Committee Draft **ISO/IEC 1st CD 27005***	
Date: **2006-01-20**	Reference number: ISO/IEC JTC 1/SC 27 **N4801**
Supersedes document SC27 N4460	
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.	
ISO/IEC JTC 1/SC27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2006-04-20** Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.

ISO/IEC 1st CD 27005*

Title: Information technology — Security techniques — Information security risk management**

Project: 27005*

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
NWI Proposal (N3407) (aim: to create a multipart standard and change type from TR 13335-1/2 to IS 13335-1 and TR 13335-3 to IS 13335-2)	14th SC27 Plenary, October 2004, Resolution 10 (N3411)		Summary of voting (N3462) Text f. 1st WD (N3483)
1st WD (N3483)	15th SC27 Plenary, May 2003, Resolution 13 (N3624) 27th SC27/WG1 meeting, October 2003, Resolution 3 (SC27 N3394rev1)	Summary of NB comm. (N3551) Text of TR 13335-4 (N3694)	Disp. of comments (N3760); Text f. 2nd WD (N3759)
2nd WD (N3759)	16th SC27 Plenary, April 2004, Resolution 2 (N4035rev1)	NB contr. (N3995); Summary of NB comm. (N3880)	Disp. of comm. (N3952) Text f. 3rd WD (N3951)
3rd WD (N3951)	29th SC27/WG1 meeting, Oct. 2004, Resolution 3 (N4195rev1)	Summary of NB comm. (N4155)	Disp. of comm. (N4171) Text 4th WD (N4170)
4th WD (N4170)	17th SC27 Plenary Apr. 2005, Resolution 9 (N4599)	Summary of NB comm. (N4378)	Disp. of comm. (N4461) Text for 1st CD (N4460)
1st CD 13335-1* (N4460)	31st SC27/WG1 meeting, Nov. 2005, Resolution 7 (N4825ev1)	Summary of Voting comments (N4731ev2)	Disp. of comments (N4802); Text f. 1st CD 27005* (N4801)

CD Consideration

In accordance with resolution 7 (SC27 N4825ev1) of the 31st SC27/WG1 Plenary held in Kuala Lumpur, 2005-11-7/11, the attached document is hereby submitted for a 3-month CD letter ballot closing by

2006-04-20.

Medium: Livelink-server

No. of pages: 1 + 82

** subject to JTC 1 endorsement on the renumbering from ISO/IEC 13335-2 to ISO/IEC 27005 (SC 27/WG1 Kula Lumpur Resolution 6)*

*** subject to JTC 1 endorsement on the change of title (SC 27/WG1 Kula Lumpur Resolution 2)*

**** Once ISO/IEC 27005* is published, ISO/IEC TR 13335-3:1999 and ISO/IEC TR 13335-4:2001 will be withdrawn.*

Secretariat ISO/IEC JTC 1/SC 27 -DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10787 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.ni.din.de/sc27

ISO/IEC TC JTC1/SC 27 N 4801

Date: 2005-11-08

ISO/IEC 1st CD 27005

ISO/IEC TC JTC1/SC 27/WG 1

Secretariat: DIN

Information technology — Security techniques — Information security risk management

Élément introductif — Élément central — Partie 2: Titre de la partie

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

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 representative 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.

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

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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 ISO/IEC 27005 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 27005 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC27, *Security techniques*.

Introduction

Information security risk management as addressed in 27005 can be used to assess risks, identify security requirements and help to establish and maintain information security management system.

Information security is the protection of information necessary to achieve business objectives using all organizational, physical, technical and other resources, to allow a coordinated, coherent, effective, efficient and secure process.

There are many specific methodologies that have been developed to address the requirements for risk management in order to address the specific specializations or focus of some sectors and organizations.

This standard provides guidelines for information security management for an organization, and does not provide the specific methodologies for information security management. An organization should select risk management methodologies that are appropriate for the organization.

This International Standard is relevant to everybody within an organization, and, where appropriate, external parties who are responsible for the management and/or the implementation of information security.

Information technology — Security techniques — Information security risk management

1 Scope

This standard provides guidelines for information security risk management that includes information and communications technology security risk management.

The techniques described in this standard follow the general concept, models and processes specified in ISO/IEC 27001. These guidelines are designed to assist the satisfactory implementation of information security based on risk management approach.

Familiarity with the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of this standard.

This International Standard is applicable to all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations), which intends to manage risks that could compromise the organization's information security.

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 17799:2005, *Information technology — Security techniques — Code of practice for information* security management
ISO/IEC 27001:2005, *Information technology — Security techniques - Information security management systems — Requirements*

3 Definitions

For the purpose of this document, the terms and definitions given in Clause 3 of ISO/IEC 27001 and Clause 2 of ISO/IEC 27002 apply.

4 Background

The process of managing information security is based on the principles set out in ISO/IEC 27001.

The process can be applied to the whole organization as well as to selected parts of it. Information security management consists of all the activities to achieve and maintain appropriate levels of confidentiality, integrity, and availability. Non-repudiation, accountability, authenticity and reliability should be considered appropriately.

Information security management includes:

- security planning, implementing and monitoring,

- ensuring that security measures address requirements,
- ensuring that personnel, physical and information security are in line with objectives,
- ensuring that incidents are dealt with in accordance with the management framework,
- ensuring that personnel are educated, trained and aware of their responsibilities and roles regarding security,
- ensuring compliance with policies, standards and procedures, and
- audit and compliance checking of the security mechanisms and objectives.

A systematic approach to risk management is necessary for the identification of requirements for information security within an organization, as well as its implementation and ongoing administration to create effective information security management system.

Information security risk management identifies the context, assesses the risks, treats the risk and proposes a security plan to implement the recommendations and decisions. Risk management analyses in depth what can happen and what damage can be before defining what should be done (and when) to reduce the damage to an acceptable level. The implementation, operation and monitoring of these solutions is part of security management.

Risk management should be applied in all information security management processes.

The information security risk management process consists of two main elements: risk assessment and risk treatment.

It is the responsibility of each organization to determine the risk assessment methodology best suited to the specific environment and culture. There are various techniques that can be used to determine the depth of risk assessment required in a given instance. Risk assessment begins by identifying the appropriate approach to risk assessment, i.e. identifying a method of risk assessment that suits the requirements of the organization.

This should be followed by consideration of threats and vulnerabilities to facilitate the selection of controls commensurate with the assessed risks. The level of detail of this consideration can vary, depending on the information assets, process or system considered, and on the identification of the most suitable approach to risk assessment.

Following the risk assessment, risk treatment decisions need to be made on whether to avoid, transfer, accept or reduce the risks that have been identified. Where the risk assessment decision is to reduce the risk, appropriate controls are identified to reduce the risks to an acceptable level.

In addition, risk management includes risk communication, which objectives are, to collect information in order to detect and identify risks, to prevent security breaches due to misunderstanding among stakeholders, and to reduce the level of the consequence, and risk monitoring and review, to ensure that the process remains adequate and supported.

Risk management processes are often defined in many functional areas throughout an organization. For example, risk management is a key process in product certification, project management, the development of a business strategy, and in information technology (IT) and corporate governance. There are many useful sources on corporate and IT governance. (For example, see IT Governance Institute's web site).

5 Generic information security risk management process

5.1 Introduction to information security risk management process

An organization that wants to enhance security should put in place a strategy for risk management that is suitable for its environment, and contains the means to address the risks in an effective manner. A strategy is required which focuses security effort where it is needed and enables a cost and time effective approach.

Information security risk management is an ongoing activity. For new information processes and systems, and information processing systems at the planning stage, risk management should be part of the design and development. For existing information processes and systems, risk management should be introduced at any appropriate point. When significant changes to information processes and systems are planned, risk management should be part of this planning process. It should take into account all information assets, processes and systems within the organization and not be applied to any one in isolation.

The main elements of the information security risk management process are shown in Figure 1. The general approach is briefly described below, and each of the boxes more fully in subsequent clauses.

As Figure 1 illustrates, risk management processes are usually iterative.

An iterative approach to risk assessment increases depth and detail of the assessment at each iteration. It is generally too costly to conduct an in-depth risk assessment for all information and systems; conversely, it is ineffective to give only peripheral attention to serious risks. The iterative process ensures that the most serious risks will be given the most detailed attention.

The first iteration of the risk assessment consists of tasks to establish the context, identify threats and vulnerabilities as well as to estimate and evaluate risks by using information that is immediately available. The result of the first risk assessment iteration may be satisfactory to support the risk treatment process. If this is not the case, e.g. because insufficient information has been available, another iteration of the risk assessment should be conducted, which would for example include gathering of additional information, refining the scope and definition of the context, further consideration of external influences and constraints, further research on vulnerabilities and applicable threats.

The goal of the risk treatment process that follows is to achieve an acceptable level of risks, e.g. by the application of appropriate controls. These controls typically include best practice controls (e.g. from ISO/IEC 17799), but often further specific controls are necessary as well.

The success of the risk treatment process depends on the results of the risk assessment. It's not unlikely that the risk treatment process does not immediately lead to an acceptable residual risk. In this situation another iteration of the risk assessment followed further risk treatment.

The following risk acceptance process has to ensure that the remaining risks are explicitly accepted by the management of the organization. This is especially important in situation where the implementation of controls are omitted or postponed, e.g. due to cost, and additional risks are therefore implicated.

During the whole risk management process it is important that risks are communicated to the appropriate parties, e.g. the management and operational staff. Even before the treatment of the risks, information about identified risks can be very valuable to manage incidents and may help to reduce potential damage.

Risk management is a continuous process. The context as well as assets, threats and vulnerabilities change over time, and this makes it necessary to continuously monitor and review risks.

Risk assessment and risk treatment processes will be discussed in detail in Clauses 5 and 6, respectively.

Information security assessment approaches are described in more detail in Annex D.

The selection of controls is described in detail in Annex E

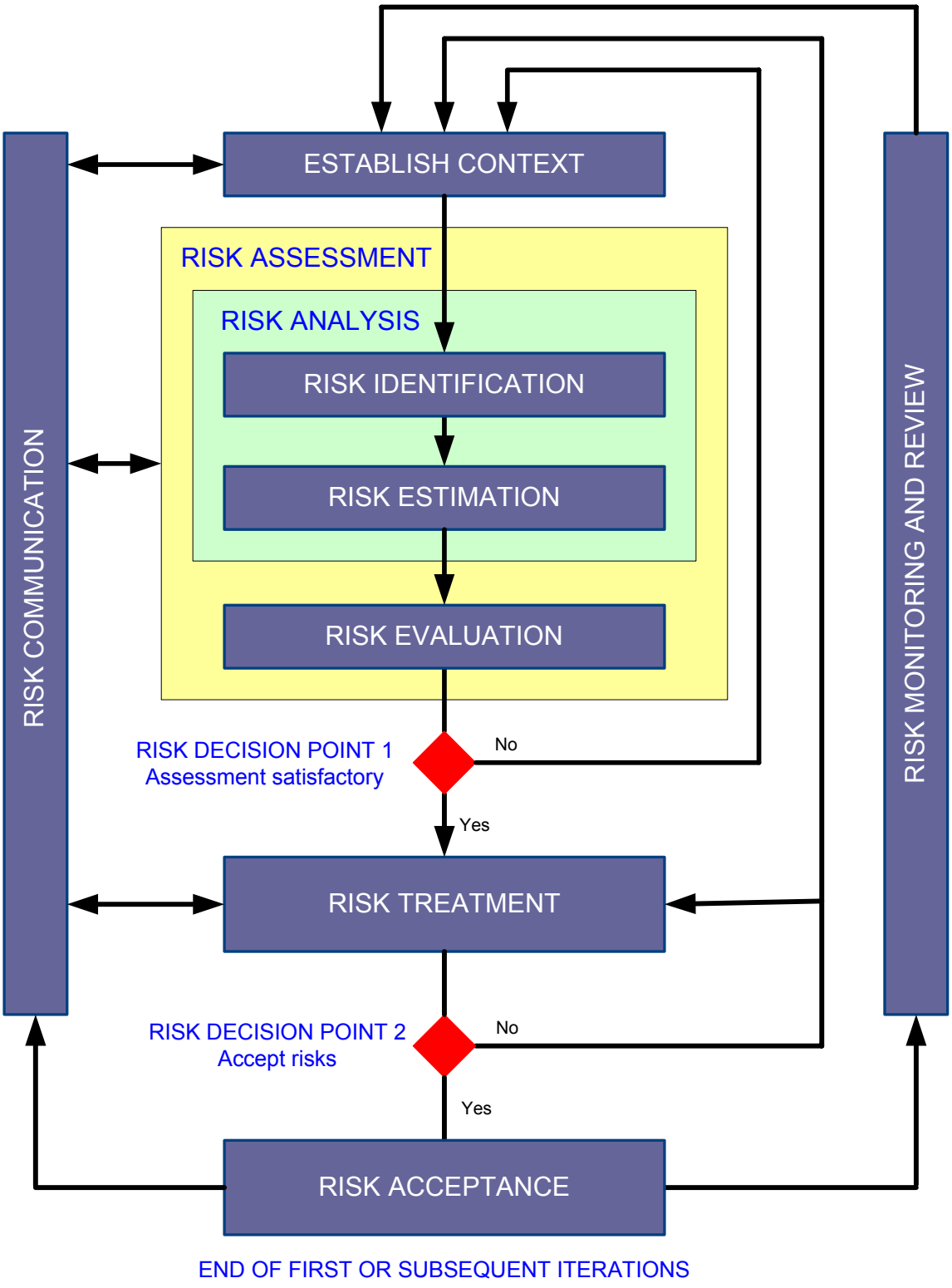

Figure 1 Information security risk management process

5.2 Process components

5.2.1 Establish the context

[Editors Note: this new clause has been developed to reflect concepts as described in TMB and AS/NZ 4370 documents;. The context establishment is wider that the one described in 27001 4.2.1c) NBs are kindly asked to review the text proposed and add explanatory text where appropriate]

Establish the context consists of setting the **basic parameters** for managing information security risks, define the **scope and boundaries** as well as an **appropriate organization** of the information security risk management process, and finally set up an **detailed structure** to run the process.

The **basic parameters** to be set include:

- selection of an appropriate risk assessment approach
- establish risk evaluation criteria
- establish impact criteria
- establish risk acceptance criteria
- determine potentially available resources

The context includes the risk evaluation criteria to be used. Criteria for evaluation of information security risks are typically (but not limited to) financial and other consequences associated with:

- legal and regulatory requirements, and contractual obligations;
- operational and business consequences of unavailability;
- operational and business consequences of loss of confidentiality;
- operational and business consequences of loss of integrity;
- customer perceptions and adverse impact on goodwill.

An organization has to define its own limits for consequences such as 'low' or 'high'. For example, financial damage that might be disastrous for a small organization might be low or even negligible for a very big organization.

Decisions concerning risk acceptability and risk treatment should be based on the operational, technical, financial, legal, regulatory, social, humanitarian or other criteria. These often depend on an organization's internal policy, goals, objectives and the interests of stakeholders

Decisions to accept risks are commonly made on the basis of whether or not an estimated risk is above or below a pre-determined threshold. In some cases, however, multiple criteria are used. For example, some risks may need to be accepted or rejected in accordance with legislative, regulatory or contractual conditions regardless of their estimated level. Furthermore, some organizations could have multiple risk acceptance thresholds, with varying monitoring and reviewing requirements.

Defining **the scope and boundaries of the risk management process** include:

- the organization's strategic business objectives, goals, processes and strategies to consider
- the organization's information security policy

- legal and regulatory requirements to follow
- area of application, e.g. by defining system or geographical boundaries
- justification for excluding issues from the scope

Before gathering input for the asset identification and valuation, the scope of the review should be defined. A careful definition of boundaries, to further define context at this stage avoids unnecessary work and improves the quality of the risk assessment. The boundary description should clearly define which of the following have to be considered when carrying out the risk assessment review for the considered information system:

- business objectives and policies,
- information and ICT assets (e.g., hardware, software, communications elements),
- people (e.g. staff, subcontractors, other external personnel),
- physical environment (e.g. buildings, facilities),
- socio-cultural environment,
- economic, legislative and regulatory environment, and
- business processes and activities (operations).

The information security policy informs the risk management process. The information security policy should contain a high-level outline of controls required and describe why they are necessary. The information security plan is based on the corporate security policy.

The organization's business objectives, goals and strategies, and legal and regulatory requirements, should be taken into account when developing the information security policy, implementing risk assessment, and risk treatment. The risk management process should be undertaken with full consideration of the need to balance costs of controls and risk reduction benefits. The resources required and the records to be kept should be specified as well.

The context concerns the relationship of information security risks to the total business risks faced by the organization. The organization should seek to identify those elements of the overall risk treatment plan where information security or ICT support for other security mechanisms is required to meet the overall risk mitigation strategy.

Setting up **an appropriate organization for the information risk management process** includes

- Identification and analyses of the stakeholders (governance)
- defining roles and responsibilities of all parts within an organization participating
- establishing the required relationships within involved parts of an organization as well as to other relevant projects or activities

Define the **detailed structure for performing the risk management process**, which includes:

- Identification of needed information, including their availability and potential gathering cost.

- Definition and appropriate assignment of process activities and tasks
- Resource management
- Definition of decision escalation paths

5.2.2 Information security risk assessment process

The information security risk assessment process is composed of risk analysis and risk evaluation, furthermore, risk analysis is composed of risk identification and risk estimation.

5.2.2.1 Information security risk analysis

Risk identification

Identify what, why and how problems and concerns can arise as the basis for further analysis. Identifying risks involves identifying assets, threats, vulnerabilities, likelihood and consequences (business impact).

This step identifies the information security risks to be managed. In some cases, risks will be similar to those in other systems or organizations; in other cases, specific analysis of risks on a case-by-case basis will be necessary. Comprehensive identification using a well-structured systematic process is critical, because a potential risk not identified at this stage is excluded from further analysis. Identification should include all risks whether or not they are under the control of the organization.

Additionally, risk identification involves identifying unacceptable consequences, however these could arise, and the consequent impacts.

There are many risk identification methodologies, such as checklists, audits and site inspections, judgments based on experience and records, flow charts, brainstorming, interviews, systems analysis, scenario analysis and systems engineering techniques. They should be selected according to the organization's needs.

Risk estimation

Determine the effectiveness of existing controls, which could exist anywhere in the organization, and analyse risks in terms of consequences and likelihood in the context of these controls. The analysis should consider the range of potential consequences and how likely these consequences are to occur. Consequences and likelihood should be combined to produce a risk estimation.

The organization should estimate risk levels based on the results of the risk identification.

In the context of information security, risk assessment for information systems involves the analysis of asset values, threats and vulnerabilities. Consequences, or business impact, should be assessed in terms of damage that would be caused by a breach of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. (Reference ISO/IEC 13335-1 for discussion of these elements.) The result of a risk assessment is a statement of the probable risk to business objectives.

A preliminary analysis can be carried out so that risks deemed to be low consequence are excluded from detailed study. Excluded risks should be listed to demonstrate the completeness of the risk assessment. Some controls, such as audit, should be implemented to review these risks deemed low consequence, to identify if such risks become higher consequence to the organization.

