria:	Defines the criteria.	
Scope or Domain	Defines the scope or domain about which data is being collected (a specific machine, a service, a group of resources, a network, a building, a department or group, a business unit, etc...).	

Remarks	Describes the observations that the organization or owner of the information may want on record.

A.2 Format for information security indicator

Indicator extensions	Effects/impact	Definition of the effects and impact derived as a consequence of the results obtained by the indicator
	Causes of deviation	Definition of possible causes that may originate deviations in the results obtained
	Positive values	It is specified whether increasing values indicate positive values (good result) or whether decreasing values are to be taken to indicate positive values
	Targets	The range of values associated to pre-established targets is defined (fulfilled, sufficient, insufficient, etc.)
	Graphic indicator	Graphic representation of results (gauge meter, traffic light, colour code etc.)

Annex B (Informative) Examples of Security Metrics and related ISO/IEC 17799 controls

ISMM	SUBJECT	PURPOSE	MEASUREMENT CRITERIA	VALUE
Budgetary Ratio	ISO 17799 Control 6.1.1. Efficiency Metric	Obtain the ratio between IT Security Investment and IT Investment.	E-BR = ITSB * 100 / ITB ITSB = Amount of money spent (HW, SW, Services, Human Resource, etc.) in IT Security ITB = Amount of money spent (HW, SW, Services, Human Resource, etc.) in IT	Percentage
Information Security Personnel	ISO 17799 Control 6.1.3. Effectiveness Metric	Obtain the ratio between IT Security Personnel effort and IT Personnel effort.	F-PR = (ITSP / ITP) * 100 ITSP = Personnel (hours per man) working in IT Security ITB = Personnel (hours per man) working in IT	Percentage
Percentage of Co-workers who have Received Training and Qualifications In Security	ISO / IEC 17799 Control 8.2.2 implementation metric.	To show the percentage of co-workers with training and qualifications in security so as to ensure consciousness of the threats and risks in the field of security.	Calculation function, expressed by the formula: I-%CFES = (TCFES / TC) X 100 TCFES = ∑co-workers who have received training in security. TC = Total no. of co-workers	Percentage
Effectiveness of the Security Training Programme	ISO / IEC 17799 Control 8.2.2 Effectiveness metric	To establish the effectiveness of the Security Training Programme as per the number of security incidents caused by lack of training / awareness.	Calculation function, expressed by the formula: F-PFS = (IPF / TIS) X 100 In which: IPF = ∑ Security incidents caused by lack of training. TIS = Total no. of security incidents.	Percentage
Percentage of IS Protected from Malware	ISO / IEC 17799 Control 10.4.1 Implementatio metric.	IT Protected from malicious code	I-%SPSM = (TSP / TSA) X 100 TSP = ∑ ISystems protected from malware. TSA = Total number of systems threatened by malicious software	Percentage
Effectiveness of Protection System Upgrades Against Malicious Software	ISO / IEC 17799 Control 10.4.1 Effectiveness metric.	To show the evolution of upgrading time for all the elements involved in the anti-malware protection system.	Calculation function, expressed by the formula: F-TASPSM = MA - MP In which: MA = The moment (date/ hour/ minute) in which the protected systems are upgraded. MP = The moment (date/ hour/ minute) in which the upgrade was published.	Number
Effectiveness of Protection System Against Malicious Software	ISO / IEC 17799 Control 10.4.1 Effectiveness metric.	To show the effectiveness of the protection system against malicious software.	Calculation function, expressed by the formula: F-SPSM = (ISM / EBSM) * 100 In which: ISM = ∑ of security incidents due to malicious software. EBSM = ∑ of malicious software events detected and blocked	Coefficient