5.2.2.2 Information security risk evaluation

Compare estimated levels of risk against pre-established criteria. This step enables risks to be ranked so as to identify management priorities. Risks assessed as low could be considered as acceptable, and treatment of these low risks may not be required. On the other hand, risks assessed as high could be considered as not acceptable, and should be treated immediately.

Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria. The criteria can be expressed as the consequences to the business, and as a part of a business impact analysis, which will include criteria such as duration of outage, monetary value (in terms of loss), and so on. Risk analysis and the criteria against which risks are compared in risk evaluation should be considered on the same basis.

The result of a risk evaluation is a priority list of risks for further action. Decisions should take into account the context of the risk and include consideration of the tolerability of the risks borne by parties other than the organization that benefit from risk evaluation. If the resulting risk falls into the low or acceptable risk categories the risk could be accepted without further treatment. The organization should develop a list of low and accepted risks, with reasons for acceptance and methods for review and monitoring, to ensure that they remain acceptable.

5.2.3 Information security risk treatment

Develop and implement a specific risk treatment plan that includes consideration of risk evaluation criteria. Risk remaining following risk treatment is considered residual risk..

Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them. Risk treatment options: risk avoidance, risk transfer, risk acceptance, or risk reduction are discussed in Clause 6.

The risk treatment plan should first identify the selected options for the treatment of risks. The plan may indicate a combination of risk treatment options for different identified risks.

When risk avoidance, risk transfer or risk acceptance is selected, then risk treatment iteration comes to an end and the monitoring and review process will start. Note that even if the identified risk exceeds risk acceptance criteria, management may nonetheless decide not to select risk reduction.

When risk reduction is selected, then controls to reduce risks should be selected.

5.2.4 Information security risk acceptance

Accept risks remained after risk treatment process.

There will always be residual risks associated with an information security programme plan; an organization's information systems can never be made absolutely secure. Certain assets may be left unprotected intentionally (e.g., because of assumed low risk or the high costs of control(s)). Risk acceptance involves a review of assessed risks after risk treatment in the light of risk acceptance criteria.

If the level of residual risk is unacceptable after applying risk treatment process, a decision should be taken as to whether to accept this risk, or repeat the risk assessment process, or repeat the risk treatment process.

The risk acceptance process is discussed in Clause 7.

The outcome of the risk treatment and risk acceptance processes is the foundation of the organization's risk treatment plan implementation. The plan should identify required management action, responsibilities, priorities, schedules, the expected outcome of treatments, budgeting, performance measures, and the review process to be set in place. Additionally, the plan should include a mechanism for assessing the

implementation of the options against performance criteria, individual responsibilities and other objectives, and to monitor critical implementation milestones.

5.2.5 Information security risk communication

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

Risk communication is an important activity at each step of the risk management process. The objectives of risk communication involves but not limited to:

- information collection to identify risks

- information flow to avoid or reduce security incident occurrences

- consultation to improve mutual understanding of the risk management process among stakeholders

The organization should develop a communication plan for both internal and external stakeholders at the earliest stage of the process. This plan should address issues relating to both the risk itself and the process to manage it.

Risk communication is discussed in Clause 8.

5.2.6 Information security risk monitoring and review

Monitor and review the risk management process to identify changes to risks for the organization at the earliest stage.

The organization should review all the risk management process regularly, and when the major circumstances change occur.

The objective of this review is to decide whether the current risk management process is still relevant or not. If not, the organization should take corrective actions.

All risk management options should be regularly reviewed as well and includes but not limited to:

- Re-defining the context;
- Risk evaluation criteria;
- Risk assessment approach and methodology;
- Risk treatment approach and options;
- Risk communication methods; and
- Risk monitoring approach and results.

Risk monitoring and review are discussed in Clause 9.

6 Information security risk assessment

6.1 Introduction to information security risk assessment process

The risk assessment identifies potential business and operational consequences of information security incidents and the likelihood of their occurrence. Incidents can affect the business, people, process or any asset of the organization. The consequence of an information security incident is a composite of possible

damages related to the value of the assets at risk and of the possible adverse impact on business objectives as a result of the business processes being affected. The likelihood of occurrence is dependent on how attractive the asset is for a potential attacker and the ease with which the vulnerabilities can be exploited. The results of the risk assessment lead to the identification of appropriate risk treatment options, which are documented in the information system security policy and consequent information security risk treatment plan.

The iterative approach is to conduct an initial risk assessment for all information systems, in each case concentrating on the business values of the information, assets, and the serious risks to which they may be exposed. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while still ensuring that the high-risk systems are appropriately assessed.

Next iteration of risk assessment for an information system involves in-depth identification of the related risks, and an assessment of their magnitude. The need for more detailed risk assessment can be determined without unnecessary investment in time and money when high level reviews are conducted for all systems, followed by more detailed risk assessments only on high risk or critical systems.

Once the risk assessment step for a system has been completed for the first time, the detailed results of the review - assets and their values, threat, vulnerability, likelihood and consequences, risk levels, and treatment identified - should be documented.

It is up to the organization to select its own approach to risk assessment. Annex D discusses risk assessment methodologies.

NOTE 1 Internal and external influences, as well as unexpected incidents, may affect the security requirements of the system, and therefore require reconsideration of all or part of the risk assessment. Internal influences could be: recent significant changes to the system, planned changes, or the consequences of information security incidents that need to be addressed.

NOTE 2 A variety of methods exists for the performance of a risk assessment ranging from checklist-based approaches to structured analysis based techniques. Automated (computer assisted) or manual products can be used. Whatever method or product is used by the organization, it should fit with the organization's culture.

NOTE 3 Documentation of the details of the risk assessment outcome is made easier using software tools. Changes occur over time, such as configuration, types of information, threat scenarios, new vulnerabilities, etc., and may be easier to record. Further, such methods can be used to examine different options, for example, during the development of a new information system, as well as being used for other systems that are similar in nature.

6.2 Information security risk analysis

6.2.1 Information security risk identification

6.2.1.1 Identification of assets

An asset is anything that has value to the organization and which therefore requires protection. For the identification of assets it should be borne in mind that an information or ICT system consists of more than hardware and software.

The assets within the review boundary established shall be identified with a sufficient level of detail in relation to the scope and level of assessment to be carried out. Conversely, any assets to be excluded from a review boundary, for whatever reason, need to be assigned to another review to ensure that they are not forgotten or overlooked. Also, for the purpose of risk management, it is important to keep record of assets, the business processes that they support and their respective relevance to the organization in an asset inventory.

Annex A provides information on identification and valuation of assets.

6.2.1.2 Identification of threats

A threat has the potential to harm information, assets, processes and systems. Threats may be of natural or human origin, and could be accidental or deliberate. Both accidental and deliberate threat sources should be identified and the likelihood of their occurrence should be assessed. It is essential that, if possible, no threat be overlooked, as failure to do so could result in risk to the organization.

Input to the threat assessment should be obtained from the asset owners or users, from personnel department staff, from facility management and ICT specialists, as well as from people responsible for the protection of the organization. Other organizations like legal bodies and national government authorities may be able to assist, for example by providing threat statistics. A list of generally possible threats is helpful to perform the threat assessment. It might be worthwhile to consult other threat catalogues (maybe specific to an organization or business) to have the list complete.

When using threat catalogues or the results of earlier threat assessments, one should be aware that threats are continually changing, especially if the business environment or the ICT changes. For example, today's viruses are increasingly more complex over time; new viruses continue to be developed that are unknown to existing anti-virus software. More information on common threat types can be found in Annex B.

6.2.1.3 Identification of vulnerabilities

This stage includes identifying weaknesses that may be exploited by a threat source to cause harm to the assets, and the business they support. Weaknesses may occur in the any of the following:

- organization,
- processes and procedures
- management,
- personnel,
- physical environment,
- ICT system configuration, and
- hardware, software or communications equipment.

The presence of a vulnerability does not cause harm in itself, as there needs to be a threat present to exploit it. A vulnerability that has no corresponding threat may not require the implementation of a control, but should be recognized and monitored for changes. It should be noted that an incorrectly implemented or malfunctioning control, or control being used incorrectly, could itself be a vulnerability. Conversely, a threat that does not have a corresponding vulnerability may not result in risk.

Vulnerabilities can be related to properties or attributes of the asset that can be used in a way, or for a purpose, other than that intended when the asset was purchased or made. For example, one of the properties of an EEPROM (Electronically Erasable Programmable Read Only Memory) is that the information stored on it can be erased and replaced. This is one of the design criteria of an EEPROM. However, this property means that the unauthorized destruction of information stored on the EEPROM is possible. This can be a vulnerability.

This stage identifies vulnerabilities that may be exploited by threats and assesses their likely level of weakness, i.e. ease of exploitation..

Examples of vulnerabilities and methods for vulnerability assessment can be found in Annex C.

6.2.1.4 Identification of impact

Once the incident happens it creates damage. This damage is directly related to the hit asset(s) or part of asset. As assets have value both for their financial cost and because of the business consequences if they are damaged or compromised.

Organizations should identify what operational consequences occur when assets are damaged in term of

- investigation and repair time
- (work)time lost
- opportunity lost
- financial cost of specific skills to repair the damage, surely if they are not 'on hand' available in the organization.

For more details refer to Annex A2.

6.2.1.5 Identification of existing and planned controls

It is important that existing and planned controls are identified as part of this process to avoid unnecessary work or cost, e.g. in the duplication of controls. It might be identified as well that an existing or planned control is either not sufficient or not justified. In this case, it should be checked whether the control should be removed, replaced by another, more suitable, control, or whether it should stay in place (for example, for cost reasons).

While identifying the existing controls, a check should be made to ensure that the controls are working correctly. The organization may rely upon the control to work correctly, but, if it does not, then this will create vulnerabilities. Consideration should be given to the situation where a selected control (or strategy) fails in operation and therefore a second (or more) layers of controls are required to address the identified risk effectively.

For the identification of existing or planned controls, the following activities can be helpful.

- Review documents containing information about the controls (for example, risk treatment plans or concepts) - if the security process is well documented, all existing or planned controls and the status of their implementation should be listed there.

- Check with the persons responsible for information security (e.g. information security officer and ICT system security officer, building manager or operations manager) and the users as to which controls are really implemented for the information process or ICT system under consideration.

- Walk through the building viewing the physical controls, compare those implemented with the list of what controls should be there, and check those implemented as to whether they are working correctly and effectively.

The identification of existing controls may determine that existing controls exceed current needs. In this case, consideration should be given to removing these controls. If removing redundant or unnecessary controls is considered, security and cost factors should be taken into account. Since controls influence each other, removing redundant controls might reduce the overall security in place. In addition, it can be cheaper to leave controls in place then to remove them, or, especially if the controls have high maintenance costs, it can be cheaper to remove them.

The existing and planned controls should be re-examined in terms of cost comparisons, including maintenance, with a view to removing (or not implementing) or improving them if they are not effective enough. Here it should be noted that sometimes it is more expensive to remove an inappropriate control than to leave it in place, and maybe add another control. It is possible as well that a control may provide protection to assets outside of the current review boundary.

The result of this step is a list of all existing and planned controls, and their implementation and usage status.

6.2.2 Information security risk estimation

6.2.2.1 Risk estimation methodologies

Risk analysis may be undertaken in varying degrees of detail depending upon the risk, the purpose of the analysis, and the information, data and resources available. Estimation methodology may be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances. The order of complexity and costs of these analyses, in ascending order, is qualitative, semi-quantitative and quantitative. In practice, qualitative estimation is often used first to obtain a general indication of the level of risk and to reveal the major risks. Later it may be necessary to undertake more specific or quantitative analysis on the major risks.

The form of analysis should be consistent with the risk evaluation criteria developed as part of establishing the context.

In more detail, the types of estimation are:

(a) Qualitative estimation

Qualitative estimation uses words to describe the magnitude of potential consequences and the likelihood that those consequences will occur. These scales can be adapted or adjusted to suit the circumstances, and different descriptions may be used for different risks. Qualitative estimation may be used:

- as an initial screening activity to identify risks which require more detailed analysis;
- where this kind of analysis is appropriate for decisions; or
- where the numerical data or resources are inadequate for a quantitative estimation.

Qualitative analysis should use factual information and data where available.

(b) Semi-quantitative estimation

In semi-quantitative estimation, qualitative scales such as those described above are given values. The objective is to produce a more expanded ranking scale than is usually achieved in qualitative estimation, not to suggest realistic values for risk such as is attempted in quantitative estimation. However, since the value allocated to each description may not bear an accurate relationship to the actual magnitude of consequences or likelihood, the numbers should only be combined using a formula that recognizes the limitations of the kinds of scales used.

Care needs to be taken with the use of semi-quantitative estimation because the numbers chosen may not properly reflect relativities and this can lead to inconsistent, anomalous or inappropriate outcomes. Semi-quantitative estimation may not differentiate properly between risks, particularly when either consequences or likelihood are extreme.

(c) Quantitative estmation

Quantitative estimation uses numerical values (rather than the descriptive scales used in qualitative and semi-quantitative estimation) for both consequences and likelihood using data from a variety of sources. The quality of the analysis depends on the accuracy and completeness of the numerical values and the validity of the models used. Quantitative estimation in most cases uses historical incident data.

6.2.2.2 Valuation of assets and impact assessment

After fulfilling the objective of asset identification by listing all assets of the information system under review, values should be assigned to these assets. These values represent the importance of the assets to the organization. Thus asset identification and valuation, based on the business needs of an organization, are major factors in the determination of risks. Asset valuation begins with classification of assets according to their priority, in terms of the importance of assets to fulfilling the business objectives of the organization.

Valuation is then determined using two measures: first, the replacement value of the asset: the cost of replacing it, and, second, the business consequences of loss or compromise of the asset, such as the potential adverse business consequences from the disclosure, modification, non-availability and/or destruction of information, and other information system assets. This can be determined from a business impact analysis. The value, determined by the consequence for business, is usually significantly higher than the simple replacement cost, depending on the importance of the asset to the organization in meeting its business objectives. Asset valuation is a key factor in the impact assessment of a security incident, because the incident may affect more than one asset, or only a part of an asset. Annex A provides more information both on asset valuation and impact assessment.

6.2.2.3 Assessment of threats

After identifying the threat source (who and what causes the threat) and the threat target (i.e. what elements of the system may be affected by the threat), it is necessary to assess the likelihood of the threats. This should take account of:

- the threat frequency (how often it might occur, according to experience, applicable statistics, etc.),
- the motivation, the capabilities (perceived and necessary), resources available to possible attackers, and the perception of attractiveness and vulnerability of information system assets for the possible attacker, for deliberate threat sources, and
- geographical factors such as proximity to chemical or petroleum plants, the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction, for accidental threat sources.

Depending on the need for accuracy, it might be necessary to split assets into their components and relate the threats to the components, for example, if geographical location changes the nature of threats to the same types of assets.

Consequences of an unlikely materialization of a threat need to be considered, as cost-effective measure may be able to be taken to limit damage should the threat materialize (e.g. removal of photocopies of vital contracts off site).

At the completion of the threat assessment, there will be a list of threats identified, the assets or groups of assets they would affect, and measures of the likelihood of threats occurring, for example, on a scale such as high, medium, or low.

6.2.2.4 Assessment of vulnerabilities

It is important to assess how severe the vulnerabilities are, in other words how easily they may be exploited. A vulnerability should be assessed considering all the threats that might exploit it in a particular situation. For instance, an information system may have a vulnerability to the threats of masquerading of user identity and misuse of resources. The vulnerability to masquerading of user identity may be high because of lack of user authentication. On the other hand, the vulnerability to misuse resources may be low because even with lack of user authentication the means by which resources might be misused are limited. Organizations should take existing control into account and measure how they reduce the vulnerabilities.

The results of this step should be a list of vulnerabilities, an identification of the threat(s) relevant to each vulnerability, and assessments of the ease of exploitation, for example, on a scale of high, medium, or low.

6.2.2.5 Assessment of impact

Consequences or business impact may be determined by modeling the outcomes of an event or set of events, or by extrapolation from experimental studies or past data. Consequences may be expressed in terms of monetary, technical or human impact criteria, or any of the other relevant criteria. In some cases, more than one numerical value is required to specify consequences for different times, places, groups or situations.

The way in which consequences and likelihood are expressed and the ways in which they are combined to provide a level of risk will vary according to the type of risk and the purpose for which the risk assessment output is to be used. The uncertainty and variability of both consequences and likelihood should be considered in the analysis and communicated effectively.

Impact in time and finance and has to be measured with the same approach used for threat likelihood and vulnerability. Coherence has to be maintained on the quantitative or the qualitative approach.

Impact assessment helps defining the full risk picture

6.2.3 Risk estimation

The final stage of risk analysis is to estimate the level of risks. Asset values and impact assessment are used to estimate consequences of incidents. Information about threats and vulnerabilities is used to estimate the likelihood of incidents. A variety of methodologies are available to use this information to estimate levels of risk. Annex D provides examples.

6.3 Information security risk evaluation

The nature of the decisions pertaining to risk evaluation and the criteria which will be used to make those decisions would have been decided when establishing the context. These decisions and the context should be revisited in more detail at this stage when more is known about the particular risks identified. To evaluate risks, organizations should compare the estimated risks (using selected methodologies as discussed in Annex D) with the risk criteria defined during the context assessment. Criteria used to make decisions shall be consistent with the defined external, internal and risk management context and take account of the objectives, of the organization and stakeholder views etc. Decisions may be based on the level of risk but consequences, likelihood, the aggregate effect of multiple risks, and the degree of confidence in the risk identification and analysis should be considered as well.

Considerations should include:

- security criteria: if one criterion is not relevant for the organization (e.g. confidentiality), then all risks impacting this criterion may not be relevant;
- importance of the business process or activity supported by a particular asset or set of assets: if the process is determined to be of low importance, risks associated with it should be given a lower consideration than risks that impact more important processes or activities;

Risk evaluation uses the understanding of risk obtained by risk analysis to make decisions about future actions. Decisions should include:

- whether a risk needs treatment;
- whether an activity should be undertaken;
- priorities for risk treatment.

During the risk evaluation stage, legal and regulatory requirements are factors that should be taken into account in addition to the estimated risks. Organizations may have found no internal risk but still need to comply with the external requirements.

7 Information security risk treatment

7.1 Information security risk treatment options

There are four options available for risk treatment: risk avoidance, risk reduction, risk transfer and risk acceptance. Normally, a combination of the four options is the outcome of the risk treatment determination; the four options are not mutually exclusive. These four options are briefly explained below.

- Risk avoidance: considering ways to remove the threat or the vulnerability, or change a process or activity so that the threat no longer applies.
- Risk transfer: transferring the risk to third parties which may take on risk, for example, insurance companies, or through outsourcing to network solution providers or managed security services.
- Risk reduction: applying appropriate controls to reduce risk (in terms of reducing the vulnerabilities or possible consequences).
- Risk acceptance (objectively): making a decision concerning all risk remained.

Risk treatment options should be assessed on the basis of the extent of risk reduction, and the extent of any additional benefits or opportunities created, taking into account the criteria developed previously. Some immediate options may be technically unfeasible or require significant investment in maintenance.A number of options should be considered and applied either individually or in combination.

Selection of the most appropriate option involves balancing the cost of implementing each option against the benefit derived from it. In general, the cost of managing risks needs to be commensurated with the benefits obtained.

When large reductions in risks may be obtained with relatively low expenditure, such options should be implemented. Further options for improvements may be uneconomic and judgement needs to be exercised as to whether they are justifiable.

Decisions should take account of the need to carefully consider rare but severe risks, which may warrant risk reduction measures that are not justifiable on strictly economic grounds. In general the adverse consequences of risks should be made as low as reasonably practicable, irrespective of any absolute criteria.

In many cases, it is unlikely that one risk treatment option will be a complete solution for a particular problem. Often the organization will benefit substantially by a combination of options such as reducing the likelihood of risks, reducing their consequences, and transferring or retaining any residual risks. An example is the effective use of contracts and risk financing supported by a risk reduction programme. Some risk treatment options can effectively address more than one risk (e.g., security training and awareness).

Where the cumulative costs of implementing all risk treatments exceeds the available budget, the risk treatment plan should clearly identify the priority ordering in which individual risk treatments should be implemented. Priority ordering can be established using various techniques, including risk ranking and cost-benefit analysis. Risk treatments which cannot be implemented within the limit of the available budget should either wait until the availability of further financial resources or, if for whatever reason any or all of the remaining treatments are considered important, a case shall be made to secure additional finances.

Context assessment provides information on legal and regulatory requirements that need to be implemented, even if no specific risk has been identified for the organization. More information can be found in ISO/IEC 27002, clause 0.3

Risk treatment options should consider

- how risk is perceived by affected parties, and
- the most appropriate ways to communicate to those parties.

Figure 2 illustrates the risk treatment option decision-making process.

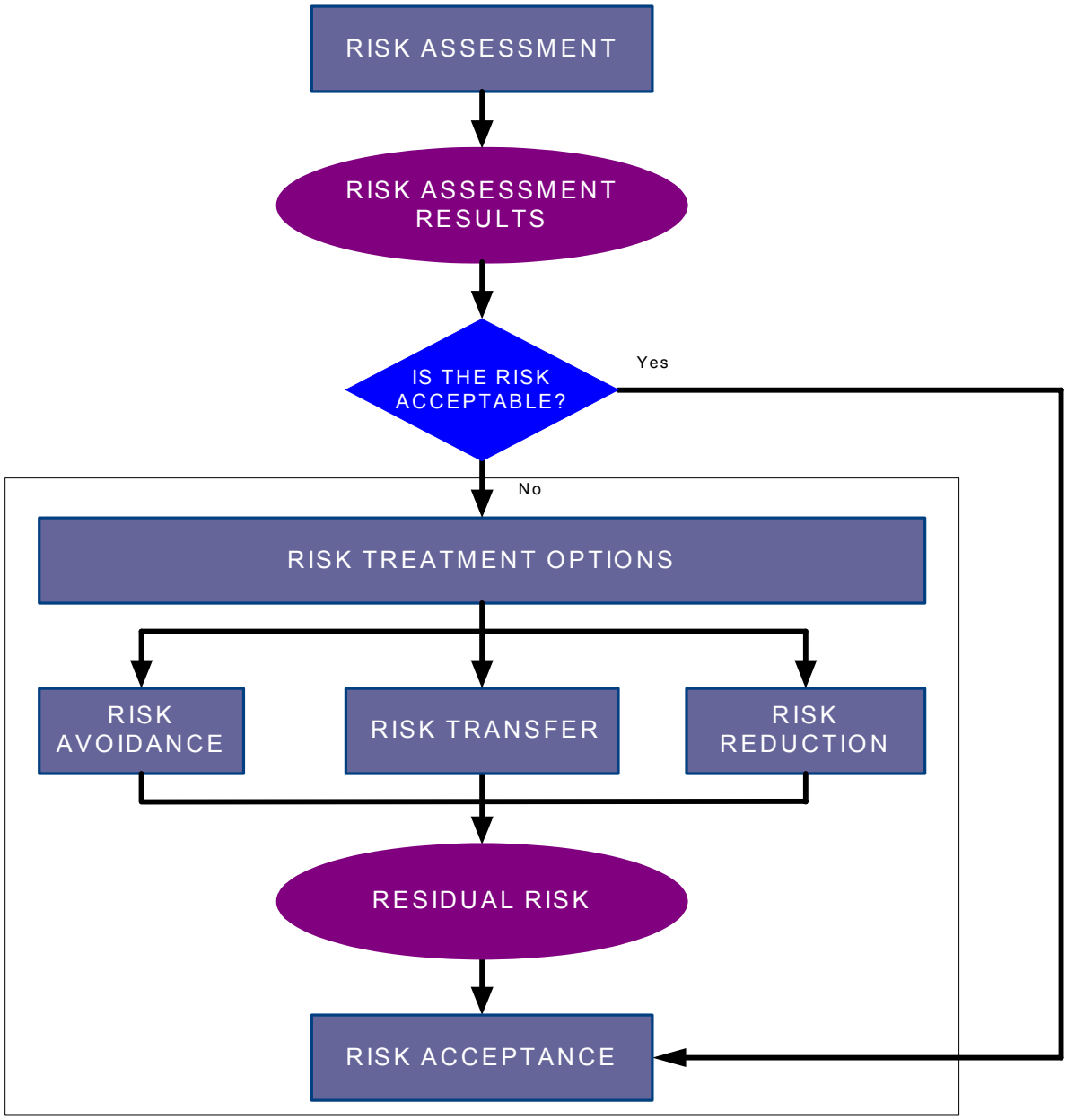

Figure 2 Risk treatment option decision-making process

7.2 Information security risk avoidance

When the identified risks are considered too high, a decision may be made to avoid the risk completely, by terminating a programme, or withdrawing from a planned or existing activity or set of activities.

7.3 Information security risk transfer

Risk transfer involves a decision to share certain risks with external parties. Risk transfer can create new risks, or modify existing, identified risks; therefore additional risk treatment may be necessary.

7.4 Information security risk acceptance

If the level of risk is high, but considerable opportunities could result from taking the risk, such as the use of a new technology, then acceptance of the risk needs to be based on an assessment of the costs of risk treatment, and the costs of rectifying the potential consequences versus the opportunities afforded by taking the risk. See Clause 7 for further consideration of risk acceptance process.

7.5 Information security risk reduction

7.5.1 General considerations

Appropriate and justified controls should be identified and selected to reduce the assessed risks to an acceptable level. The measures of risks should be used as the basis for identifying all controls that are necessary for appropriate protection. Existing and planned controls, the information security architecture, and constraints of various types should be taken into account to allow a proper selection.

In general, controls may provide one or more of the following types of protection: prevention, deterrence, detection, reduction, recovery, correction, monitoring, and awareness. These attributes act on the threat, vulnerability and/or impact. Which of these attributes is most preferable depends on the specific circumstances, and on what each control is supposed to achieve. In many cases controls will provide more than one, again providing additional benefits. Where possible, controls that do provide multiple benefits should be sought in preference to those that do not.

During control selection it is important to weigh the cost of acquisition, implementation and maintenance of the controls against the value of the assets being protected, and the return on investment in terms of risk reduction and potential new business opportunities afforded by certain controls. The cost of implementation and maintenance of a control can be much higher than the cost of the control itself, hence they should be taken into account during selection. Additionally, consideration should be given to specialized skills that may be needed to implement controls.

Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues may hamper the use of certain controls. In these instances, the system and security managers should work together to identify optimal solutions. Moreover, it could be the case that a control would decrease the performance. Again, system and security managers together should try to identify a solution that allows the necessary performance while guaranteeing sufficient security.

The result of this first step is a list of possible controls, with their cost, benefit, and priority of implementation.

7.5.2 Identification and review of constraints

There are many constraints which can affect the selection of controls. These constraints should be taken into account when making recommendations and during the implementation. Typical constraints are:

Time constraints:

Many types of time constraints can exist. For example, controls should be implemented within a time period acceptable for management. Another type of time constraint is whether a control can be implemented within the lifetime of the information or system. A third type of time constraint may be the period of time management decides is an acceptable period to be exposed to a particular risk.

Financial constraints:

Controls should not be more expensive to implement or to maintain than the value of assets they are designed to protect, except where compliance is mandatory (e.g, with legislation). Every effort should be made not to exceed assigned budgets. However, in some cases it may not be possible to achieve the desired security and level of risk acceptance within those budget constraints. This therefore becomes a management decision as to the resolution of this situation.

Great care should be taken if the budget reduces the number or quality of controls to be implemented since this can lead to the implicit acceptance of greater risk than planned. The established budget for controls should only be used as a limiting factor with considerable care.

Technical constraints:

Technical problems, like the compatibility of programmes or hardware, can easily be avoided if account is taken of them during the selection of controls. Also, the retrospective implementation of controls to an existing process or system is often hindered by technical constraints. These difficulties may move the balance of controls towards the procedural and physical aspects of security. It may be necessary to revise the information security programme in order to achieve security objectives. This can occur when controls do not meet the expected results in reducing risks without lessening productivity.

Cultural constraints:

Cultural constraints to the selection of controls may be specific to a country, a sector, an organization, or even a department within an organization. They cannot be ignored because many controls rely on the active support of the staff. If the staff do not understand the need for the control or do not find it culturally acceptable, it is likely that the control will become ineffective over time.

Ethical constraints,

These may be of more concern in some industry sectors than others, for example, government and healthcare.

Environmental constraints:

Environmental factors may influence the selection of controls, like space availability, extreme climate conditions, surrounding natural and urban geography, etc.

Legal constraints:

Legal factors such as personal data protection or criminal code provisions for information processing could affect the selection of controls. Other laws and regulations such as labour relations and privacy legislation, fire department, health and safety, and economic sector regulations, etc. could affect control selection as well.

Ease of use:

Controls should be selected to provide optimal ease of use while achieving an acceptable level of residual risk to the business. Controls that are difficult to use will impact their effectiveness, as users may try to circumvent or ignore them as much as possible. Complex access controls within an organization could encourage users to find alternate, unauthorized methods of access.

Personnel constraints:

The availability and salary cost of specialized skill sets to implement controls should be considered. Expertise may not be readily available to implement planned controls, or the expertise may be overly costly for the organization.

Constraints of integrating new and existing controls:

New controls may not easily be implemented if there is incongruity or incompatibility with existing controls. For example, a plan to use biometric tokens for physical access control may cause conflict with an existing PIN-pad based system for access control. The cost of changing controls from the existing control to the planned controls taking into consideration some elements that should be added to the overall costs of risk treatment.

8 Information security risk acceptance

. Organization should make decision to accept risk based on the acceptance criteria. This decision comes from two reasons. One is successful risk reduction, that is, the residual risk after the implementation of controls does not exceed the criteria for risk acceptance. The other is risk retention, that is, even though the risk, whether initial or residual, exceeds the criteria, management decides to accept risk, taking into account various conditions, such as budget, time constraints, etc.

Risk acceptance involves a review of assessed risks in the light of risk acceptance criteria. This includes a judgement of how much the controls selected reduce the risks, for example, by reducing the consequences and/or vulnerabilities. These residual risks are categorized according to those that are considered 'acceptable' and those that are considered 'unacceptable' to the organization. Unacceptable risks should not be tolerated; thus additional controls reducing those risks should be considered. For each of these unacceptable risks, a business decision needs to be made. Either the risk is finally accepted, or the expense of additional controls needs to be approved to reduce the risk to an acceptable level. It is a management decision whether these risks will be accepted because of other constraints (like costs, or simply impossibility of prevention - as in the case of planes crashing on a building or earthquakes; however, plans to recover from such incidents can still be made), or whether additional and maybe expensive controls are selected to reduce the unacceptable risks. Acceptable risk can become unacceptable due to organizational changes or greater exposure of assets, and ongoing risk assessments should be performed to monitor and evaluate risk level changes.

When new or changed risks in an operational environment are assessed as unacceptable, risk treatment may take time to implement. In such cases, management should understand that such risks are accepted for the period of time it takes to implement the risk treatment. It may be appropriate to place constraints on operations during this time.

9 Information security risk communication

An organization should establish procedures for risk communications among decision makers and stakeholders in order to achieve the following:

- to provide assurance of the organization's risk management,
- to collect risk information, and
- to avoid the occurrence of security breaches due to the lack of mutual understanding among decision makers and stakeholders.

An organization should develop communications plans for both normal business and emergency situations. The objectives of communications are

- to inform the organization's attitude regarding information security, and
- to reduce impact when events such as security breaches occur.

Effective internal and external communication to all stakeholders is important as it may have a significant impact on decisions made. This communication will ensure that those responsible for implementing risk management, and those with a vested interest understand the basis on which decisions are made and why particular actions are required.

Perceptions of risk can vary due to differences in assumptions and concepts and the needs, issues and concerns of stakeholders as they relate to the risk or the issues under discussion. Stakeholders are likely to make judgments on the acceptability of the risk based on their perception of risk. This is especially important to ensure that the stakeholders' perceptions of risk, as well as their perceptions of benefits, can be identified and documented and the underlying reasons being clearly understood and addressed.

It is important to cooperate with the appropriate public relations or communications unit within the organization to coordinate all tasks related to risk communication. This is crucial in the event of crisis communication actions, for example, in response to particular incidents.

10 Information security risk monitoring and review

It must be remembered that few risks remain static. Ongoing monitoring and review is necessary to ensure that the context, the outcome of the risk assessment and risk treatment, as well as management plans, remain relevant and appropriate to the circumstances. Factors that could affect the likelihood and consequences of threats occurring could change, as could factors that affect the suitability or cost of the various treatment options. It is therefore necessary to regularly repeat the risk assessment process. Major changes affecting the organization should be a reason for a more specific review. Results of monitoring and review activities should be fed back into the risk assessment process. New threats, vulnerabilities or changes in likelihood or impacts can increase previously assessed low risks or impacts. Review of low and accepted risks should consider each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated impact. If risks do not fall into the low or acceptable risk category, they should be treated using one or more of the options considered in the following clauses. The selected options for risk treatment should be reviewed periodically.

10.1 Monitoring and review of risk elements

Organizations should ensure that the following are continuously reviewed:

- new threats that could be active both outside and inside the organization and that have not been assessed,
- proper assessment of the likelihood of occurrence,
- possibility that new or increased vulnerabilities could allow threats to exploit these new or changed vulnerabilities, and
- increased impact or consequences of assessed threats, vulnerabilities and risks in aggregation resulting in an unacceptable level of risk.

Organizations should ensure that risk assessment and risk treatment resources are continuously available to review risk, to address new or changed threats or vulnerabilities, and to advise management accordingly.

10.2 Information security risk management monitoring and review

The risk management process should be monitored and reviewed. Organizations should make sure that the process and related procedures are followed so that management has assurance that no risk or risk element is overlooked or underestimated and that the necessary actions are taken and decisions are made to provide a realistic risk understanding and ability to respond.

Additionally, the organization should regularly verify that the criteria and thresholds used to measure the risk and its elements are still valid and consistent with business objectives, strategies and policies, and that changes to the business context are taken into consideration adequately level during the risk management process. This monitoring and review should address (but is not limited to):

- legal and environmental context,
- competition context,
- risk evaluation criteria,
- asset value and categories,

- risk element consideration thresholds,
- risk treatment decisions thresholds, and
- control cost values.

Annex A Valuation of assets and impact assessment

(informative)

A.1 Asset valuation

The valuation of an organization's assets is an essential step in the overall information security risk assessment process. The value assigned to each asset should be expressed in terms that are relevant to the asset and to the business entity involved. The value assigned can then be ranged in its relevance. To perform the asset valuation, an organization first needs to identify all of its assets. Moreover, it is valuable to assign an asset owner who will be responsible for determining the asset's value.

To assure that all assets are accounted for, it is often helpful to group them by category, such as:

- information and ICT assets (e.g., hardware, software, communications elements),
- people (e.g. staff, subcontractors, other external personnel),
- environment (e.g. buildings, facilities), and
- business processes and activities (operations).

Within these broad categories, types of assets can be any of the following:

- information/data (e.g. files containing payment details, product information),
- hardware (e.g. computer, printer),
- software, including applications (e.g. text processing programmes, programmes developed for special purposes),
- communications equipment (e.g. telephones, copper cable, fibre),
- networks and network hardware, software and firmware,
- media (e.g. floppy discs, CD ROMs and other removable media),
- documents (e.g. contractes),
- funds (e.g. in Automatic Teller Machines),
- manufactured goods,
- services (e.g. information services, computing resources),
- knowledge resources,
- confidence and trust in services (e.g. payment services),
- environmental equipment, and
- organisation's reputation.

The next step is to agree upon the scale to be used and the criteria for assigning a particular location on that scale to each asset, based on valuation. Because of the diversity of assets found within most organizations, it

is likely that some assets which have a known monetary value will be valued in the local unit of currency while others which have a more qualitative value may be assigned a value ranging for example from ”very low” to ”very high”. The decision to use a quantitative based scale versus a qualitative scale is really a matter of organizational preference, but should be relevant to the assets being valued. Both valuation types could be used for the same asset.

Typical terms used for the qualitative valuation of assets include words such as: negligible, very low, low, medium, high, very high, and critical. The choice and range of terms suitable to an organization is strongly dependent on an organization's needs for security, organizational size, and other organization specific factors.

The criteria used as the basis for assigning a value to each asset should be written out in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined and since many different individuals are likely to be making the determinations. Possible criteria used to determine an asset’s value include its original cost, its replacement or re-creation cost, or its value may be abstract, e.g., the value of an organization’s reputation.

Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability as the result of an incident. Such a valuation would provide three important dimensions to asset value, in addition to replacement cost, based on estimates of the adverse business consequences which would result from security incidents with an assumed set of circumstances. It is emphasized that this approach accounts for consequences that are necessary to factor into the risk assessment equation.

Many assets may during the course of valuation have several values assigned. For example: a business plan may be valued based on the labour expended to develop the plan, it might be valued on the labour to input the data, and it could be valued based on its value to a competitor. Each of the assigned values will most likely differ considerably. The assigned value may be the maximum of all possible values or may be the sum of some or all of the possible values. In the final analysis, which value or values are assigned to an asset should be carefully determined since the final value assigned enters into the determination of the resources to be expended for the protection of the asset.

Ultimately, all asset valuations need to be reduced to a common basis. This may be done with the aid of criteria such as those that follow. Criteria that may be used to assess the possible consequences resulting from a loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability of assets are:

- violation of legislation and/or regulation,
- impairment of business performance,
- loss of goodwill/negative effect on reputation,
- breach associated with personal information,
- endangerment of personal safety,
- adverse effects on law enforcement,
- breach of confidentiality,
- breach of public order,
- financial loss,
- disruption to business activities, and
- endangerment of environmental safety.