ISMM	SUBJECT	PURPOSE	MEASUREMENT CRITERIA	VALUE
Ratio of PCs with Firewall Software Protection	ISO 17799 Control 12.6.1. Implementation Metric	To measure firewall implementation level	I-RPFSP=100*PCs with firewall/total Pcs	Percentage
Ratio of computer Servers with Firewall Software Protection	ISO 17799 Control 12.6.1. Implementation Metric	To measure firewall implementation level	I-RSFSP=100*Servers with firewall/total servers	Percentage
Ratio of PCs with Antispam Protection	ISO 17799 Control 10.8.4. Implementation Metric	To measure antispam measures implementation level	I-RPAP=100*PCs with antispam/total PCs	Percentage
Ratio of computer Servers with Antispam Protection	ISO 17799 Control 10.8.4. Implementation Metric	To measure antispam measures implementation level	I-RSAP=100*Servers with antispam/total Servers	Percentage
Ratio of PCs with Spyware Protection	ISO 17799 Control 15.1.4. Implementation Metric	To measure spywareP implementation level	I-RPSP=100*PCs with spywareP/total PCs	Percentage
Ratio of computer Servers with Spyware Protection	ISO 17799 Control 15.1.4. Implementation Metric	To measure spywareP implementation level	I-RSSP=100*Servers with spywareP/total Servers	Percentage
Ratio of PCs with Intrusion Attack Software Protection	ISO 17799 Control 12.6.1. Implementation Metric	To measure anti-intrusions sw implementation level	I-RPIASP=100*PCs atack sw P/total PCs	Percentage
Ratio of computer Servers with Intrusion Attack Software Protection	ISO 17799 Control 12.6.1. Implementation Metric	To measure anti-intrusions sw implementation level	I-RSIASP=100*Servers atack sw P/total Servers	Percentage
Effectiveness of number of information security incidents	ISO 17799 Control 13.1.1. Effectiveness Metric1	Obtain the number of reported incidents for a concrete domain/scope	E-NISI = NISI In which: NISI = Σ of information security incidents reported in the domain	Number
Ratio of Information Security Incidents per User	ISO 17799 Control 13.1.2. Implementation Metric	To show the proportion between the total number of information security incidents and the total number of information systems users in the organization. This ratio should also be determined for each category of incident.	I-RISIU=security incidents/users per domain	Percentage

ISMM	SUBJECT	PURPOSE	MEASUREMENT CRITERIA	VALUE
Unavailability Ratio of Information Services	ISO 17799 Control 14.1.1 Effectiveness Metric	Obtain the availability of the information services in a concrete domain	E-ARIS = min (ARIS(1) ,…, ARIS(i), …, ARIS(n)) In which: ARIS(i) = (Total_time_available(i) – Total_time_unavailable(i)) / Total_time(i) ARIS(i): Availability ratio of the "i" system that belongs to the evaluated domain	Percentage
Access Credential Reactivation Ratio	ISO 17799 Control 11.2.3.F-1	Efficiency of access credential reactivation ratio	F-ACRR = NRA / NUSR In which: NRA: Number or reactivations NUSR: Number of users of the system	Coefficient
Ratio of Information Systems with Contingency Plans	ISO 17799 Control 14.1.1. Effectiveness Metric	Information System contingency plan implantation ratio	I-ISCP = NISCP / NIS In which: NISCP: Number of Information Systems with the global contingency plan for a domain NIS: Number of information Systems in the domain	Percentage
Back-up Frecuency Ratio	ISO 17799 Control 10.5.1.I-1. Implementation Metric	Identify the backup frequency ratio for a domain	I-ISBKP = NISBKP / NIS In which: NISBKP: Number of Information Systems with backup NIS: Number of information Systems	Percentage

Annex C
(informative)

Specific measurement techniques

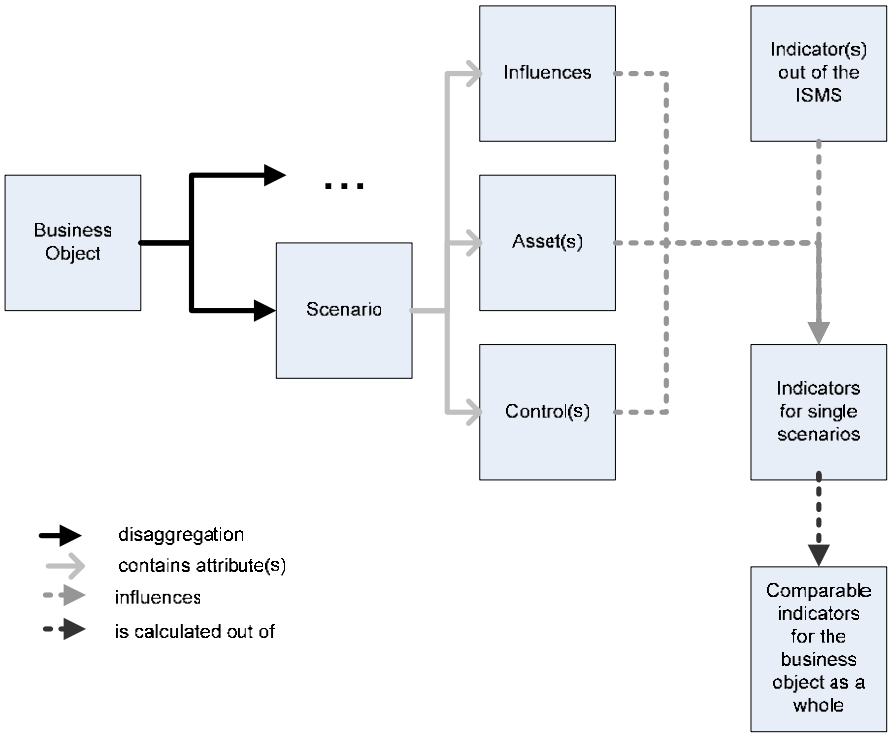
C.1 Metric for Information Security in an organization based on assessment of scenarios