These criteria are examples of issues to be considered for asset valuation. For carrying out valuations, an organization needs to select criteria relevant to its type of business and security requirements. This might mean that some of the criteria listed above are nor applicable, and that others might need to be added to the list.

After establishing the criteria to be considered, the organization should agree on a scale to be used organization-wide. The first step is to decide on the number of levels to be used. There are no rules with regard to the number of levels that are most appropriate. More levels provide a greater level of granularity, but sometimes a too fine differentiation makes consistent assignments throughout the organization difficult. Normally, any number of levels between 3 (e.g. low, medium, and high) and 10 can be used as long as it is consistent with the approach the organization is using for the whole risk assessment process.

Also, an organization may define its own limits for asset values, like 'low', 'medium', or 'high'. These limits should be assessed according to the criteria selected, e.g. for possible financial loss, they should be given in monetary values, but when considering endangerment of personal safety, monetary valuation will not be appropriate. Finally, it is entirely up to the organization to decide what is considered as being 'low' or a 'high' consequence. A consequence that might be disastrous for a small organization could be low or even negligible for a very large organization.

The input for the valuation of assets – both replacement cost and business consequence – should be provided by owners and users of the assets. The person(s) carrying out the risk assessment will list the assets, then seek assistance from those involved in business planning, finance, information systems and other relevant activities in order to identify values for each of these assets. The values assigned should be related to the cost of obtaining, implementing and maintaining the asset, and the potential adverse business consequences from loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, or reliability. Each of the assets identified should be of value to the organization. However, there will not be a direct or easy way to establish financial value for all. It is necessary to establish the value or extent of importance in non-financial, i.e. qualitative, terms to the organization as well. Otherwise it will be difficult to identify the level of protection and the amount of resource the organization should devote to protect the assets. An example for such a qualitative valuation scale could be a distinction between low, medium and high, or, in more detail:

negligible - low - medium - high - very high.

It should be emphasized at this stage that the method for assessment should allow not only quantitative valuation, but qualitative valuation as well, where quantitative valuation is impossible or illogical (for example, the potential for loss of life, or loss of business goodwill). Explanation should be given of the valuation scale used.

Dependencies of assets on business processes should be identified, since this might influence the values of the assets. The more relevant and numerous the business processes supported by an asset, greater the value of this asset. Dependencies of assets on other assets should be identified as well, since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its life-cycle, at all stages, including storage and processing, i.e. the security needs of data storage and processing programmes should be directly related to the value representing the confidentiality of the data stored and processed. Also, if a business process is relying on the integrity of certain data being produced by a programme, the input data of this programme should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly air conditioning. Thus information about dependencies will assist in the identification of threats and particularly vulnerabilities. Additionally, it will help to assure that the true value of the assets (through the dependency relationships) is given to the assets, thereby indicating the appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

- if the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same, and

- if the values of the dependent asset (e.g. data) is greater, then the value of the asset considered (e.g. software) should be increased according to:

the degree of dependency, and

the values of the other assets.

An organization may have some assets that are available more than once, like copies of software programmes or the same type of computer used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these assets are overlooked easily, therefore care should be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity, authenticity, non-repudiation and accountability), non-availability and destruction (preservation of availability and reliability), and replacement cost.

A.2 Impact assessment

A security incident can impact more than one asset, or only a part of an asset. Impact is related to the degree of success of the incident. As a consequence, there is an important difference between the asset value and the impact resulting from the incident. Impact is considered as having either an immediate (operational) effect or a future (business) that includes financial and market consequences. In this standard, only the immediate impact is considered.

Operational impact is either direct or indirect.

- Direct:
  - The financial replacement value of lost (part of) asset.
  - The cost of acquisition, configuration and installation of the new asset or backup.
  - The cost of suspended operations due to the incident until the service provided by the asset(s) is restored.
  - Impact results in a security breach.
- Indirect:
  - opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere),
  - the cost of interrupted operations, and
  - potential misuse of information obtained through a security breach.
  - violation of statutory or regulatory obligations;
  - violation of ethical codes of conduct.

As such, the first assessment (with no safeguard of any kind) will estimate an impact as very close to the (combination of the) concerned asset value(s). For any next iteration for this (these) asset(s), the impact will be different (normally much lower) due to the presence and the effectiveness of the implemented controls.

Annex B Common Threat Types

(informative)

The following list gives examples of typical threats. The list can be used during the threat assessment process. Threats may be deliberate, accidental or environmental (natural). The following list indicates for each threat type where D (deliberate), A (accidental), E (environmental) are relevant. D is used for all deliberate actions aimed at information assets, A is used for all human actions which accidentally can damage information assets, E is used for all incidents which are not based on human actions. The threats shown as "A", "D" and/or "E" are not in priority order, and are therefore listed alphabetically.

Air conditioning failure	A, D, E
Bomb attack	A, D
Communications infiltration	D
Damage to lines	A, D
Deterioration of storage media	E
Dust	E
Earthquake	E
Eavesdropping	D
Electromagnetic radiation	A, D, E
Electrostatic charging	E
Extremes of temperature and humidity	A, D, E
Failure of communications services (i.e. network services)	A, D
Failure of power supply	A, D, E
Failure of water supply	A, D, E
Fire	A, D
Flooding	A, D, E
Hardware failures	A
Hurricane	E
Illegal import/export of software	A, D
Illegal use of software	A, D
Industrial Action	A, D
Lightning	E
Maintenance error	A, D

1	Malicious software	A, D
2	Masquerading of user identity	D
3	Misrouting of messages	A
4	Misuse of resources	A, D
5	Network access by unauthorized users	D
6	Operational staff error	A, D
7	Power fluctuation	A, E
8	Repudiation	D
9	Rerouting of messages	D
10	Software Failure	A, D
11	Staff shortage	A, D
12	Technical failure of network components	A
13	Theft	D
14	Traffic analysis	D
15	Traffic overloading	A, D
16	Transmission errors	A
17	Unauthorized use of storage media	D
18	Use of arms	A, D
19	Use of network facilities in an unauthorized way	D
20	Use of software by unauthorized users	A, D
21	Use of software in an unauthorized way	A, D
22	User errors	A, D
23	Wilful Damage	D

Particular attention should be paid to human threat sources. These are specifically itemized in the following table:

Threat-Source	**Motivation**	**Threat Actions**
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation,

	Monetary gain Unauthorized data alteration	interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access(access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

1

2 Additional catalogues of threats can be found in Annex B of ISO/IEC TR 15446 and Section 4 of SP800-12.

Annex C Common vulnerabilities and methods for vulnerability assessment

(informative)

C.1 Common vulnerabilities

The following lists give examples for vulnerabilities in various security areas, including examples of threats that might exploit these vulnerabilities. The lists can provide help during the assessment of vulnerabilities. It is emphasized that in some cases other threats may exploit these vulnerabilities as well.

1. Environment and infrastructure

Lack of physical protection of the building, doors, and windows

(could be exploited by, for example, the threat of theft)

Inadequate or careless use of physical access control to buildings and rooms

(could be exploited by, for example, the threat of wilful damage)

Unstable power grid

(could be exploited by, for example, the threat of power fluctuation)

Location in an area susceptible to flood

(could be exploited by, for example, the threat of flooding)

2. Hardware

Lack of periodic replacement schemes

(could be exploited by, for example, the threat of deterioration of storage media)

Susceptibility to voltage variations

(could be exploited by, for example, the threat of power fluctuation)

Susceptibility to temperature variations

(could be exploited by, for example, the threat of extremes of temperature)

Susceptibility to humidity, dust, soiling

(could be exploited by, for example, the threat of dust)

Sensitivity to electromagnetic radiation

(could be exploited by, for example, the threat of electromagnetic radiation)

Insufficient maintenance/faulty installation of storage media

(could be exploited by, for example, the threat of maintenance error)

Lack of efficient configuration change control

(could be exploited by, for example, the threat of operational staff error)

3. Software

Unclear or incomplete specifications for developers

(could be exploited by, for example, the threat of software failure)

No or insufficient software testing

(could be exploited by, for example, the threat of use of software by unauthorized users)

Complicated user interface

(could be exploited by, for example, the threat of operational staff error)

Lack of identification and authentication mechanisms like user authentication

(could be exploited by, for example, the threat of masquerading of user identity)

Lack of audit trail

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Well-known flaws in the software

(could be exploited by, for example, the threat of use of software by unauthorized users)

Unprotected password tables

(could be exploited by, for example, the threat of masquerading of user identity)

Poor password management (easily guessable passwords, storing of passwords in clear, insufficient frequency of change)

(could be exploited by, for example, the threat of masquerading of user identity)

Wrong allocation of access rights

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Uncontrolled downloading and using software

(could be exploited by, for example, the threat of malicious software)

No 'logout' when leaving the workstation

(could be exploited by, for example, the threat of use of software by unauthorized users)

Lack of effective change control

(could be exploited by, for example, the threat of software failure)

Lack of documentation

(could be exploited by, for example, the threat of operational staff error)

Lack of back-up copies

(could be exploited by, for example, the threat of malicious software or the threat of fire)

Disposal or reuse of storage media without proper erasure

(could be exploited by, for example, the threat of use of software by unauthorized users)

Unnecessary services enabled

(could be exploited by, for example, the threat of use of unauthorized software)

Immature or new software

(could be exploited by, for example, the threat of incompetent or inadequate testing)

widely-distributed software

(could be exploited by, for example, the threat of loss of integrity in the distribution process)

4. Communications

Unprotected communication lines

(could be exploited by, for example, the threat of eavesdropping)

Poor joint cabling

(could be exploited by, for example, the threat of communications infiltration)

Lack of identification and authentication of sender and receiver

(could be exploited by, for example, the threat of masquerading of user identity)

Transfer of passwords in clear

(could be exploited by, for example, the threat of network access by unauthorized users)

Lack of proof of sending or receiving a message

(could be exploited by, for example, the threat of repudiation)

Dial-up lines

(could be exploited by, for example, the threat of network access by unauthorized users)

Unprotected sensitive traffic

(could be exploited by, for example, the threat of eavesdropping)

Inadequate network management (resilience of routing)

(could be exploited by, for example, the threat of traffic overloading)

Unprotected public network connections

(could be exploited by, for example, the threat of use of software by unauthorized users)

Insecure network architecture

(could be exploited by, for example, the threat of intrusion)

5. Documents

Unprotected storage

(could be exploited by, for example, the threat of theft)

Lack of care at disposal

(could be exploited by, for example, the threat of theft)

Uncontrolled copying

(could be exploited by, for example, the threat of theft)

6. Personnel

Absence of personnel

(could be exploited by, for example, the threat of staff shortage)

Unsupervised work by outside or cleaning staff

(could be exploited by, for example, the threat of theft)

Insufficient security training

(could be exploited by, for example, the threat of operational staff error)

Lack of security awareness

(could be exploited by, for example, the threat of user errors)

Incorrect use of software and hardware

(could be exploited by, for example, the threat of operational staff error)

Lack of monitoring mechanisms

(could be exploited by, for example, the threat of use of software in an unauthorized way)

Lack of policies for the correct use of telecommunications media and messaging

(could be exploited by, for example, the threat of use of network facilities in an unauthorized way)

Inadequate recruitment procedures

(could be exploited by, for example, the threat of wilful damage)

7. Procedural

Lack of information processing facilities authorization

(could be exploited, for example, by the threat of willful damage)

Lack of formal process for authorization of public available information

(could be exploited, for example, by the threat of input of corrupted data)

Lack of formal process for access right review (supervision)
(could be exploited, for example, by the threat of unauthorized access)
Lack of formal policy on mobile computer usage
(could be exploited, for example, by the threat of theft)
Lack of formal procedure for ISMS documentation control
(could be exploited, for example, by the threat of input of corrupted data)
Lack of formal procedure for ISMS record supervision
(could be exploited, for example, by the threat of input of corrupted data)
Lack of formal procedure for user registration and de-registration
(could be exploited, for example, by the threat of unauthorized access)
Lack of control of off-premise assets
(could be exploited, for example, by the threat of theft)
Lack or insufficient Service Level Agreement
(could be exploited, for example, by the threat of maintenance error)
Lack or insufficient 'clear desk and clear screen' policy
(could be exploited, for example, by the threat of information theft)
Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties
(could be exploited, for example, by the threat of unauthorized access)
Lack or insufficient provisions (concerning security) in contracts with employees
(could be exploited, for example, by the threat of fraud and theft)
Lack of continuity plans
(could be exploited, for example, by the threat of technical failure)
Lack of proper allocation of information security responsibilities
(could be exploited, for example, by the threat of repudiation)
Lack of e-mail usage policy
(could be exploited, for example, by the threat of misrouting of messages)
Lack of procedures of risk identification and assessment
(could be exploited, for example, by the threat of unauthorized system access)
Lack of procedures for classified information handling
(could be exploited, for example, by the threat of user errors)

Lack of procedures of provisions compliance with intellectual rights

(could be exploited, for example, by the threat of information theft)

Lack of procedures for reporting security weaknesses

(could be exploited, for example, by the threat of use of network facilities in unauthorized way)

Lack of procedures for introducing software into operational systems

(could be exploited, for example, by the threat of operational staff error)

Lack of change control procedure

(could be exploited, for example, by the threat of maintenance error)

Lack of procedure of monitoring of information processing facilities

(could be exploited, for example, by the threat of unauthorized access)

Lack of regular audits (supervision)

(could be exploited, for example, by the threat of unauthorized access)

Lack of regular management reviews

(could be exploited, for example, by the threat of misuse of resources)

Lack of established monitoring mechanisms for security breaches

(could be exploited, for example, by the threat of willful damage)

Lack of information security responsibilities in job descriptions

(could be exploited, for example, by the threat of user errors)

Lack of fault reports recorded in administrator and operator logs

(could be exploited, for example, by the threat of use of software in an unauthorized way)

Lack of records in administrator and operator logs

(could be exploited, for example, by the threat of operational staff error)

Lack of defined disciplinary process in case of security incident

(could be exploited, for example, by the threat of information theft)

8. Common vulnerabilities in business application processing

Incorrect parameter set up

(could be exploited, for example, by the threat of user error)

Applying application programmes to the wrong data in terms of time

(could be exploited, for example, by the threat of unavailability of data)

Failure to produce management reports

(could be exploited, for example, by the threat of unauthorized access)

Incorrect dates

(could be exploited, for example, by the threat of user errors)

9. Generally applying vulnerabilities

Single point of failure

(could be exploited by, for example, the threat of failure of communications services)

Inadequate service maintenance response

(could be exploited by, for example, the threat of hardware failures improperly designed, inappropriately chosen, and poorly operated safeguards

(could be exploited by, for example, the threat of communications infiltration)

C.2 Methods for vulnerability assessment

Information system testing

Proactive methods such as information system testing can be used to identify vulnerabilities efficiently, depending on the criticality of the ICT system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include:

- automated vulnerability scanning tool,
- security testing and evaluation (STE), and
- penetration testing.

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], sendmail relaying). It should be noted, however, that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

Security testing and evaluation (STE) is another technique that can be used in identifying ICT system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an ICT system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the ICT system are secured. Penetration testing, when used in the risk assessment process, can be used to assess an ICT system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the ICT system from the viewpoint of a threat source and to identify potential failures in the ICT system protection schemes.

The results of these types of security testing will help identify a system's vulnerabilities.

It is important to note that penetration tools and techniques can give false results unless the vulnerability is successfully exploited. To exploit particular vulnerabilities one needs to know the exact system/ application/ patches setup on tested system. If those data are not known at the time of testing, it might not be possible to successfully exploit particular vulnerability (for example, gaining remote reverse shell); however, it is still possible to crash or restart a tested process or system. In such a case, the tested object should be considered as vulnerable as well.

Annex D Information security risk assessment approaches

(informative)

D.1 High-level information security risk assessment

The high-level assessment allows definition of the priorities and chronology in the actions. For various reasons, such as budget, it may not be possible to implement all controls simultaneously and only the most critical risks can be addressed through the risk treatment process. Besides, it can be premature to begin detailed risk management if implementation is only envisaged within one or two years. To reach this objective, the high-level assessment may begin with a high-level assessment of consequences instead of starting with a systematic analysis of threats, vulnerabilities, assets and consequences.

Another reason to start with the high-level assessment is to synchronize with other plans related to change management (or business continuity). For example, it is not sound to completely secure a system or application if it is planned to outsource it in the near future although it may still be worth doing the risk work in order to sort out the outsource contact.

Features of the high-level risk assessment iteration may include the following.

- The high-level risk assessment may address a more global or generic view of the organization and its information systems, considering the technology aspects as independent from the business issues. By doing this, the context analysis concentrates more on the business and operational environment than technological components.

- The high-level risk assessment may address a more limited and generic list of threats and vulnerabilities grouped in defined domains or, to expedite the process, it may focus on risk or attack scenarios instead of their elements.

- Risks presented in a high-level risk assessment are frequently more general risk domains than specific identified risks. As the scenarios or the threats are grouped in domains, the risk treatment proposes lists of controls in this domain. The risk treatment activities try then first to propose and select common controls that are valid across the whole system.

- However, the high-level risk assessment, because it seldom addresses technology details, is more appropriate to provide organizational and non-technical controls and generic management aspects of technical controls, or key generic and common technical safeguards such as back-ups and anti-virus.

The advantages of a high-level risk assessment are as follows.

- The incorporation of an initial simple approach is likely to gain acceptance of the risk assessment programme.

- It should be possible to build a strategic picture of an organizational security programme, i.e. it will act as a good planning aid.

- Resources and money can be applied where they are most beneficial, and systems likely to be in the greatest need of protection will be addressed first.

- The subsequent actions will be more successful.

As the initial risk analyses are at a high level, and potentially less accurate, the only potential disadvantage is that some processes or systems may not be identified as requiring a second, detailed risk assessment. This can be avoided if there is adequate information on all aspects of the organization and its information and systems.

The high-level risk assessment considers the business values of the information systems and the information handled, and the risks from the organization's business point of view. At the first decision point, several factors assist in determining whether the high-level assessment is adequate to treat risks; these factors may include the following:

- the business objectives to be achieved by using various information systems,
- the degree to which the organization's business depends on each information system, i.e. whether functions that the organization considers critical to its survival or the effective conduct of business are dependent on each system, or on the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of the information stored and processed on this system,
- the level of investment in each information system, in terms of developing, maintaining, or replacing the system, and
- the assets of the information system, for which the organization directly assigns value.

When these factors are assessed, the decision becomes easier. If the objectives of a system are extremely important to an organization's conduct of business, or if the assets are at high risk, then a second iteration, the detailed risk assessment, should be conducted for the particular information system (or part thereof).

A general rule to apply is: if the lack of information security can result in significant adverse consequences to an organization, its business processes or its assets, then a second iteration risk assessment, at more detailed level, is necessary to identify potential risks.

D.2 Detailed information security risk assessment

The detailed information security risk assessment process involves in-depth identification and valuation of assets, the assessment of threats to those assets, and assessment of vulnerabilities. The results from these activities are then used to assess the risks and then identify justified security controls.

The detailed step usually requires considerable time, effort and expertise, and may therefore be most suitable for information systems at high risk.

The final stage of the detailed information security risk assessment is to assess the overall risks, which is the focus of this Annex. As identified earlier, assets that have value and have some degree of vulnerability are at risk whenever a threat to the assets exists. The assessment of the risks is a combination of the potential adverse business consequences of unwanted incidents, and the level of assessed threats and vulnerabilities. The risks are in effect measures of the exposure to which a system, and the associated organization, may be subjected. Risks are a function of:

- the asset values,
- the threats, and their associated likelihood of the occurrence, that may threaten the assets.
- the ease of exploitation of vulnerabilities by threats to cause harm, and
- the existing or planned controls, which might reduce the severity of vulnerabilities, threats and consequences.

The objective of risk assessment is to identify and evaluate the risks to which information and systems are exposed, in order to treat the risks appropriately. When assessing the risks, several aspects are considered including consequences and likelihood.

Consequences may be assessed in several ways, including using quantitative, e.g. monetary, and qualitative measures (which can be based on the use of adjectives such as moderate or severe), or a combination of both. To assess the likelihood of threat occurrence, the time frame over which the asset will have value or needs to be protected should be established. The likelihood of a threat occurring is affected by the following:

- the attractiveness of the asset, applicable when a deliberate human threat is being considered,
- the ease of conversion of the asset into reward, applicable if a deliberate human threat is being considered,
- the technical capabilities of the threat agent, applicable to deliberate human threats;
- the likelihood of the threat, and
- the susceptibility of the vulnerability to exploitation, applicable to both technical and non-technical vulnerabilities.

Many methods make use of tables, and combine subjective and empirical measures.. It is more important that the organization uses a method with which they are comfortable, have confidence and that will produce repeatable results. A few examples of table-based techniques are given below.

Example 1 Matrix with predefined values:

In risk assessment methods of this type, actual or proposed physical assets are valued in terms of replacement or reconstruction costs (i.e. quantitative measurements). These costs are then converted onto the same qualitative scale as that used for information (see below). Actual or proposed software assets are valued in the same way as physical assets, with purchase or reconstruction costs identified and then converted to the same qualitative scale as that used for information. Additionally, if any application software is found to have its own intrinsic requirements for confidentiality or integrity (for example if source code is itself commercially sensitive), it is valued in the same way as for information.

The values for information are obtained by interviewing the selected business personnel (the 'data owners') who can speak authoritatively about the data, to determine the value and sensitivity of the data actually in use, or to be stored, processed or accessed. The interviews facilitate assessment of the value and sensitivity of the information in terms of the worst case scenarios that could be reasonably expected to happen from adverse business consequences due to unauthorized disclosure, unauthorized modification, non-availability for varying time periods, and destruction.

The valuation is accomplished using information valuation guidelines, which cover such issues as:

- personal safety,
- personal information,
- legal and regulatory obligations,
- law enforcement,
- commercial and economic interests,
- financial loss/disruption of activities,
- public order,
- business policy and operations, and
- loss of goodwill.

The guidelines facilitate identification of the values on a numeric scale, such as the 1 to 4 scale shown in the example matrix below, thus enabling the recognition of quantitative values where possible and logical, and qualitative values where quantitative values are not possible, e.g. for endangerment of human life.

The next major activity is the completion of pairs of questionnaires for each threat type, for each grouping of assets that a threat type relates to, to enable the assessment of the levels of threats (likelihood of occurrence)

and levels of vulnerabilities (ease of exploitation by the threats to cause adverse consequences). Each question answer attracts a score. These scores are accumulated through a knowledge base and compared with ranges. This identifies threat levels on say a high to low scale, and vulnerability levels similarly, as shown in the example matrix below, differentiating between the types of consequences as relevant. Information to complete the questionnaires should be gathered from interviews with appropriate technical, personnel and accommodation people, and physical location inspections and reviews of documentation.

Threat types to be considered are broadly grouped under: deliberate unauthorized actions by people, environmental matters, errors by people, and equipment/software/line failure.

The asset values, and the threat and vulnerability levels, relevant to each type of consequence, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 8. The values are placed in the matrix in a structured manner. An example is given below:

	Levels of Threat	Low			Medium			High		
	Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Table 1

For each asset, the relevant vulnerabilities and their corresponding threats are considered. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the consequence of the threat and the vulnerability. For example, if the asset has the value **3**, the threat is '**high**' and the vulnerability '**low**', the measure of risk is **5**. Assume an asset has a value of 2, e.g. for modification, the threat level is 'low' and the vulnerability is 'high', then the measure of risk is 4. The size of the matrix, in terms of the number of threat severity categories, vulnerability severity categories, and the number of asset valuation categories, can be adjusted to the needs of the organization. Additional columns and rows will necessitate additional risk measures. The value of this approach is in ranking the risks to be addressed.

Example 2 Ranking of Threats by Measures of Risk:

A matrix or table can be used to relate the factors of consequences (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects). The first step is to evaluate the consequences (asset value) on a predefined scale, e.g., 1 through 5, of each threatened asset (column 'b' in the table). The second step is to evaluate the likelihood of threat occurrence on a predefined scale, e.g., 1 through 5, of each threat (column 'c' in the table). The third step is to calculate the measure of risk by multiplying (b x c). Finally the threats can be ranked in order of their associated measure of risk. Note that in this example, 1 is taken as the lowest consequence and the lowest likelihood of occurrence.

Threat descriptor (a)	Consequence (asset) value (b)	Likelihood of threat occurrence (c)	Measure of risk (d)	Threat ranking (e)
Threat A	5	2	10	2
Threat B	2	4	8	3

Threat C	3	5	15	1
Threat D	1	3	3	5
Threat E	4	1	4	4
Threat F	2	4	8	3

Table 2

As shown above, this is a procedure which permits different threats with differing consequences and likelihood of occurrence to be compared and ranked in order of priority, as shown here. In some instances it will be necessary to associate monetary values with the empirical scales used here.

Example 3 Assessing a value for the likelihood and the possible consequences of risks:

In this example, the emphasis is placed on the consequences of information security incidents and on determining which systems should be given priority. This is done by assessing two values for each asset and risk, which in combination will determine the score for each asset. When all the asset scores for the system are summed, a measure of risk to that ICT system is determined.

First, a value is assigned to each asset. This value relates to the potential adverse consequences that can arise if the asset is threatened. For each applicable threat to the asset, this asset value is assigned to the asset.

Next a likelihood value is assessed. This is assessed from a combination of the likelihood of the threat occurring and the ease of exploitation of the vulnerability, see Table 3.

Levels of Threat	Low			Medium			High		
Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Likelihood Value	0	1	2	1	2	3	2	3	4

Table 3

Next, an asset/threat score is assigned by finding the intersection of asset value and likelihood value in Table 4. The asset/threat scores are totaled to produce an asset total score. This figure can be used to differentiate between the assets forming part of a system.

Asset Value	0	1	2	3	4
Likelihood Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

Table 4

The final step is to total all the asset total scores for the assets of the system, producing a system score. This can be used to differentiate between systems and to determine which system's protection should be given priority.

In the following examples all values are randomly chosen.

Suppose System S has three assets A1, A2 and A3. Also suppose there are two threats T1 and T2 applicable to system S. Let the value of A1 be 3, similarly let the asset value of A2 be 2 and the asset value of A3 be 4.

If for A1 and T1 the threat likelihood is low and the ease of exploitation of the vulnerability is medium, then the likelihood value is 1 (see Table 3).

The asset/threat score A1/T1 can be derived from Table 4 as the intersection of asset value 3 and likelihood value 1, i.e. 4. Similarly, for A1/T2 let the threat likelihood be medium and the ease of exploitation of a vulnerability be high, giving an A1/T2 score of 6.

Now the total asset score A1T can be calculated, i.e., 10. The total asset score is calculated for each asset and applicable threat. The total system score is calculate by adding A1T + A2T + A3T to give ST.

Now different systems can be compared to establish priorities, and different assets within one system as well.

Above example shows in terms of ICT systems, however similar approach can be applied to business processes.

Example 4 Distinction between tolerable and intolerable risks:

Another way of assessing the risks is to only distinguish between tolerable and non-tolerable risks. The background of this is that the assessment of risks are only used to rank the risks in terms of where action is needed most urgently, and the same can be achieved with less effort.

With this approach, the matrix used simply does not contain numbers but only **T**s and **N**s stating whether the corresponding risk is tolerable or not. For example, the matrix of Method 3 could be changed into:

Asset Value	0	1	2	3	4
Likelihood Value					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Table 5

Again, this is only an example, and it is left to the reader where to draw the line between tolerable and intolerable risks.

Annex E Selection of ICT Controls

E.1 General

In this Annex, controls are suggested according to the security concerns identified by risk assessment, taking into account the threats, and finally the type of information process or system is considered.

Factors which might influence the control selection, like any constraints that have to be considered, any legal or other requirements which have to be fulfilled, etc, are addressed below.

Control selection should always include a balance of operational (non-technical) and technical controls. Operational controls include those which provide physical, personnel, and administrative security.

Physical security controls include strength of internal building walls, key coded door locks, fire suppression systems, and guards. Personnel security covers personnel recruitment checks, (especially people in 'positions of trust'), staff monitoring, and security awareness programmes.

Procedural security includes secure operating procedures documentation, application development and acceptance procedures as well as procedures for information security incident management. Related to this category, it is very important that appropriate business continuity, including contingency planning/disaster recovery, strategy and plan(s) are developed for each system. The plan should include details of the key functions and priorities for recovery, processing needs, and the organizational procedures to follow if a disaster or service interruption occurs. Such plans should include the steps required to control sensitive information being processed or stored, while still permitting the organization to conduct business.

Technical security encompasses hardware and software security as well as communications controls. These controls are selected according to the risks to provide security functionality and assurance. The functionality will cover, for example, identification and authentication, logical access control requirements, audit trail/security logging needs, dial-back security, message authentication, encryption, and so on. Assurance requirements document the level of trust needed in security functions and thus the amount and type of checking, security testing, etc., necessary to confirm that level. In deciding on the complimentary blend of operational and technical controls, there will be different options for implementing the technical security requirements. A technical security architecture should be defined for each option to help identifying that security can be provided as required, and that it is feasible with available technology.

An organization may choose to make use of evaluated products and systems as part of the final system solution. Evaluated products are those that have been examined by a third party. The third party may be another part of the same organization or an independent organization specializing in product and system evaluation. The evaluation may be performed against a set of predetermined criteria that are created specifically for the system being built or it may be a generalized set of criteria that can be used in a variety of situations. The evaluation criteria may specify functional requirements and/or assurance requirements. A number of evaluation schemes exist, many of them sponsored by government and international standards organizations. An organization could decide to make use of evaluated products and systems when it requires confidence that the set of functionality implemented is what is required, and when it needs to trust in the correctness and completeness of the implementation of that functionality. Alternatively, focused pragmatic security testing could provide assurance of confidence in the security provided.

When selecting controls for implementation, a number of factors should be considered including:

- the types of functions performed - prevention, deterrence, detection, recovery, correction, monitoring, and awareness,
- the relative strength of the controls,
- capital, operating and maintenance costs of the controls,

- the help provided to the users to perform their function, and
- ease of use of the control for the user.

Generally, a control will fulfill more than one of these functions. When examining the overall security, or set of controls to be used, a balance should be maintained between the types of functions if at all possible. This helps the overall security to be more effective and efficient. A cost / benefit analysis may be required as well as a trade-off analysis (a method of comparing competing alternatives using a set of criteria which are weighted for relative importance in regard to the particular situation).

There are two different sets of controls, mechanisms and/or procedures, which can be applied to protect information systems. On one hand, there are quite a few organizational control categories that are generally applicable for each information or ICT system if the specific circumstances make them necessary, irrespective of the individual components. Because of their general applicability, controls from these categories should always be considered. Furthermore, many of them are not expensive to implement, since they are based on introducing organizational structures and procedures. On the other hand, there are ICT system specific controls; the selection of these controls depends on the type and characteristics of the ICT system under review. Of course, it is always possible that one or more of these categories or specific controls are not applicable for an ICT system. For example, encryption might not be necessary if the information sent or received has no need for confidentiality, and integrity can be checked otherwise. More detailed selections can only be made by considering further information. After all control types applicable for the ICT system considered are identified, further information on these control types and on specific controls can be obtained by using one or more of the documents in the Bibliography. Before implementing the controls selected, they should be checked carefully against the controls already in place and/or planned. The use of a more detailed analysis should be considered to select additional controls. If controls are selected according to different criteria (e.g. baseline controls and additional controls), the final set of controls to be implemented should be put together carefully. After reviewing several ICT systems, it should be considered whether an organization-wide baseline could be established. Another possibility of selecting controls without a detailed consideration is to apply application-specific baselines. For example, there are baseline manuals available for telecommunications, health care, banking, and many more. When using these manuals, it is, for example, possible to check the existing or planned controls against the ones recommended.

The process of control selection always requires some knowledge of the type and characteristic of the information system considered (for example, a stand-alone workstation, or a workstation connected to a network), since this has significant influence on the controls selected to protect the system. Also, it is helpful to have an idea of the infrastructure, in terms of buildings, rooms, etc. Another important factor involved in the selection of controls is the assessment of existing and/or planned controls. This avoids unnecessary work, and waste of time, effort, and money. Hence, it is highly recommended that the risk assessment process described in Clause 5 be always used as a basis for the selection of controls. When selecting controls, business requirements and the organization's approach to security should be taken into account.

E.2 Selection of controls according to the type of ICT system

Identification of the Type of ICT System

For the assessment of an existing or planned ICT system, the ICT system considered should be compared with the following components, and the components representing the system should be identified. In the following clauses, controls are suggested for each of the components listed below. Components to choose from are:

- stand-alone workstation,
- workstation (client without shared resources) connected to a network, and
- server or workstation with shared resources connected to a network.

Identification of Physical/Environmental Conditions

The assessment of the environment includes the identification of the physical infrastructure supporting the existing and planned ICT system, as well as related existing and/or planned controls. Since all controls should be compatible with the physical environment, these assessments are essential for a successful selection. When considering the infrastructure, the following questions can be helpful. Additionally, the reader should think of the environment of the organization and any special circumstances that need to be taken into account.

- Perimeter and building
  - Where is the building situated - within its own site with a perimeter fence, or on the street at a place with lots of traffic etc.?
  - Is the building single or multi-occupancy?
  - If multi-occupancy, who are the other occupants?
  - Where are the sensitive/critical areas?
- Access control
  - Who has access to the building?
  - Is there a physical access control system in place?
  - How robust is the structure of the building?
  - How robust are the doors, windows etc. and what protection is afforded to them?
  - Is the building guarded and if so is it for 24 hours per day or only during working hours?
  - Is the building and/or room housing critical ICT equipment fitted with intruder alarms?
- Protection in place
  - How is (are) the rooms(s) containing the ICT system protected?
  - What fire detection, alarm, and suppression facilities are fitted and where?
  - What water/liquid leakage detection, alarm and dissipation facilities are fitted and where?
  - Are support utilities like UPS, plumbing and air conditioning (to control the temperature and humidity) in place?

By answering these questions, the existing physical and related controls can easily be identified. It is worth noting that it is not a time consuming exercise when considering a building location to identify issues concerning the doors, locks and physical access controls and procedures at the same time.

Detailed information on control selection in defined security areas can be found in ISO/IEC 17799: 2005.

E.3 Selection of controls according to security concerns and threats

The selection of controls according to security concerns and threats described in this clause can be used in the following way.

The first step is to identify and assess the security concerns. The requirements for confidentiality, integrity, availability, accountability, authenticity and reliability should be considered. The strength and number of controls selected should be appropriate to the assessed security concerns. Second, for each of the security

concerns, typical threats are listed and for each threat, controls are suggested according to the ICT system considered. The different types of ICT systems are introduced above and an overview of possible controls is given in the sub-clauses. In this way, it is possible to fulfill specific security needs and to aim the protection at where it is really needed.

Assessment of security concerns

In order to select appropriate controls in an effective way, it is necessary to have an understanding of the security concerns of the business operations supported by the ICT system considered. With the help of the identification of the security concerns, taking into account threats that might realize these concerns, controls can be selected, as described below.

If an assessment according to this clause proves very high security concerns, a more detailed approach is recommended in order to achieve appropriate protection.

Security concerns may include:

- loss of confidentiality,
- loss of integrity,
- loss of availability,
- loss of accountability,
- loss of authenticity, and
- loss of reliability.

An assessment should include the ICT system itself, the information stored or processed on it and the business operations it fulfils. This identifies the objectives of the controls that will be selected. Different parts of an ICT system or of the information stored and processed might have different security concerns. It is important to relate the security concerns directly to the assets since this influences the threats which might apply and hence the selection of controls.

Security concerns can be assessed by considering whether the consequence of a failure or breach in security could cause serious damage, minor damage, or no damage, to business operations. For example, if confidential information is processed on an ICT system, the unauthorized disclosure of this information to a competitor might enable this competitor to make cheaper offers, and hence cause serious damage to the business of the organization. On the other hand, if information available in the public domain were processed on the ICT system, unauthorized disclosure would not cause any damage at all. Consideration of possible threats can help clarify security concerns. The assessment discussed below should be done separately for each asset since the security concerns for different assets might be different. However, where there is sufficient knowledge on security concerns, assets with the same or similar business requirements and security concerns can be summarized in groups.

If there is more than one type of information processed on an ICT system, the different types may need to be considered separately. The protection afforded an ICT system should be sufficient for all kinds of information processed. Thus, if some information has high security concerns, the whole system should be protected appropriately. In the case where the amount of information with high security concerns is small, it might be worthwhile considering moving that information to another system, if that is compatible with the business processes.

Where all possible losses of confidentiality, integrity, availability, accountability, authenticity and reliability are identified as only likely to cause minor damage, either a high level or baseline approach should provide sufficient security for the ICT system considered. Where any of these losses is identified as likely to cause serious damage, it should be assessed whether controls additional to the ones suggested below should be selected.

Loss of confidentiality

Consider the consequences arising from the loss of confidentiality of the asset(s) reviewed (intentional or unintentional). For example, loss of confidentiality might lead to

- loss of public confidence, or deterioration of public image,
- legal liabilities, including those that might arise from breach of data protection legislation,
- adverse effects on organizational policy,
- endangerment of personal safety,
- loss of public confidence, or deterioration of public image, and
- financial loss.

In accordance with the answers to the questions above, it should be decided whether the consequences that could result from a loss of confidentiality would be serious, minor or none. This decision should be documented.

Loss of integrity

Consider the consequences arising from the loss of integrity of the asset(s) reviewed (intentional or unintentional). For example, loss of integrity might lead to

- incorrect decisions being made,
- fraud,
- disruption of business functions,
- loss of public confidence, or deterioration of public image,
- financial loss, and
- legal liabilities, including those that might arise from breach of data protection legislation.

In accordance with the answers to the questions above, it should be decided whether the adverse consequences that could result from a loss of integrity would be serious, minor or none. This decision should be documented.