Metric for IT-security in an organization provides an objective and comprehensive indicator for the state of organization's security. It is based on scenario technique and allows modelling the organization's context. It is applicable to both, big and small organizations and provides useful results for responsible persons.
The metric requires that a working ISMS (Information Security Management System) is available to the system to assess.

C.1.1 Foundation of the metric

C.1.1.1 General metric structure

The metric is based on assessment of scenarios. Scenarios, which are known from risk assessments, are situations that can possibly happen; they consist of threats, vulnerabilities and consequences. For assessment, all scenarios possibly occurring are listed; afterwards their (negative) influence on the business object is written down. Security of a system can be assessed as soon as there are enough details to list all scenarios and to assess consequences of these scenarios.
After all scenarios are rated, combination of ratings to indicators for the security of the whole organization is carried out, following defined rules. Resulting indicators are comparable between organizations, as it will be described in the following.
Before, a diagram should summarize the structure of the metric:



C.1.1.2 Definition of Information Security

The best way to provide comparable indicators for security is alignment with the intuitive understanding of security. Intuitive security can be expressed in two statements:

- If two organizations possess the same set of assets, but organization A looses more assets than organization B, organization B is intended to be more secure.
- If organization A posses more assets as organization B and both loose the same amount of assets, organization A is intended to be more secure than organization B.

One can conclude out of these statements, that an organization is less secure if the percentage of assets lost is bigger. Thus the formula

S = 100% – [percentage of assets lost]

is a good indicator for security, expressing actual security as a percentage of total security.

Instead of assets themselves, the monetary value of assets must be taken into consideration, as different types of assets can not be summarized otherwise.

C.1.1.3 Dimensions of Information Security

One single indicator for information security is not sufficient as different aspects of security must be regarded.
There are three aspects of security – so called dimensions – which are widely accepted:

- Availability
- Confidentiality
- Integrity

Security is measured against these three dimensions. In some cases, financial resources of the incidents mainly direct to financial consequences, for example if standard hardware is lost. Including these consequences into one or more of the three dimensions mentioned will cause wrong values; thus an additional dimension, “financial resources”, is needed.
It is possible that consequences affect more than one of these four dimensions.
These four dimensions are totally different in nature; no one can claim to be the main dimension of security. Thus indicators for the four dimensions are calculated separately.
Note: Although other criteria might be taken into account, only these four dimensions will be used for the metric of information security.
Besides, extension of the metric to other dimensions would not pose a problem at the concept level. But comparability will suffer from it and it would produce higher amount of work. Thus it is highly recommended to restrict measurement to these four dimensions.

C.1.1.4 Foundation of assessment

Assessment is conducted in scenarios. All scenarios must be considered, even if they are not likely to happen.
Consequences are evaluated in scenarios of medium severity. If there is a huge difference between high and small severity or if different values of assets must be applied (especially for availability), one scenario should be split to different scenarios for the different severities or values of assets.
If a scenario is split into some others, it is necessary, that all incidents of the original scenario can clearly be assigned to one of the new scenarios to preserve independence. The original scenario must be removed from the set of scenarios.

C.1.2 Initial step

C.1.2.1 Policies for assessment

The metric contains detailed procedures on how one can assess scenarios and how one can combine them. However, it does not explain in detail how one can organize assessments. Having no direct impact on the results of the metric, it still has indirect influence if disregarded. Thus, some organizational requirements have to be fulfilled. Clauses provided here are abstract descriptions of the important needs. They must be refined in organizational specific manner and documented in a policy. The following organizational requirements have to be fulfilled:

- There must be an employee responsible for assessment meetings.
- At least one security officer, one representative of the management, one employee responsible for defence of the discussed scenario(s), and one employee directly affected by the consequences of the scenario must be present during assessment meetings.
- Results of assessment meetings must be documented.