Loss of availability

Consider the consequences arising from other than short-term loss of availability of applications or information, i.e. which business functions, if interrupted, would result in response or completion times not being met. The extreme form of loss of availability, permanent loss of data and/or physical destruction of hardware or software, should be considered as well. For example, the loss of availability of critical applications or information might lead to

- incorrect decisions being made,
- inability to perform critical tasks,
- loss of public confidence, or deterioration of public image,

- financial loss,
- legal liabilities, including those that might arise from breach of data protection legislation and from not meeting contracted deadlines, and
- significant recovery costs.

It should be noted that the adverse consequences resulting from loss of availability could vary considerably for different time periods of such loss. Where this is the case it will be advisable to consider the consequences that might arise in such different time periods, and assess the consequences for each time period as serious, minor or none (this information should be used in the control selection).

In accordance with the answers to the questions above, it should be decided whether the adverse consequences that could result from a loss of availability would be serious, minor or none. This decision should be documented.

Loss of accountability

Consider the consequences arising from the loss of accountability of users of systems or subjects (e.g. software) acting on the behalf of the user. Additionally, this consideration should include automatically generated messages that can cause an action to occur. For example, loss of accountability might lead to:

- system manipulation by users,
- fraud,
- industrial espionage,
- untraceable actions,
- false accusations and
- legal liabilities, including those that might arise from breach of data protection legislation.

In accordance with the answers to the questions above, it should be decided whether the adverse consequences that could result from a loss of accountability would be serious, minor or none. This decision should be documented.

Loss of authenticity

Consider the consequences arising from the loss of authenticity of data and messages, regardless whether they are used by people or systems. This is particularly important in distributed systems where decisions made are distributed to a wide community or where reference information is used. For example, loss of authenticity might lead to:

- fraud,
- a valid process being used with invalid data leading to a misleading result,
- manipulation of the organization by outsiders,
- industrial espionage,
- false accusations, and

- legal liabilities, including those that might arise from breach of data protection legislation.

In accordance with the answers to the questions above, it should be decided whether the adverse consequences that could arise from a loss of authenticity would be serious, minor or none. This decision should be documented.

Loss of reliability

Consider the consequences arising from the loss of reliability of systems. Moreover, it is important to address functionality that is a sub-characteristic of reliability (see ISO 9126: date). For example, loss of reliability might lead to:

- fraud,
- lost market share,
- demotivated staff,
- unreliable suppliers,
- loss of customer confidence and
- legal liabilities, including those that might arise from breach of data protection legislation.

In accordance with the answers to the questions above, it should be decided whether the adverse consequences that could result from a loss of reliability would be serious, minor or none. This decision should be documented.

Controls for confidentiality

The threat types that might endanger confidentiality are listed below, with controls to protect against these threats suggested. If relevant for the control selection, the type and characteristics of the ICT system should be taken into account.

It should be noted that most of the controls discussed provide a more 'general' protection, i.e. they are aimed at a range of threats and provide protection by supporting an overall effective information security management. Hence, they are not listed here in detail, but their effect is not to be underestimated and they should be implemented for an overall effective protection. The threats are ordered alphabetically.

Eavesdropping

A way of getting access to sensitive information is eavesdropping, for example by tapping a line or listening to a telephone conversation. Controls against that are listed below.

- Physical Controls: These can be rooms, walls, buildings, etc., which make eavesdropping impossible or hard to do. Another way to do that is to add noises. In case of telephones, appropriate cabling can provide some protection against eavesdropping.
- Information security policy: Another way to avoid eavesdropping is to have strict rules about when, where and in which way sensitive information should be exchanged.
- Data confidentiality protection: Another way to protect against eavesdropping is to encrypt the message before it is exchanged.

Electromagnetic radiation

Electromagnetic radiation can be used by an attacker to obtain knowledge about information processed on an ICT system. Controls against electromagnetic radiation are listed below.

- Physical controls: These can be cladding for rooms, walls etc, and these controls do not permit electromagnetic radiation to go beyond the cladding.
- Data confidentiality protection: It should be noted that this protection only applies as long as the information is encrypted, and not for information that is processed, displayed or printed.
- Use of ICT equipment with low radiation: Equipment with built-in protection can be obtained.

Malicious code

Malicious code can lead to a loss of confidentiality, e.g. via the capture and disclosure of passwords. Controls against that are listed below.

- Protection against malicious code,
- Information security incident management: The timely reporting of any unusual incident can limit the damage in case of malicious code attacks. Intrusion detection can be used to detect attempts to gain entry to a system or network.

Masquerading of user identity

Masquerading of user identity can be used to circumvent authentication and all services and security functions related to that. In conclusion it can lead to confidentiality problems whenever this masquerade allows access to sensitive information. Controls in this area are listed below.

- I&A: Masquerade becomes more difficult if I&A controls based on combinations of something known, something possessed as well as intrinsic characteristics of users are applied.
- Logical access control and audit: Logical access control cannot distinguish between an authorized user and somebody masquerading as this authorized user, but the use of access control mechanisms in place can reduce the area of impact. Review and analysis of audit logs can detect unauthorized activities.
- Protection against malicious code: Since one of the ways to get hold of passwords is to introduce malicious code to capture passwords, protection against such software should be in place.
- Network management: Another way of getting hold of sensitive material is to masquerade as a user in traffic, e.g. e-mail. ISO/IEC is currently working on several documents containing further information about detailed controls for network security.
- Data confidentiality protection: If, for some reason, the above type of protection is not possible or not sufficient, additional protection can be provided using storage encryption of the sensitive data.

Misrouting/re-routing of messages

Misrouting is the deliberate or accidental wrong directing of messages, whereas re-routing can take place for both, good and bad purposes. Re-routing can for example be done to maintain integrity of availability.

Misrouting and re-routing of messages can lead to a loss of confidentiality if it allows unauthorized access to these messages. Controls against that are listed below.

- Network management: Controls to protect against misrouting and re-routing can be found in other documents ISO/IEC is currently developing containing further information about detailed controls for network security.

- Data confidentiality protection: In order to avoid unauthorized access in case of misrouting or re-routing, the messages can be encrypted.

Software failure

Software failures can endanger confidentiality if that software is protecting confidentiality, for example, access control or encryption software, or if the software failure causes a loophole e.g. in an operating system. Controls to protect confidentiality in this case are listed below.

- Incident management: Everybody noticing a malfunction of software should report that to the responsible person so action can be taken as soon as possible.

- Operational issues: Some software failures can be avoided by thorough testing of the software before it is used, and through software change control.

Theft

Theft can endanger confidentiality if the ICT component stolen has any sensitive information on it that can be accessed by the thief. Controls against theft are listed below.

- Physical controls: This can be material protection making access to the building, area or room containing the ICT equipment more difficult, or specific controls against theft.

- Personnel: Controls for personnel (controlling outside personnel, confidentiality agreements, etc.) should be in place making theft difficult.

- Data confidentiality protection: This control should be implemented if theft of ICT equipment containing sensitive information seems likely, e.g. laptops.

- Media controls: Any media containing sensitive material should be protected against theft.

Unauthorized access to computers, data, services and applications

Unauthorized access to computers, data, services and applications can be a threat if access to any sensitive material is possible. Controls to protect against unauthorized access include appropriate identification and authentication, logical access control, audit at the ICT system level, and network segregation at the network level.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Access control mechanisms should be used to provide logical access control. Review and analysis of audit logs can detect unauthorized activities by people with access rights to the system.

- Network segregation: In order to make unauthorized access more difficult, network segregation should be in place.
- Physical access control: Beside logical access control, protection can be provided by physical access control.
- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls should be in place to protect the media from unauthorized access.
- Data confidentiality protection: If, for some reason, the above type of protection is not possible or not sufficient, additional protection can be provided using storage encryption of the sensitive data.

Unauthorized access to storage media

The unauthorized access and use of storage media can endanger confidentiality if any confidential material is stored on that media. Controls to protect confidentiality are listed below.

- Operational issues: Media controls can be applied to provide, for example, physical protection and accountability for the media and assured storage deletion guarantees that nobody can obtain confidential material from a previously deleted medium. Special care should be taken to protect easily removable media, such as floppy discs, back-up tapes and paper.
- Physical security: The appropriate protection of rooms (strong walls and windows as well as physical access control) and security furniture can protect against unauthorized access.
- Data confidentiality protection: Additional protection for sensitive material on storage media can be achieved by encrypting the material. A good key management system is necessary to allow the trouble-free application of encryption.

Controls for integrity

The threat types that might endanger integrity are listed below, with controls to protect against these threats suggested. If relevant for the control selection, the type and characteristics of the ICT system should be taken into account.

Deterioration of storage media

Deterioration of storage media threatens the integrity of anything that is stored on that media. If integrity is important, the following controls should be applied.

- Media controls: Sufficient media controls include integrity verification that detects that stored files have been corrupted.
- Back-ups: Back-ups should be made of all important files, business data, etc. If a loss of integrity is noticed, e.g. via media controls or during the back-up testing, the back-up or a previous generation of the back-up should be used to restore the integrity of the files.
- Data integrity protection: Cryptographic means can be used to protect the integrity of data in storage.

Maintenance error

If maintenance is not done regularly or mistakes are made during the maintenance process, the integrity of all related information is threatened. Controls to protect integrity in this case are listed below.

- Maintenance: Correct maintenance is the best way to avoid maintenance errors. This includes documented and verified maintenance procedures, and appropriate supervision of work.
- Back-ups: If maintenance errors have taken place, back-ups can be used to restore the integrity of the damaged information.
- Data integrity protection: Cryptographic means can be used to protect the integrity of information.

Malicious code

Malicious code can lead to a loss of integrity, e.g. if data or files are altered by the person who gains unauthorized access with help of malicious code or by the malicious code itself. Controls against that are listed below.

- Protection against malicious code.
- Incident management: The timely reporting of any unusual incident can limit the damage in case of malicious code attacks. Intrusion detection can be used to detect attempts to gain entry to a system or network.

Masquerading of user identity

Masquerading of user identity can be used to circumvent authentication and all services and security functions related to that. In conclusion it can lead to integrity problems whenever this masquerade allows access and modification to information. Controls in this area are listed below.

- I & A: Masquerade becomes more difficult if I & A controls based on combinations of something known, something possessed as well as intrinsic characteristics of users are applied.
- Logical access control and audit: Logical access control cannot distinguish between an authorized user and somebody masquerading as this authorized user, but the use of access control mechanisms in place can reduce the area of impact. Review and analysis of audit logs can detect unauthorized activities.
- Protection against malicious code: Since one of the ways to get hold of passwords is to introduce malicious code to capture passwords, protection against such software should be in place.
- Network management: Another way of unauthorized access is to masquerade as a user in traffic, e.g. e-mail. ISO/IEC is currently working on several documents containing further information about detailed controls for network security.
- Data integrity protection: If, for some reason, the above type of protection is not possible or not sufficient, additional protection can be provided using cryptographic means like digital signatures.

Misrouting/re-routing of messages

Misrouting is the deliberate or accidental wrong directing of messages, whereas re-routing can take place for both, good and bad purposes. Re-routing can for example be done to maintain integrity of availability. Misrouting and re-routing of messages can lead to a loss of integrity, for example if messages are altered and then sent to the original addressee. Controls against that are listed below.

- Network management: Controls to protect against misrouting and re-routing can be found in other documents ISO/IEC is currently developing containing further information about detailed controls for network security.

- Data integrity protection: In order to avoid unauthorized alteration in case of misrouting or re-routing, hash functions and digital signatures can be used.

Non-repudiation

Controls for non-repudiation should be applied when it is important to have a proof that a message was sent and/or received, and that the network has transported the message. There are specific cryptographic controls as a basis for non-repudiation (data integrity and non-repudiation).

Software failure

Software failures can destroy the integrity of the data and information that is processed with help of this software. Controls to protect integrity are listed below.

- Reporting of software malfunctions: Reporting of software malfunctions as soon as possible helps to limit the damage in the case of software failures.
- Operational issues: Security testing can be used to ensure that software is functioning correctly and software change control can avoid that software problems are caused because of updates or other software changes.
- Back-ups: Back-ups, for example a previous generation, can be used to restore the integrity of data that have been processed by software that is not functioning correctly.
- Data integrity protection: Cryptographic means can be used to protect the integrity of information.

Supply failure (power, air conditioning)

Supply failures can cause integrity problems, if, because of them, other failures are caused. For example, supply failures can lead to hardware failures, technical failures or to problems with storage media. Controls against those specific problems can be found in the respective subsections; controls against supply failures are listed below.

- Power and air conditioning: Suitable power supply and air conditioning related controls, e.g. power surge protection, should be used where necessary to avoid any problems resulting from supply failure.
- Back-ups: Back-ups should be used to restore any information that has been damaged.

Technical failure

Technical failures, for example in a network, can destroy the integrity of any information that is stored or processed in that network. Controls to protect against this are listed below.

- Operational issues: Configuration and change management, as well as capacity management, should be used to avoid failures of any ICT system or network. Documentation and maintenance are used to ensure the trouble-free running of the system or network.
- Network management: Operational procedures, system planning and proper network configuration should be used to minimize the risks of technical failures.
- Power and air conditioning: Suitable power supply and air conditioning related controls, e.g. power surge protection, should be used where necessary to avoid any problems resulting from supply failure.
- Back-ups: Back-ups should be used to restore any information that has been damaged.

Transmission errors

Transmission errors can destroy the integrity of the information transmitted. Controls to protect integrity are listed below.

- Cabling: Careful planning in laying of cables can avoid transmission errors, for example, if the error is caused by overloading.

- Network management: Network equipment should be properly operated and maintained to avoid transmission errors. ISO/IEC is currently working on several documents containing further information about detailed controls for network security that can be used to protect against transmission errors.

- Data integrity protection: Checksums or cyclic redundancy codes in communication protocols can be used to protect against accidental transmission errors. Cryptographic means can be used to protect the integrity of data in transit in case of deliberate attacks.

Unauthorized access to computers, data, services and applications

Unauthorized access to computers, data, services and applications can be a threat to the integrity of this information if unauthorized alteration is possible. Controls to protect against unauthorized access include appropriate identification and authentication, logical access control, audit at the ICT system level, and network segregation at the network level.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Controls should be used to provide logical access control, through the use of access control mechanisms. Review and analysis of audit logs can detect unauthorized activities by people with access rights to the system.

- Network segregation: In order to make unauthorized access more difficult, network segregation should be in place.

- Physical access control: Beside logical access control, protection can be provided by physical access control.

- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls should be in place to protect the media from unauthorized access.

- Data integrity: Cryptographic means can be used to protect the integrity of information in storage or in transit.

Use of unauthorized programmes and data

Use of unauthorized programmes and data endangers the integrity of information stored and processed on the system where that happens, if the programmes and data are used to alter the information in an unauthorized way, or if the programmes and data that are used contain malicious code (e.g. games). Controls to protect against this are listed below.

- Security awareness and training: All employees should be aware of the fact that they should not install and use any software without the allowance of the ICT system security manager, or the person responsible for the security of the system.

- Back-ups: Back-ups should be used to restore any information that has been damaged.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Logical access control should ensure that only authorized persons can apply software to process and alter information. Review and analysis of audit logs can detect unauthorized activities.

- Protection from malicious code: All programmes and data should be checked for malicious code before it is used.

Unauthorized access to storage media

The unauthorized access and use of storage media can endanger integrity since it allows unauthorized alteration of the information stored on these media. Controls to protect integrity are listed below.

- Operational issues: Media controls can be applied to provide, for example, physical protection and accountability for the media to avoid unauthorized access, and integrity verification to detect any compromise of the integrity of information stored on the media. Special care should be taken to protect easily removable media, such as floppy discs, back-up tapes and paper.

- Physical security: The appropriate protection of rooms (strong walls and windows as well as physical access control) and security furniture can protect against unauthorized access.

- Data integrity: Cryptographic means can be used to protect the integrity of information stored on the media.

User error

User errors can destroy the integrity of information. Controls against that are listed below.

- Security awareness and training: All users should be trained appropriately to avoid user errors when processing information. This should include training on defined procedures for specific actions, such as operational or security procedures.

- Back-ups: Back-ups, for example a previous generation, can be used to restore the integrity of information that has been destroyed because of user errors.

Controls for availability

The threat types that might endanger availability are listed below, with controls to protect against these threats suggested. If relevant for the control selection, the type and characteristics of the ICT system should be taken into account.

It should be noted that most of the controls discussed provide a more 'general' protection, i.e. they are not aiming at specific threats but provide protection by supporting an overall effective information security management. Hence, they are not listed here in detail, but their effect is not to be underestimated and they should be implemented for an overall effective protection.

The availability demands can range from not time-critical data or ICT systems (but the loss of such data and unavailability of such systems is still considered critical) to highly time-critical data or ICT systems. The former can be protected against by back-ups whereas the latter may require some resilience system to be present. The threats are ordered alphabetically.

Destructive attack

Information can be destroyed by destructive attacks. Controls to protect against that are listed below.

- Disciplinary process: All employees should be aware of the consequences if they (intentionally or unintentionally) destroy information.
- Media controls: All media should be appropriately protected from unauthorized access using physical protection and accountability for all media.
- Back-ups: Back-ups should be made of all important files, business data, etc. If a file or any other information is not available (for whatever reason), a back-up or a previous generation of the back-up should be used to restore the information.
- Material protection: Physical access controls should be used to avoid any unauthorized access that would facilitate to unauthorized destruction of ICT equipment or information.
- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.
- Logical access control and audit: Logical access control should ensure that no unauthorized access to information that allows the destruction of that information can take place. Review and analysis of audit logs can detect unauthorized activities.

Deterioration of storage media

Deterioration of storage media threatens the availability of anything that is stored on that media. If availability is important, the following controls should be applied.

- Media controls: Regular testing of storage media should detect any deterioration, hopefully before the information is really unavailable. The media should be stored in a way that any outside influence that could cause deterioration cannot take place.
- Back-ups: Back-ups should be made of all important files, business data, etc. If a file or any other information is not available (for whatever reason), a back-up or a previous generation of the back-up should be used to restore the information.

Failure of communication equipment and services

Failure of equipment and communication services threatens the availability of information communicated via these services. Controls to protect the availability are listed below.

- Redundancy and Back-ups: Redundant implementation of communication services components can be used to lower the likelihood of communication services failures. Depending on the maximal acceptable downtime, standby equipment may be used to fulfill the requirements as well. In any case, configuration and layout data should be backed up to ensure availability in case of an emergency.
- Network management: ISO/IEC is currently working on several documents containing further information about detailed controls for network security that can be applied to protect against failures of communications equipment or services.
- Cabling: Careful planning in laying of cables can avoid damages; if there is a suspicion that a line might be damaged it should be inspected.

- Non-repudiation: If a proof of network delivery, or sending or receiving of a message is needed, non-repudiation should be applied; then communication failures or missing information could be easily detected.

Fire, water

Information and ICT equipment can be destroyed by fire and/or water. Controls to protect against fire and water are listed below.

- Physical protection: All buildings and rooms containing ICT equipment or media on which important information is stored should be protected appropriately against fire and water.
- Business continuity plan: In order to protect business from the disastrous effects of fire and water, a business continuity plan should be in place, and back-ups of all important information should be available.

Maintenance error

If maintenance is not done regularly or mistakes are made during the maintenance process, the availability of all related information is threatened. Controls to protect integrity in this case are listed below.

- Maintenance: Correct maintenance is the best way to avoid maintenance errors.
- Back-ups: If maintenance errors have taken place, back-ups can be used to restore the availability of the lost information.

Malicious code

Malicious code can be used to circumvent authentication and all services and security functions related to that. In conclusion it can lead to a loss of availability, e.g. if data or files are destroyed by the person gaining unauthorized access with help of malicious code or by the malicious code itself. Controls against that are listed below.

- Protection against malicious code;
- Incident management: The timely reporting of any unusual incident can limit the damage in case of malicious code attacks. Intrusion detection can be used to detect attempts to gain entry to a system or network.

Masquerading of user identity

Masquerading of user identity can be used to circumvent authentication and all services and security functions related to that. In conclusion it can lead to availability problems whenever this masquerade leads to possibilities to remove or destroy information. Controls in this area are listed below.

- I & A: Masquerade becomes more difficult if I & A controls based on combinations of something known, something possessed as well as intrinsic characteristics of users are applied.
- Logical access control and audit: Logical access control cannot distinguish between an authorized user and somebody masquerading as this authorized user, but the use of access control mechanisms in place can reduce the area of impact. Review and analysis of audit logs can detect unauthorized activities.

- Protection against malicious code: Since one of the ways to get hold of passwords is to introduce malicious code to capture passwords, protection against such software should be in place.

- Network management: Another way of unauthorized access is to masquerade as a user in traffic, e.g. e-mail. ISO/IEC is currently working on several documents containing further information about detailed controls for network security.

- Data back-up: Data back-up cannot protect against masquerading of user identity but reduces the consequence of damaging incidents resulting from that.

Misrouting/rerouting of messages

Misrouting is the deliberate or accidental wrong directing of messages, whereas re-routing can take place for both, good and bad purposes. Re-routing can for example be done to maintain integrity of availability. Misrouting of messages leads to a loss of availability of the messages. Controls against that are listed below.

- Network management: Controls to protect against misrouting and re-routing can be found in other documents ISO/IEC is currently developing containing further information about detailed controls for network security.

- Non-repudiation: If a proof of network delivery, or sending or receiving of a message is needed, non-repudiation should be applied.

Misuse of resources

Misuse of resources can lead to unavailability of information or services. Controls to protect against that are listed below.

- Personnel: All personnel should be aware of the consequences of misusing resources; disciplinary processes should be applied if necessary.

- Operational issues: The system use should be monitored to detect unauthorized activities, and segregation of duties should be applied to minimize the possibilities of misuse of privileges.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Controls should be used to provide logical access control to resources, through the use of access control mechanisms. Review and analysis of audit logs can detect unauthorized activities.

- Network management: Appropriate network configuration and segregation should be applied to minimize the possibility of misuse of resources in networks.

Natural disasters

In order to protect against loss of information and services because of natural disasters, the following controls should be in place.

- Natural disaster protection: All buildings should be protected as much as possible from natural disasters.

- Business continuity plan: A business continuity plan should be in place and fully tested, for each building, and back-ups of all important information, services and resources should be available.

Software failures

Software failures can destroy the availability of the data and information that is processed by the related software. Controls to protect availability are listed below.

- Reporting of software malfunctions: Reporting of software malfunctions as soon as possible helps to limit the damage if in case of software failures.
- Operational issues: Security testing can be used to ensure that software is functioning correctly and software change control can avoid that software problems are caused because of updates or other software changes.
- Back-ups: Back-ups, for example a previous generation, can be used to restore the data that have been processed by software that is not functioning correctly.

Supply failure (power, air conditioning)

Supply failures can cause availability problems, if, because of them, other failures are caused. For example, supply failures can lead to hardware failures, technical failures or to problems with storage media. Controls against those specific problems can be found in the respective subsections; controls against supply failures are listed below.

- Power and air conditioning: Suitable power supply and air conditioning related controls, e.g. power surge protection, should be used where necessary to avoid any problems resulting from supply failure.
- Back-ups: Back-ups should be made of all important files, business data, etc. If a file or any other information is lost because of supply failures, back-ups should be used to restore the information.

Technical failures

Technical failures, for example in networks, can destroy the availability of any information that is stored or processed in this network. Controls to protect against that are listed below.

- Operational issues: Configuration and change management, as well as capacity management, should be used to avoid failures of any ICT system. Documentation and maintenance are used to ensure the trouble-free running of the system.
- Network management: Operational procedures, system planning and proper network configuration should be used to minimize the risks of technical failures.
- Business continuity plan: In order to protect business from the disastrous effects of technical failures, a business continuity plan should be in place, and back-ups of all important information, services and resources should be available.

Theft

Theft obviously endangers the availability of information and ICT equipment. Controls against theft are listed below.

- Physical controls: This can be material protection making access to the building, area or room containing the ICT equipment and information more difficult, or specific controls against theft.

- Personnel: Controls for personnel (controlling outside personnel, confidentiality agreements, etc.) should be in place making theft difficult.

- Media controls: Any media containing important material should be protected against theft.

Traffic overloading

Traffic overloading threatens the availability of information communicated via these services. Controls to protect the availability are listed below.

- Redundancy and Back-ups: Redundant implementation of communication services components can be used to lower the likelihood of traffic overloading. Depending on the maximal acceptable downtime, standby equipment may be used as well to fulfill the requirements. In any case, configuration and layout data should be backed up to ensure availability in case of an emergency.

- Network management: The proper configuration, management and administration of networks and communication services should be used to avoid overloading.

- Network management: ISO/IEC is currently developing documents containing further information about detailed controls for network security that can be applied to protect against traffic overloading.

Transmission errors

Transmission errors can destroy the availability of the information transmitted. Controls to protect availability are listed below.

- Cabling: Careful planning in laying of cables can avoid transmission errors, for example, if the error is caused by overloading.

- Network management: Network management cannot protect against transmission errors but can be used to recognize problems occurring from transmission errors and to raise alarms in such cases. This allows timely reaction to these problems. ISO/IEC is currently developing documents containing further information about detailed controls for network security that can be applied to protect against transmission errors.

Unauthorized access to computers, data, services and applications

Unauthorized access to computers, data, services and applications can be a threat to the availability of this information if unauthorized destruction is possible. Controls to protect against unauthorized access include appropriate identification and authentication, logical access control, audit at the ICT system level, and network segregation at the network level.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Controls should be used to provide logical access control, through the use of access control mechanisms. Review and analysis of audit logs can detect unauthorized activities by people with access rights to the system.

- Network segregation: In order to make unauthorized access more difficult, network segregation should be in place.

- Physical access control: Besides logical access control, protection can be provided by physical access control.

- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls should be in place to protect the media from unauthorized access.

Use of unauthorized programmes and data

Use of unauthorized programmes and data endangers the availability of information stored and processed on the system where that happens, if the programmes and data are used to delete information, or if the programmes and data that are used contain malicious code (e.g. games). Controls to protect against that are listed below.

- Security awareness and training: All employees should be aware of the fact that they should not implement any software without the authorisation of the ICT system security manager, or the person responsible for the security of the system.

- Back-ups: Back-ups should be used to restore any information, services or resources that has been damaged or lost.

- I & A: Appropriate I & A controls should be used in combination with logical access control to prevent unauthorized access.

- Logical access control and audit: Logical access control should ensure that only authorized persons can apply software to process and delete information. Review and analysis of audit logs can detect unauthorized activities.

- Protection from malicious code: All programmes and data should be checked for malicious code before it is used.

Unauthorized access to storage media

The unauthorized access and use of storage media can endanger availability since it could result in unauthorized destruction of the information stored on these media. Controls to protect availability are listed below.

- Operational issues: Media controls can be applied to provide, for example, physical protection and accountability for the media to avoid unauthorized access to the information stored on the media. Special care should be taken for easily removable media, such as floppy discs, back-up tapes and paper.

- Physical security: The appropriate protection of rooms (strong walls and windows as well as physical access control) and security furniture protect against unauthorized access.

User error

User errors can destroy the availability of information. Controls against that are listed below.

- Security awareness and training: All users should be trained appropriately to avoid user errors when processing information. This should include training on defined procedures for specific actions, such as operational or security procedures.

- Back-ups: Back-ups, for example a previous generation, can be used to restore the information that has been destroyed because of user errors.

Controls for accountability, authenticity and reliability

The scope of accountability, authenticity and reliability differs widely in different domains. These differences mean that a lot of different controls may be applicable. Therefore, only general guidance can be given below.

The controls discussed above provide a more 'general' protection, i.e. they are aimed at a range of threats and provide protection by supporting an overall effective information security management. Hence, they are not listed here, but their effect is not to be underestimated and they should be implemented for an overall effective protection.

Accountability

In order to protect accountability, any threat that may lead to actions taken not being attributable to a specific entity or subject should be considered. Some examples of such threats are account sharing, a lack of traceability of actions, masquerading of user identity, software failure, unauthorized access to computers, data, services and applications, and weak authentication of identity.

There are two types of accountability that should be considered. One type deals with identifying the user accountable for specific actions on information and ICT systems. Audit logs can provide this. The other type is relating to the accountability between users in a system. Non-repudiation services, split knowledge or dual control can achieve this.

Many controls can be used to, or can contribute to, enforcing accountability. Controls ranging from such things as security policies, security awareness, and logical access control and audit, to one-time passwords and media controls, may be applicable. The implementation of a policy for information ownership is a prerequisite for accountability. Selection of specific controls will be dependent upon the specific usage of accountability within the domain.

Authenticity

The confidence in authenticity can be reduced by any threat which may lead to a person, system or process not being sure that an object is what it purports to be. Some examples that may lead to this situation arising include data changes not being controlled, the origin of data not being checked, and the origin of data not being maintained.

Many controls can be used to, or can contribute to, enforcing authenticity. Controls ranging from the use of signed reference data, logical access control and audit, to the use of digital signatures, may be applicable. Selection of specific controls will be dependent upon the specific usage of authenticity within the domain.

Reliability

Any threat that may lead to inconsistent behaviour of systems or processes, will result in reduced reliability. Some examples of such threats are inconsistent system performance and unreliable suppliers. The loss of reliability might result in poor customer service or loss of customer confidence.

Many controls can be used to, or can contribute to, enforcing reliability. Controls ranging from such things as business continuity plans, introduction of redundancy in the physical architecture and system maintenance to identification and authentication, and logical access control and audit, may be applicable. Selection of specific controls will be dependent upon the specific usage of reliability within the domain.

E.4 Baseline approach to risk treatment

The objective of baseline protection is to establish a minimum set of controls to protect all or some information and ICT systems of an organization. Using baseline protection makes it possible to apply organization-wide controls as a start, and then to use an in-depth risk assessment to determine the most suitable controls for systems at high risk or systems critical to the business. The baseline approach can be used as well to treat common risks. Where large or unusual risks are identified, it is necessary to complete risk assessment to determine appropriate treatment options. The risk assessment phase can be made very brief if previous work has established a baseline (or code of practice) for the treatment of specific types of risk. A good source of information for compiling a baseline minimum set of controls for an organization is to refer to a general security code-of-practice.

If all of an organization's information systems have only a low level of security requirements, then selecting baseline protection as the outcome of the risk assessment process can be an acceptable outcome, and it may be the most cost-effective strategy. In this case, the baseline has to be chosen such that it reflects the degree of protection required by the majority of information systems. Most organizations will always need to meet some minimum standards to protect sensitive data in compliance with legislation and regulation, e.g. data protection legislation. However, where an organization's systems vary in business sensitivity, size, and complexity, it would neither be logical nor cost-effective to apply baseline protection to all systems.

The appropriate baseline protection can be achieved through the use of control catalogues, which itemize a set of controls to protect assets, business processes and activities, and information and ICT systems against the most common threats. The level of baseline security can be adjusted to the needs of the organization. If the high-level risk assessment has been conducted and all of the necessary information was available for this, then a detailed step of assessing threats, vulnerabilities and risks may not be necessary. All that has to be done to apply baseline protection is to select those parts of the control catalogue that are relevant for the information or ICT system considered. After identifying the controls already in place, a comparison is made with those controls listed in the baseline catalogue. Those that are not already in place, and are applicable, should be implemented.

Baseline catalogues may specify controls to be used in detail, or they may suggest a set of security requirements to be addressed with whatever controls appropriate to the system under consideration. Both approaches have advantages. Several documents are available that provide sets of baseline controls. Also, sometimes a similarity of environments can be observed among companies within the same industrial sector. After the examination of the basic needs, it may be possible for baseline control catalogues to be used by a number of different organizations. For example, catalogues of baseline controls could be obtained from:

- international and national standards organizations,
- industry sector standards or recommendations, or
- another organization, preferably with similar business objectives, and of comparable size.

An organization may generate its own baseline, established commensurate with its environment, and with its business objectives.

There are a number of advantages to using baseline protection.

- A small amount of resources is needed for risk assessment for each control implementation, and thus less time and effort is spent on selecting security controls.
- Baseline controls may offer a cost-effective solution, as the same or similar baseline controls can be adopted to protect various assets, information systems and business processes without great effort if a large number of the organization's business processes and information systems operate in a common environment and if the security needs are comparable, and, therefore, there will be consistency of security controls throughout the organization.

Applying baseline protection without risk assessment is an unacceptable alternative, for several reasons.

- If the baseline level is set too high, there might be an excessive level of security on some information systems, at an unnecessarily high cost.
- If the level is set too low there may be a lack of security on some information systems, resulting in a higher level of exposure.
- There might be difficulties in managing security relevant changes. For instance, if a system is upgraded, it might be difficult to assess whether the original baseline controls are still sufficient.
- Some risks may be overlooked or ignored leaving the organization vulnerable.

E.4.1 Development of an organization-wide baseline

When an organization decides to apply baseline security either to the whole organization or to parts of it the following questions should be considered.

- Which parts of the organization or systems can be protected by the same baseline, and which require a different consideration, or whether the same baseline should be applied throughout the whole organization?
- What security level should the baseline (or the various baselines) aim at?
- How can the controls forming the different (if necessary) baselines be determined?

The following picture illustrates the various ways baseline security can be applied:

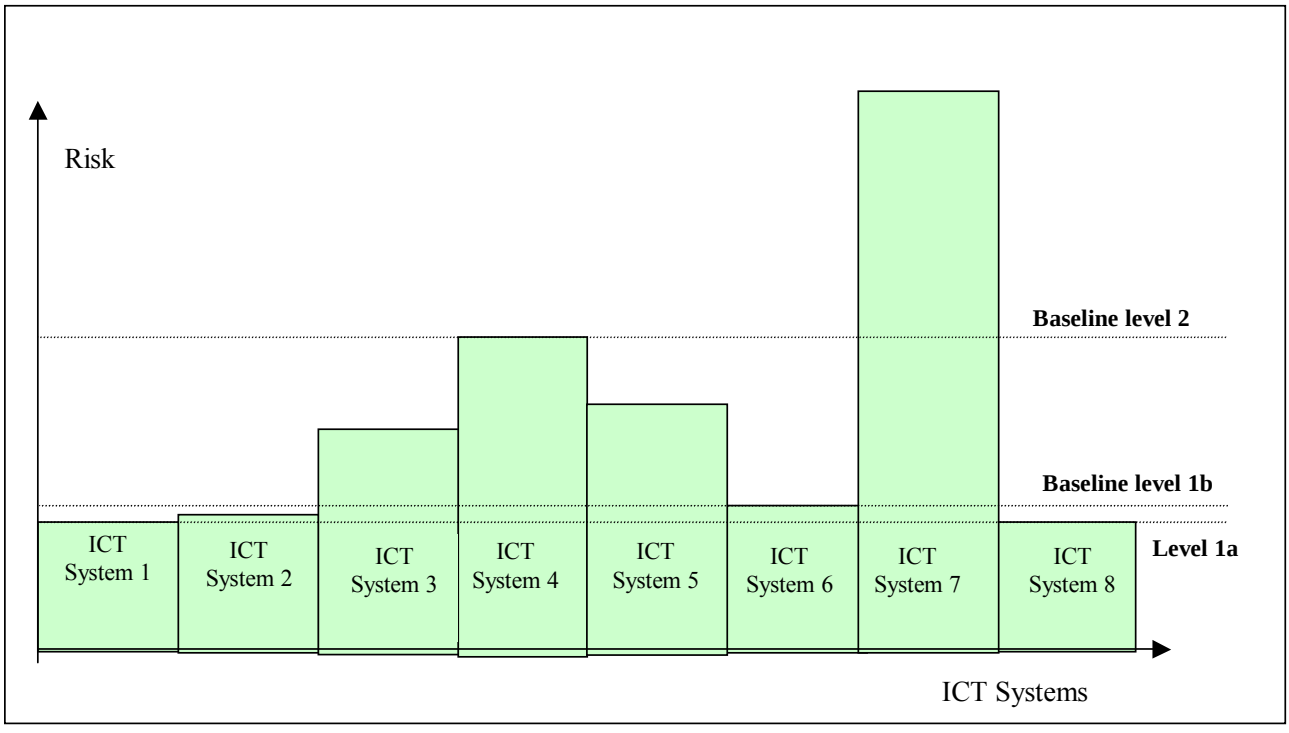

Figure E-1 - Different baseline levels

The advantage of applying different baseline levels within one organization is that most systems will be protected appropriately, i.e. not too little and not too much protection is applied (like for ICT systems 1, 2, 6, and 8 with baseline level 1 and ICT systems 3, 4, and 5 with baseline level 2 in Figure E-1). If ICT systems with different security requirements are 'really different' (in the sense that most of the controls required to protect each of the ICT systems are different), then the application of different baselines is recommended for the organization. If there are fundamentally different security requirements, the decision of using a baseline approach should be re-considered.

If, on the other hand, the only difference between the various baseline levels is that some additional controls are needed to form higher baseline levels, then it might not be worthwhile to implement several different baseline levels. If only one baseline level is implemented, the organizational overhead can be reduced considerably, and everybody within the organization can rely on the same level of security being present.

The level at which baseline security should aim is, of course, related to the decision whether one or more levels of baseline security can logically be implemented. If different baseline levels are chosen, these levels can be adjusted fairly accurately to the security requirements of the ICT systems they are supposed to protect. Generally, any baseline level should not aim at security below the lowest security requirements of the ICT systems to be protected (like below the requirements of ICT system 2 in Figure E-1). It is sensible to aim at a level that is sufficient for most (Baseline level 1a in Figure E-1) or all (Baseline level 1b) of the ICT systems that are supposed to be protected. It is often advisable to aim at the highest security level of the ICT systems to be protected by the baseline controls since this is normally not very expensive but provides sufficient security for all ICT systems involved. A careful consideration of the involved ICT systems is necessary to make the final decision on which ICT systems should be protected by the same baseline. Some ICT systems are very much the same in nature and/or protection requirements – in that case, it is useful to protect them by the same baseline. If, on the other hand, a few ICT systems are totally different in their protection requirements, it is very often the easiest way to consider them separately.