C.1.2.2 Information for identification and assessment of scenarios

For a sound identification and assessment of scenarios, internal and external data of attacks, losses etc. are useful. Useful information can be found in external documents like

- Articles of specialist journals
- Research documents like proceedings, theses etc.
- Documents from market research
- Statistics from insurances and other organizations

Of special interest are internal documents and datasets like

- Documents about internal knowledge regarding security
- Plans of infrastructure
- Lists of inventory
- Results of risk assessment
- Results from penetration testing
- Results from system monitoring
- Indicators already used in the ISMS and metric results of the NIST 800-55 [Swanson2003] metrics guide

It must be assured that information stems from reliable sources and that it can be applied to the business objects or scenarios to assess. Special effort must be laid upon comparison of delimitations between values needed and values available. If there is not enough information or there is doubt about correctness, experts should be consulted.
In case of internal statistics, it should be assured by experts that data gathering is complete.

C.1.2.3 Identification of scenarios

This clause provides a preliminary list of scenarios. This list can be used as a first step for identification of scenarios. If risk assessment is already conducted, scenarios may be taken over, but it is highly recommended to adapt scenarios to the preliminary list to maintain good comparability.
Selection of relevant scenarios from the preliminary list is the first step of scenario identification. It should align with the following rules:

- Each scenario exposing a potential risk to the organization is relevant.
- Existing controls may not yet be included in the estimation of risk at this step.
- Organizational aspects or context, regarding location and high/low exposure to attacks should be regarded.
- Scenarios leading to a low damage or impact are less important than scenarios leading to a big damage or impact.

Summarizing rules in one statement, all scenarios are relevant, which can occur if all controls fail, but the context of the organization (products to sell, location etc.) stays the same.

The next step is **identification of additional scenarios**. Additional scenarios are needed to model organization-specific aspects, not yet included in the preliminary list. It can not be said for sure that additional scenarios are needed, but it is at least necessary to check absence of additional scenarios. After identification, relevance of additional scenarios should be checked with criteria stated above, too.

The last and optional step of identification of scenarios is **summarization and/or refinement of scenarios**.
It is very important that the resulting set of scenarios fulfils the following requirements:
a) It is complete, meaning that all possible scenarios are mentioned.

b) Incidents belonging to different scenarios occur pair wise independent. If no overlapping scenarios are identified (that means that no incident can belong to two different scenarios), there is usually no reason for doubt about fulfilment of this requirement.
Note: Independence is requested for the occurrence of incidents, not the rate of incidents. Thus if two different scenarios refer to the same vulnerability, they are still independent. Changes in the environmental conditions solely lead to changes in probability and scenarios stay still independent.

c) Scenarios contain enough details to be used for assessment of the mean time between two incidents and the consequences. If they do not, refinement is necessary. The influence of controls on the scenario can be modelled.

d) Scenarios must be well-defined, meaning that clearly defined borders are available and that a scenario is separable from other scenarios.

The following operations on the set of scenarios can be executed to fulfil these requirements:

- **Combination of scenarios**: This operation is useful, if scenarios exist which are not very important. Two scenarios may be combined if their consequences are similar. If there are two scenarios with both having small influence or both having big influence, they may be combined. However, combining a scenario of big severity with a scenario of small severity is not allowed.
- **Split scenarios:** If it is difficult to assess scenarios (e.g. very big difference between "small" and "big" occurrences of the scenario), splitting scenarios is compulsory. Additionally it may be applied if scenarios are very important to get a more detailed assessment.

In some cases it may be useful to combine different scenarios and split them afterwards (in another direction).

If scenarios were already assessed, certain rules should be regarded during combination and splitting of scenarios. Details about that are described in clause

C.1.2.4 Financial values of assets in the four dimensions

The financial values of assets are needed at two places: During calculation of the sum of assets and during assessment of loss. Especially if more than one person is involved in assessment, it is necessary to document the financial values that they do not differ.

Financial values of assets are assessed in the four dimensions availability, confidentiality, integrity, and financial resources. An asset is assigned four possibly different values, one for each dimension.

Wherever possible, supporting material like market or purchase prices should be used to provide a reliable assessment.

As aspects assessed in the four dimensions are totally different, also assessment will differ in the four dimensions:

- **Availability**: The financial value of availability for one hour is calculated by

$$\frac{\textit{financial consequences due to loss of availability in a typical incident}}{\textit{duration of a typical incident (in hours)}}$$

- **Confidentiality**: The financial value of confidentiality of one dataset is calculated by

$$\frac{\textit{financial consequences due to loss of confidentiality in a typical incident}}{\textit{duration of a typical incident (in hours)}}$$

All consequences like punishment, reputation, lost orders etc. must be regarded.

- **Integrity**: The financial value of integrity of one dataset is calculated by

$$\frac{\textit{financial consequences due to loss of integrity in a typical incident}}{\textit{duration of a typical incident (in hours)}}$$

All consequences like punishment, reputation, lost orders etc. must be regarded.

- **Financial resources**: In opposite to the other dimensions, values are rather objective. An asset must be assigned the price, which has to be paid for repair or replacement with a product of the same quality and performance. Either administrative work like installation, testing, and special circumstances and quick ordering must be regarded. If no other values are available, values out of the balance sheets can be used.

Deviations from normal values must be documented and explained.
If an asset is very import or is difficult to assess (for example the availability to operate), management decision is useful.

C.1.2.5 Assess sum of assets

The sum of assets is calculated per business object and per dimension (availability, confidentiality, integrity and financial resources). All assets belonging to one business object have to be listed and the values of the assets have to be summarized. Assets belonging to the given business object but sourced out to other business objects must also be included. If there is doubt whether an asset does belong to a business object, the boundary of the business object should be refined. If uncertainty remains, the decision for one – if available the likely – direction is taken. This decision must be documented.
There may be different values of one asset in one dimension – because scenarios are split. In this case only the biggest value may be taken.
It is very important that values used here do not differ to values used in assessment of loss. Because of that, values calculated in assessment of loss must be used.
The results of this step must be documented for each business object.

C.1.3 Assessment of scenarios

The basis for the metric is the adequate assessment of loss of assets in scenarios. Every scenario has to be assessed with the rules stated in this clause.

C.1.3.1 Assessment of scenarios in general

Assessment is carried out on single scenarios. The following values are assessed:

- **Number of occurrences of the scenario**: This value can be calculated out of the (assessed) time between two incidents by 1 / [time between incidents].
- **Consequences due to loss of availability**: This value describes the monetary consequences regarding availability, which are likely to occur in a scenario of medium severity. If big differences between severities of the scenario occur, the scenario should be refined, each scenario describing a different severity of consequences.
- **Consequences due to loss of confidentiality**: Same as the consequences due to loss of availability but for confidentiality.
- **Consequences due to loss of integrity**: Same as the consequences due to loss of availability but for integrity.
- **Consequences on financial resources**: Same as the consequences due to loss of availability but for financial resources.

For assessment the following steps have to be performed:

- **Possible consequences** (not for the number of occurrences of the scenario): All possibly affected assets should be listed. Data support and use of expert knowledge should be gained wherever possible.
- **Controls involved**: All controls possibly influencing the scenario should be listed. Additionally the quality of the controls and the performance of the ISMS should be documented. As in the step before, data support and use of expert knowledge should be gained wherever possible.
- **Assessment**: In this step, the actual combination of influences for one scenario is performed. Data support and use of expert knowledge should be gained wherever possible. The following steps should be executed for assessment:
    a. **Gather all available data** necessary for a founded assessment of the scenario. Especially internal data sources mentioned in clause C.x.x.x [Editor's Note: add reference] should be regarded.
    It is useful to search for reliable figures on scenarios at least similar to the actual scenario, which can be taken as basis for assessment.

b. **Describe all controls involved**, its quality and its influence on the scenario as a whole. Especially operability and performance of ISMS must be described.
c. **Model influence of (additional) controls** by giving mathematical formulas for calculation or a precise value. If reliable figures were found during gathering of data, these figures should be taken, and additional or missing context should be modelled. Especially if no reliable figures are available, experts should be consulted. To provide figures of maximum confidence, a constellation easy to assess should be taken; additional or missing context or controls should be modelled.

Context which leads to a higher or lower number of occurrences or damages is described and modelled in the given values. The result of this step is a detailed description, giving numbers for calculation and formulas for combination.

- **Final value**: The final value for the number of occurrences and the four final values for the consequences are the result of assessment of the scenario. They are calculated out of the documented results in the step before.

It is important, to include solely consequences directed to the given scenario. If assets can be lost due to other reasons, this may not be regarded in this scenario.

C.1.3.2 Splitting and refinement of scenarios

If it becomes evident that scenarios must be split or should be combined and there are already values for assessment available, special rules have to be applied.
If scenarios occur with rates λ_i, then the combined scenario occurs with rate

$$\lambda_t = \sum_i \lambda_i$$

The damage of the combined scenario is $d_t = \sum_i \frac{\lambda_i}{\lambda_t} \cdot d_i$ if single scenarios result in damages d_i (for each dimension of security).

The following rules have to be applied to split scenarios, if assessed values are already available:

- If the original scenario already was assigned a rate λ, then the following formula for split scenarios holds: $\lambda = \sum_i \lambda_i$
- If also a damage d was assigned, then the formula $\lambda \cdot d = \sum_i \lambda_i \cdot d_i$ holds additionally.

If it becomes evident that scenarios must be split or should be combined and there are already values for assessment available, special rules have to be applied.
If scenarios occur with rates λ_i, then the combined scenario occurs with rate

$$\lambda_t = \sum_i \lambda_i$$

The damage of the combined scenario is $d_t = \sum_i \frac{\lambda_i}{\lambda_t} \cdot d_i$ if single scenarios result in damages d_i (for each dimension of security).

The following rules have to be applied to split scenarios, if assessed values are already available:

- If the original scenario already was assigned a rate λ, then the following formula for split scenarios holds: $\lambda = \sum_i \lambda_i$
- If also a damage d was assigned, then the formula $\lambda \cdot d = \sum_i \lambda_i \cdot d_i$ holds additionally.

C.1.3.3 Use of indicators for assessment

Indicators, giving guidance on the efficiency of (usually single) controls, are used in the ISMS. NIST 800-55 [Swanson2003] gives guidance how one can develop such indicators and provides examples like

- Percentage of systems that have had risk levels reviewed by management.
- Percentage of total systems for which security controls have been tested and evaluated in the past year.
- The average time elapsed between vulnerability or weakness discovery and implementation of corrective action.
- Percentage of systems with automatic virus definition updates and automatic virus scanning.
- Percentage of systems that perform password policy verification.

In quite a lot of cases, these values can be used as input for a more detailed assessment of number of occurrences, consequences, or the quality of controls.
On the one hand there are indicators telling the quality of controls directly (e.g. percentage of systems that perform password policy verification). On the other hand there are indicators giving a hint for the quality of the controls (e.g. percentage of systems that have had risk levels reviewed by management).
Both values can be used during assessment – the first one usually providing more exact results.
Additionally data from monitoring of a system or control can be used. If it is guaranteed that all incidents belonging to a special type of incident are recorded, these values should be taken as they are intended to provide most exact results.

C.1.3.4 Making use of data from other assessments

The metric results of each business object can be used in other business objects to model the influence of other business objects or organizations. By that, either the hierarchical structure of an organization and outsourcing can be modelled. To achieve this, a scenario belonging to the main business object is assigned the results from the subordinate business object. By that, the behaviour of the underlying business object is summarized in one scenario.
The following aspects must be fulfilled if a subordinate business object is taken over into a scenario belonging to a main business object:

- **The scope must fit**: Functions used in the scenario of the main business object must be the same as functions assessed in the subordinate business object. This implies, that not only part of or more than functionality assessed in the subordinate business object is used.
- **Independence:** The subordinate business object, taken over into a scenario, must be independent from the other scenarios in the main business object like other scenarios, too. Talking about independent organizations at different locations, this will probably fit in most cases. Concerns about independence may be raised if two business objects of the same organization, located in the same building, and with quite similar work to perform should be combined. In these cases, it should be investigated whether independence may be assumed. The alternative is modelling the (two or more) business objects in one business object, uniting dependent scenarios.
- **Disjoint**: There is no overlapping in assets between the subordinate business object and the rest of the main business object.

Instead of the monetary consequences and the number of occurrences per year, the results of the metric in the subordinate business object are used. In addition the financial value of assets belonging to the business object under assessment but possibly affected in the subordinate business process, like

- All types of availability
- Data handed over to the subordinate business object

have to be listed together with their financial values.
Thus following values should be available when taking over results of a business object into a scenario:

- The metric results of the subordinate business object (for each dimension and for each threshold – for details see clause [Editor's Note: fix reference]
- Value G of assets belonging to the main business object, but used in the subordinate business object

More than one subordinate business process can be reused per business object (each modelled in an own scenario).

C.1.4 Assessment of business objects

C.1.4.1 Result of the metric

Values assessed for scenarios have to be combined to one value for the business object.
But taking only expectation of security as indicator will rain significance: It is a big difference whether a scenario is occurring quite often but having only limited financial consequences (and thus only having little impact on security), or whether a scenario is occurring very seldom, but likely to kill the organization when occurring (and thus having big impact on security when occurring). But taking the expectation of security can lead to equal results for both, as one can see on a provided example in "Additional information".
To model these differences, the following two indicators for security are calculated in addition to the expectation:

- Probability that at least a given security is reached (being equal to the probability that a given percentage of loss is not exceeded). This value is good for getting an impression about the expected distribution of security and is referred to as "likely security" in the following.
- Probability that no scenario occurs, which – on its own – leads to a security less than a given threshold (being equal to the probability that no scenario occurs with leads to a loss bigger than a given percentage of assets). This probability is good for determination whether there are very big risks and is referred to as "lowest security" in the following.

C.1.4.2 Calculation of expectation and likely security

It is known from probability calculus, that the Poisson-process can be used to describe occurrence of incidents during a given period. If the average number λ of occurrences per year is given, it is possible to calculate the probability, that there are exactly n occurrences in a year.
For calculation let be

- n the number of scenarios
- $S = \{i_1, i_2, \ldots i_n\}$ the set of all IDs of scenarios in the business object, which are not a surrogate for subordinate business processes.
- A_i, C_i, I_i, and F_i the resulting monetary consequences for availability, confidentiality, integrity, and financial resources for a given scenario i.
- λ_i the number of occurrences for a given scenario i (per year)

To make documentation of calculation easier, the following abbreviation is taken for a given dimension D:

$$B_i := \begin{cases} A_i & \text{if D = "availability"} \\ C_i & \text{if D = "confidentiality"} \\ I_i & \text{if D = "integrity"} \\ F_i & \text{if D = "financial resources"} \end{cases}$$

For a given dimension D and a calculated (financial) value T of the sum of assets for D, the following values are calculated:

- $\mu_S = 100\% - \frac{\mu}{T}$ with μ being the expectation

$$\mu = \sum_{i=1}^{n} B_i \cdot \lambda_i \quad (*)$$

- R_k = "probability that security is at least Q_k"
  where Q_k is out of Q = {
  99.99%, 99.95%, 99.9%, 99.5 %, 99%,
  97%, 95%, 93%, 85%, 90%,
  80%, 75%, 65%, 50%
  }
  The following inequation must be fulfilled for a given Q_k:

$$\sum_{i \varepsilon S} x_i \cdot B_i \leq T \cdot (100\% - Q_k) \qquad (*)$$

with x_i being the number of occurrences of scenario i.
As independence of scenarios can be assumed, a given set of occurrences $x_1, x_2, \ldots, x_n$ happens with the probability

$$r = \prod_{i \varepsilon S} Poisson(x_i; \lambda_i) = \prod_{i \varepsilon S} \frac{e^{-\lambda_i} \cdot \lambda_i^{x_i}}{x_i!}$$

Let be E the set of all tuples $t_e = (x_{1,e}, x_{2,e}, \ldots, x_{n,e})$ fulfilling (*).

Then R_k can be calculated by

$$R_k = \sum_{e \varepsilon E} r$$

And thus the result of R_k is:

$$R_k = \sum_{e \varepsilon E} \prod_{i \varepsilon S} \frac{e^{-\lambda_i} \cdot \lambda_i^{x_{i,e}}}{x_{i,e}!}$$

It is strongly recommended to automatism this calculation. As the number of scenarios is not fixed, recursive procedures are helpful. For efficient implementation it is necessary to check after every increase of a x_i, whether it is still possible to fulfil (*).
There is no matter of the order of scenarios. But it must be assured, that the financial consequence is not 0 for each scenario and dimension regarded. Additionally, it must be decided whether very small consequences should be left out in this calculation, as their contribution is low but calculation effort rises considerably.

C.1.4.3 Calculation of lowest security

The variables

- Q_k (thresholds)
- T (sum of assets in the dimension)
- B_i (financial consequences)

for a given dimension D are defined accordingly to clause C.x.x.x. [Editor's Note: fix reference]
Then the probability that no scenario occurs which leads to security less than Q_k on its own is:

$$V_k = \prod_{i,\ B_i > (100\% - Q_k) \cdot T} Poisson(0; \lambda_i) = \prod_{i,\ B_i > (100\% - Q_k) \cdot T} e^{-\lambda_i}$$

C.1.4.4 Use of results of subordinate business objects

For a business object taken over, the following values are provided for each dimension D and each threshold Q_k (see C.x.x.x): [Editor's Note: fix reference]

- Expectation μ_s of security
- Probability p_L that the likely security is not less than Q_k in the dimension D
- Probability p_M that no scenario occurs which – on its own – will lead to a security less than Q_k in the dimension D
- Value G of assets belonging to the main business object, used in the subordinate business object

Definitions of the variables used here align with definitions in clauses C.x.x.x and C.x.x.x [Editor's Note: fix reference]; additionally, S' is the set of all IDs of scenarios in the business object, which are a surrogate for a subordinate business process.
For a given threshold Q_k and dimension D the following formulas are used to calculate the indicators for the business object including the influence of the subordinate business objects:

- **For the expectation of security**:

$$\mu_s = 100\% - \frac{\sum_{i=1}^{n} B_i \cdot \lambda_i + \sum_{i \varepsilon S'} (100\% - \mu_{s,i}) \cdot G_i}{T}$$

- **For the likely security**:

$$R_k = \sum_{e \varepsilon E} \left[\prod_{i \varepsilon S} \frac{e^{-\lambda_i} \cdot \lambda_i^{x_{i,e}}}{x_{i,e}!} \cdot \prod_{i \varepsilon S'} p_{L,Q_i} \right]$$

For all tuples e = ($x_{1, \ldots} x_{n,} y_{1, \ldots} y_m$) with m being |S'| and y_i ε Q.

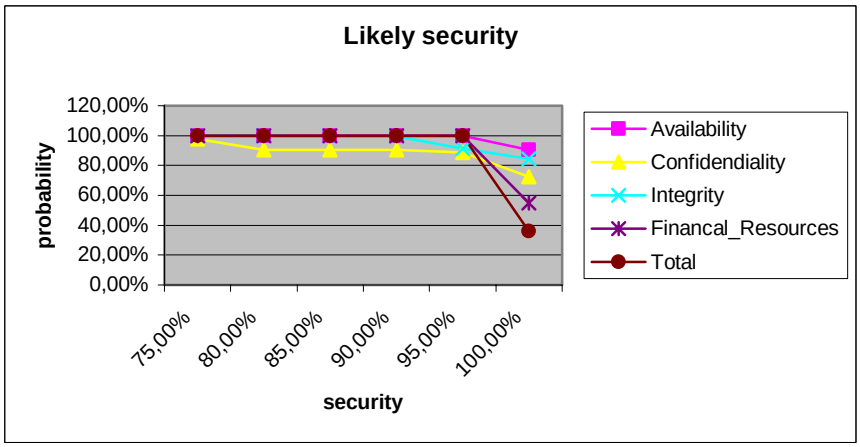
$$\sum_{i \varepsilon S} x_i \cdot B_i + \sum_{i \varepsilon S'} (100\% - y_i) \cdot G_i \leq T \cdot (100\% - Q_k)$$

- **For the lowest security**:

$$V_k = \prod_{i,\ B_i > (100\% - Q_k) \cdot T} e^{-\lambda_i} \cdot \prod_{i,(100\% - Q_r) \cdot G_i > (100\% - Q_k) \cdot T, Q_o = \max(Q_r)} p_{M,Q_o}$$

C.1.4.5 Graphical representation of results

The following diagram shows an example for the likely security:



C.1.4.6 Examples of Scenarios

This clause provides examples of possible scenarios that may be used for this technique. For each, scenario, the possible effects are also marked.

Table B.1 — Examples of Scenarios

	Effect / Scenario	Physical damage of building	Physical damage / loss of hardware	Physical damage of data	Logical damage of data => loss	Reduce / kill availability /	Loss of confidential-
1.	Fire	**YES**	**YES**	**YES**		**YES**	
2.	Power failure		**POSS.**		**POSS.**	**YES**	
3.	Inadmissible environmental conditions	**POSS.**	**POSS.**	**POSS.**		**YES**	
4.	Storm	**YES**	**YES**	**YES**		**YES**	
5.	Lightning	**YES**	**YES**	**YES**	**POSS.**	**YES**	
6.	Water	**YES**	**YES**	**YES**	**POSS.**	**YES**	
7.	Espionage						**YES**
8.	Unauthorized external access to systems, including digital vermin				**YES**	**YES**	**YES**
9.	(D)Dos, Spam					**YES**	
10.	Spoofing, Session-Hijacking, Probes, Scan						**YES**
11.	Phishing, Masquerade, Social Engineering						**YES**
12.	Internal attack over network				**YES**	**YES**	**YES**

	Effect Scenario	Physical damage of building	Physical damage / loss of hardware	Physical damage of data	Logical damage of data => loss	Reduce / kill availability /	Loss of confidential-
13.	Accidentally destruction or uncovering				**YES**		**YES**
14.	Fraud				**YES**		**YES**
15.	Sabotage	**POSS.**	**YES**	**YES**	**YES**	**YES**	**YES**
16.	Theft (physical)		**YES**				
17.	Vandalism	**POSS.**	**YES**	**YES**		**YES**	
18.	Disturbance of operation due to internal problems					**YES**	
19.	Unavailability of personnel and loss of personnel					**YES**	
20.	Loss of external connection (telephone and network)					**YES**	
21.	Loss of stored data due to technical error			**POSS.**	**POSS.**		