The same is true if an organization decides to implement the same baseline organization-wide. This baseline can aim at three different levels:

- a low level, adding specific controls to protect all information systems with higher requirements,
- a medium level, adding specific controls to protect all information systems with higher requirements, or
- a high level, sufficient to protect all information systems that are protected by baseline security.

As already explained above, a medium or high level for baseline security may be sensible for many of organizations in order to achieve sufficient protection, reliable security throughout the organization and a reduction of organizational overhead. In the end, the decision has to be made according to the organization's security policy and the security requirements of the information systems considered.

Annex F Security awareness and training

F.1 Introduction

Security awareness is an essential element for effective security. The lack of security awareness and consequent poor security practices by personnel within an organization can significantly reduce, and potentially negate, the effectiveness of controls. Individuals within an organization are generally considered to be one of the weakest security links. In order to ensure that an adequate level of security awareness exists within an organization it is important to establish and maintain an effective security awareness programme. The aim of a security awareness programme is to modify people's behaviour enabling them to take responsibility for the protection of information assets of the organization. This may be achieved by explaining to the employees, partners and suppliers:

- the need for security,
- the security objectives, strategies, policies and procedures, and
- each person's roles and responsibilities.

In addition the programme should be designed to motivate employees, partners, contractors, and suppliers, and ensure acceptance of their responsibilities for security.

A security awareness programme should be implemented at all levels in the organization from management to the individuals responsible for day-to-day business activities. It will often be necessary to develop and deliver different awareness material to people in different parts of an organization, and to people with different roles and responsibilities. A comprehensive security awareness programme should be developed and delivered in stages. Each stage builds upon the lessons of the previous, beginning with the concept of security and working through to responsibilities for implementing and monitoring security.

F.2Security awareness programme

The objective of the security awareness programme is to increase the level of awareness within the organization to the point where security becomes second nature and the process becomes a routine that all employees can easily follow. The programme should ensure that the staff and the end users have enough knowledge of the business processes, activities, assets, information system and ICT systems, and that they understand why controls are necessary and how to use them correctly. Only controls accepted by staff and end users can work effectively.

The input to the security awareness programme should come from all levels of the organization. It should include the corporate information security policy and it should cover all objectives of the organizational information security plan. Management support from all departments is necessary for the awareness team. In detail, the following topics should be covered by courses, talks, or any other activities described in the security awareness programme:

- the explanation of the importance of security to both the organization and the individual,
- the security needs and objectives for information systems in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability,
- the implication of security incidents to both the organization and the individual,
- the correct use of information systems, including hardware and software,

- the objectives behind, and an explanation of, the corporate information security policy, any security guidelines and directives, and the risk management strategy, leading into an understanding of risks and controls,
- the necessary protection for and the risks to the information systems,
- restricted access to information areas (authorized personnel, door locks, badges, entrance log) and to information (logical access control, read/update rights), and why these restrictions are necessary,
- the need to report breaches of security or attempts,
- procedures, responsibilities and job descriptions,
- anything the staff and end users should not do because of security factors,
- the consequences if staff are responsible for security breaches,
- the ICT system security plans to implement and check controls,
- why these controls are necessary, and how to use them correctly,
- procedures related to security compliance checking, and
- change and configuration management.

The development of the security awareness programme starts with a review of the security strategies, objectives and policies. This process should be conducted by a team of individuals who are in the position to identify the critical functions of the organization and who have the full support of senior management.

The review team should determine the breakdown of requirements in accordance with the corporate information security policy. This should be combined with overall security initiatives and published in various formats such as awareness posters, periodicals, company bulletins, and internal mail.

The team should then conduct specific briefings on security concerns. A thorough review of the requirements should be conducted to build the required information base for the briefings. Each briefing should be conducted at regular time intervals (e.g. every six months) to ensure that all staff are familiar with the risks inherent in information systems.

The responsibility for determining the objectives and content of the awareness programme should be allocated at the senior management level to the information security forum (see Part 1 of ISO/IEC 13335). The responsibility for its development and implementation should be allocated to the corporate information security officer and to a security awareness development team. This should be done in conjunction with other corporate training and education activities. However, it is within the responsibility of every individual to review and be intimately familiar with the security policies and procedures of their work environment, hence the security awareness programme should be implemented at all levels of the organization.

To develop a security awareness programme that blends with the socio-cultural environment as well as the administrative nature of an organization, the following aspects need to be considered:

- needs analysis,
- programme delivery,
- monitoring, and
- awareness programme content.

F.2.1 Needs analysis

To determine the level of awareness already existing within the target groups (executives, management and employees) and the most acceptable methods of conveying new information to them, it is necessary to perform a security knowledge needs analysis. A needs analysis examines policy, procedures, attitudes, security knowledge and desired performance in relation to current actual performance. Additionally, the needs analysis should target known areas of policy weakness or non-compliance, as high risk. This can be done through different techniques, e.g., interviews, questionnaires, and then compiling outcomes in order to prioritise main security needs.

F.2.2 Programme delivery

A comprehensive security awareness programme should include both interactive and promotional techniques. The focus of this part of an awareness programme should be the deficiencies that were identified through the needs analysis. Employees need to gain an appreciation and understanding that business processes, activities, assets, information and ICT systems are valuable and that the threats to those are real.

One benefit derived from such an organizational security awareness programme is that it provides employees an opportunity to participate in the security programme. Interactive techniques (staff meetings, training courses, etc.) provide two-way communications that allow participants and security personnel to validate the concepts and requirements that resulted from the needs analysis. Promotional techniques (video, email security banners, posters, publications, etc.) are single directional communications methods that allow management to broadcast concepts, information, and attitude in an inexpensive manner.

F.2.3 Monitoring of security awareness programmes

There are three distinct components that comprise effective monitoring of security awareness programmes:

- Periodic performance evaluations - which will determine the effectiveness of an awareness programme by monitoring security related behaviour and identify where changes affecting the programme delivery might be required,

- Awareness change management - whenever there are changes to the overall security programme (i.e. policy or strategy changes, new assets or technology are introduced, variations in threats occur, etc.), or due to staff turnover, there will be a need to alter the security awareness programme to update the existing knowledge and skill levels to reflect those changes, and

- Attendance monitoring – have staff sign attendance forms to create a formal record of attendance. This establishes personally accountability for behaviour when using ICT systems.

F.3 Security training

Besides the general security awareness programme, which should apply to everybody within an organization, specific security training is required for personnel with tasks and responsibilities related to information security. The degree of depth of security training should be dependent on the overall importance information security has for the organization, and should vary according to the security requirements of the performed roles. If necessary, more extensive education, like participation in university lectures, courses etc., should be provided as well. An information security training programme should be developed to cover all security needs relevant for the organization. Another activity is the presentation of courses that train specific employees on the proper security practices. In some circumstances, it may be effective to integrate appropriate security requirements within other training courses or materials required by an organization. This approach should be considered in addition to, or as an alternative to, stand-alone security awareness programmes. Finally, courses are required which provide education at a professional level in very specific security topics.

When determining the personnel for whom specific security training is necessary, the following should be considered:

- personnel with key responsibilities for information and ICT system design and development,
- personnel with key responsibilities for information and ICT system operations,
- corporate, project, information security and ICT system security officers, and
- personnel with security administration responsibilities, e.g., for access control or directory management.

In addition, a check should be made to see if special security training is required for current and planned tasks, projects, etc. Whenever tasks or projects with special security requirements are started, it should be ensured that the corresponding security training programme is developed before the project starts, and that the activities are carried out in time.

The topics covered by the security training courses should be dependent on the role and function of the person participating. General issues could be:

- what is security,
- prevention of breaches of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability,
- potential adverse business consequences, for the organization or the individual,
- information sensitivity categorization scheme,
- the overall security process,
- a description of the overall process,
- risk assessment components,
- controls, and the training necessary to comply with the controls,
- roles and responsibilities, and
- ICT system security policy.

The correct implementation and use of controls is one of the most important issues that should be covered by the security training programme. Each organization should develop its own security training programme according to its needs, and existing or planned controls. The following are examples of control related topics that should be covered, with an emphasis on the need for balance between non-technical and technical controls:

- security policy,
- roles and responsibilities,
- personnel security,
- physical security (including buildings, office areas, equipment rooms, and equipment),
- security infrastructure,
- hardware and software security,
- communications security,
- network infrastructure, (bridges, routers, gateways, firewalls,)

- Internet and other external connections,
- media security,
- logical access control,
- identification and authentication,
- regular security compliance checking,
- accounting and security audit,
- information security incident management, and
- business continuity, including contingency planning/disaster recovery, strategy and plan(s).

Annex G Control monitoring and review

G1. General considerations

An organization should establish procedures for control monitoring and review in order to achieve the following:

- to measure the effectiveness of controls to verify that security requirements have been met,
- to review the level of residual risk taking into account change to the organization and its environment.

Monitoring and review of the effectiveness of the information security programme, even though often neglected, is one of the most important aspects of information security. The implemented controls can only work effectively if they are selected and checked in real business life and operational context. It shall be assured that they are used correctly, and that any security incidents and changes are detected and dealt with. The prime intent of the follow-up activity is to ensure that security controls continue to function as implemented. Over time there is a tendency for the performance of any service or mechanism to deteriorate. Follow-up is intended to detect this deterioration and initiate corrective action. This is the only way to maintain the security levels necessary to protect ICT systems. The procedures described in this annex form the basis of an effective check phase activity of information security management systems

G.2 Maintenance of controls

The majority of controls will require maintenance and administrative support to ensure their correct and appropriate functioning during their life. These activities (maintenance and administration) should be planned and performed on a regular scheduled basis. In this manner their overhead can be minimized, and the value of the controls preserved.

To detect malfunctions, periodic inspection is necessary. A control never checked is of little value as there is no way of knowing what reliance can be placed on it.

Maintenance activities include:

- checking of log files,
- modifying parameters to reflect changes and additions,
- re-initiation of seed values or counters,
- reviewing access controls,
- reviewing the adequacy of monitoring tools, and
- updating with new versions.

and other activities.

The cost of maintenance and administration should always be factored in when assessing and selecting between different controls. This is because maintenance and administrative costs can differ widely between one control and the next. Hence, this can often become a significant determinant in the selection of controls. Generally speaking, it is desirable to minimize the ongoing maintenance and administrative costs wherever possible as they represent recurring costs rather than one time costs.

G.3 Security Compliance Checking and Approval

Once the risk treatment plan which includes risk reduction option is completed and signed-off by the responsible managers, controls are implemented, security compliance checked, and tested. A security compliance check review should be conducted to ascertain that the security controls have been implemented correctly, that they are being used effectively and tested properly. Security testing can be conducted as part of this review. Testing is an important technique to ensure that the implementation has been carried out and completed correctly. Security testing should be guided by a security test plan that describes the testing approach, schedule and environment. Penetration testing can be used if justified by the risks assessed. Detailed security testing procedures should be written, a standard test report used, and the testing should be repeatable. The objective is to perform implementation and testing in a manner that ensures that the requirements from the information security plan are met and the risk is reduced as specified. Security compliance testing should be regularly conducted throughout the life cycle of the system.

Security compliance checking is the review and analysis of the implemented controls. It is used to check whether information and ICT systems or services conform to the security requirements documented in the information security policy, ICT system security policy and ICT system security plan. Security compliance checking should encompass compliance with applicable legislative and regulatory requirements.

Information security compliance checks may be used to check the conformance of:

- new information and ICT systems, processes and services both before and after implementation,
- existing information and ICT systems, processes or services after elapsed periods of time have occurred (e.g. annually), and
- existing information and ICT systems, processes and services when changes to the information security policy or ICT system security policy have been made, to see which adjustments are necessary to maintain the required security level.

Information security compliance checks may be conducted using external or internal personnel and are essentially based on the use of checklists relating to the information security policy and ICT system security policy.

The controls protecting the information processes and ICT systems may be checked by:

- conducting periodic checks, and tests,
- monitoring operational performance against actual incidents occurring, and
- conducting spot checks to check the status of security levels and objectives in particular areas of sensitivity or concern.

To assist the conduct of any information security compliance check, valuable information about the activities on an ICT system can be obtained from

- the use of software packages used to record events, and
- the use of audit trails to trace the entire history of events.

Information security compliance checking, for approval and regular checks thereafter, should be based on the agreed control lists from the last risk assessment results, on the information security policy and ICT system security policy, as well as security operating procedures which management has approved, including for incident reporting. The objectives are to ascertain whether controls are implemented, implemented correctly, used correctly, and where relevant, tested.

It helps to have a comprehensive checklist and agreed report formats - these are not to be underestimated. These checklists should cover general identification information, e.g. configuration detail, security responsibilities, policy documents, surrounding locale. Physical security should address external aspects, like

outside buildings, including accessibility through manhole covers, and internal aspects, like soundness of construction, locks, fire detection and prevention (including alarm aspects), similarly for water/liquid detection, failure of power, etc.

There are many things to detect, such as:

- areas open to physical penetration or circumvented controls; for example, wedges under doors which should operate under a keypad and card system, and

- incorrect mechanisms, or incorrect installation of mechanisms, e.g. lack or poor distribution or wrong type of detection facilities. Are smoke/heat detectors plentiful enough for an area, and at the correct height? Is there adequate response to alarms? Are alarms properly linked to a control point? Are there any new sources of danger - someone suddenly using a room to store flammables? Are there adequate power back-up and failure procedures? Are the correct types of cable used and not located near sharp tray edges?

To detect security gaps for other aspects of security, the following questions might be helpful.

- For *personnel security*, watch for the procedures for employment. Are references actually taken? Are employment gaps checked? Are personnel really aware and knowledgeable of security? Is there dependence on one person for a key function?

- For *administrative security*, how are documents really disposed of? Is the documentation in general use actually up-to-date? Are the risk assessment, status check and incident reporting activities actually used as they should? Is the business continuity plan coverage correct, and is it current?

- For *hardware/software security*, is there redundancy at the required level? How good are user ID/password selection and procedures? Does the audit trail cover error logging and traceability issues to the right granularity and selection? Does an evaluated product meet the agreed requirement?

- For *communications security*, is the required redundancy there? If there is a dial-up facility, is the requisite equipment and software in place and used properly? If encryption and/or message authentication is required, how effective is the key management system and related operation?

It is important that compliance is maintained with all required controls, and relevant laws, regulations and policies, since any control, regulation or policy can only be effective as long as users comply, and information systems conform, with them. Some sample controls in this area are listed below.

- Compliance with information security policy and controls

- Regular checks should be conducted to ensure that all controls that should be in place, as listed in the corporate information security policy and the relevant ICT system security policy, and other relevant documents, e.g. security operating procedures documents and disaster recovery plans, are implemented correctly, used correctly and effectively (including by end users), and tested, if necessary.

- Compliance with legal and regulatory requirements

- The compliance checks mentioned above should encompass legal and regulatory requirements related to the country or countries in which the organization and its information and ICT systems are located. This may include legislation on data protection and privacy, software copying, records management, and/or cryptography.

.

G.4 Change management

Change management is the process used to help identify whether different security controls are required when changes to information, assets, processes or systems occur. Information processes and systems and the environment in which they operate are constantly changing. These changes are a result of a wide variety

of factors, including the availability of new ICT features and services, or the discovery of new threats and vulnerabilities.

When a change to an information process or system occurs or is planned, it is important to determine what, if any, impact the change will have on the security of the organization. If an ICT system has a configuration control board or other organizational structure to manage technical system changes, the information security officer should be assigned to the board and be given the responsibility to make decisions about whether the change will affect security, and if so how. In some cases, there may be reasons for making changes that will reduce security. In these situations, the decrease in security should be assessed and a management decision made which is based on all relevant factors. In other words, changes to a system should adequately address security concerns. For major changes that involve the purchase of new hardware, software or services, an assessment will be required to determine the new security requirements. On the other hand, many changes made to systems are minor in nature and do not require the extensive analysis that is needed for major changes. For both types of changes, a risk assessment that considers the benefits and costs should be made. For minor changes, this can be performed informally at meetings, but the results and the management decisions should be monitored.

ICT configuration management or control is the process of maintaining system configuration and can be done formally, through an approved configuration management plan, or informally. The primary security goal of configuration management is to ensure system integrity. This includes maintaining up-to-date system configuration documentation, and managing approved changes to the system in such a manner that such changes do not reduce the effectiveness of controls and the overall security of the organization.

Configuration management is not intended to prevent changes to information systems because of security concerns. A related goal of configuration management is to ensure that changes to the system are reflected in other documents, such as disaster recovery and business continuity plans. Security documentation should be considered part of the configuration management plan and process.

G.5 Control monitoring

The effectiveness of security controls should be reviewed and verified periodically, by monitoring and compliance checking to ensure that the controls are functioning and being used in the manner expected. Many controls produce an output that should be checked for security significant events, e.g., logs, alarm reports. General system audit functions can provide useful information from a security perspective and can be used in this regard. Automated review and analysis of system logs is an effective tool for helping to ensure the intended performance. Additionally, these tools can be used to detect events, and their use may have a deterrent effect. Regular review should be scheduled and should be conducted by an independent party. The independent party need not necessarily be from outside the organization, but should not be under the supervision or control of those responsible for the implementation or daily management of the security programme. Monitoring is an ongoing activity which checks whether the system, its users, and the environment maintain the level of security as prescribed in the information security policy and plan.

Most ICT systems produce output in the form of logs of the occurrence of events. These logs should be centralized, saved, and analysed using various techniques, including statistical, expert system, manual, or scenario analysis, to permit the early detection of trend changes, and the detection of incidents occurring repeatedly. The responsibilities for the analysis of those logs should be allocated.

In distributed environments, logs may only record information related to a single environment. To truly understand the nature of a complex event, it is necessary to bring together the information from different logs, and fuse them into a single event record. These fused event records should then be subjected to analysis. Event record fusion is a complex task and its most important aspect is the identification of parameter(s) that permit the different log records to be combined with confidence.

The procedure for monitoring security controls needs to be described and documented. The approach and frequency of security log reviews should be stated. The use of statistical analysis methods and tools should be described. Guidance should be given for how to adjust audit thresholds based on various operational conditions.

Additionally, control monitoring uses the incident handling process as an important tool. Incident handling provides the organization with actual statistics and examples of risks which have occurred. Such incidents may indicate deficiencies in the risk assessment process and if the assessed risks are in line with the actual consequences.

Bibliography

[1] ISO/IEC ISO/IEC Guide 73: 2002, Risk management – Vocabulary – Guidelines for use in standards

[2] ISO/IEC TR 13569: 2005 Financial services - Information security guidelines

[3] ISO/IEC TR 15446 Guide for the production of Protection Profiles and Security Targets

[4] ETSI Baseline Security Standard - Features and Mechanisms [reference]

[5] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology

[6] NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook