ISO/IEC JTC1/SC27 N3759

ISO/IEC JTC1/SC27/WG1 N13759

REPLACE: N3551

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE: Text for 2nd Working Draft

TITLE: Text for ISO/IEC 2nd WD 13335-2 - Information technology - Security techniques – Management of information and communications technology security (MICTS) – Part 2: Techniques for information and communications technology security risk management

SOURCE: Project Editors (Elzbieta Andrukiewicz, Alice Sturgeon)

DATE: 2003-11-30

PROJECT: 1.27.39.02 (13335-2)

STATUS: In accordance with resolution 3 (reference document SC27 N3794rev1) of the 27th SC 27/WG 1 meeting in Paris, France, 2003-10-20/24, this document is circulated for **STUDY AND COMMENT**.

The SC27 National Bodies and Liaison Organizations are requested to submit their contributions on this document directly to the SC27 Secretariat by **2004-03-30**.

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

ACTION: **COM**

DUE DATE: **2004-03-30**

DISTRIBUTION: P- and L-Members
W. Fumy, SC 27 Chairman
M. De Soete, T. Humphreys, M. Ohlin, WG-Conveners

MEDIUM: Livelink-server

NO. OF PAGES: 156

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

Editors' Notes

1. At the editing meeting in Paris, it was agreed that, because of the insufficient time to review all comments, and because the major issue was restructuring, that NBs would review their comments on the 1st WD 13335-2 (as contained in 27 N3483) and on the revision of TR 13335-4 (ref. 27 N3694), to determine whether their comments were still applicable and valid and, if so, to resubmit their comments in response to 27 N3759 (Text for 2nd WD 13335-2).
2. Note that this Disposition of Comments contains the editing group's disposition of the comments on 27 N3635; the NB comments are found in 27 N3693.
3. This 2nd WD proposes the restructuring agreed at the October editing meeting. Most of the technical comments submitted in 27 N3668 have not been addressed; however, the editors were able to consider most of the editorial comments. No integration of merged text has been done in this 2nd WD. For readers' understanding of the restructuring, the merged parts are identified with a notation of square brackets [ ] that indicate the original location of the various pieces of text.
4. Note that all references need to be updated, and this will be done once the restructuring is agreed. Table and Figure numbering also needs updating, again, once the tables and figures to be included have been agreed.

Table of Contents

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 3.

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 this ISO/IEC WD 13335-2 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 13335 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC IS 13335 consists of the following parts, under the general title *Information technology – Management of information and communications technology security*:

- *Part 1: Concepts and models for information and communications technology security management,*
- *Part 2: Techniques for information and communications technology security risk management.*

ISO/IEC 13335 Part 1 supersedes ISO/IEC TR 13335 Part 1 and Part 2. ISO/IEC 13335 Part 2 supersedes ISO/IEC TR 13335 Part 3 and Part 4.

ISO/IEC TR 13335-5 consists of one part: *Guidelines for the management of information technology security*: *Part 5: Management guidance on network security.*

Introduction

ISO/IEC 13335-2, Information technology – Security techniques –Management of information and communications technology (ICT) security – Part 2: Techniques for information and communications technology security risk management, is the second in a series that deals with the management aspects of planning, implementation and operations, including maintenance, of ICT security.

Part 2 describes and recommends techniques for ICT security risk management. These techniques can be used to assess security requirements and risks, and help to establish and maintain the appropriate security safeguards, i.e. the correct ICT security level. The results achieved in this way may need to be enhanced by additional safeguards dictated by the actual organization business objectives, strategies, policies, environment and applicable laws and regulations. This part of ISO/IEC 13335 is relevant to everybody within an organization, and, where appropriate, those outside of the organization, who are responsible for the management and/or the implementation of ICT security.

ISO/IEC 13335 is organized into parts.

Part 1 (ISO/IEC 13335 Management of information and communications technology security – Part 1: Concepts and models for ICT security management) provides an overview of the fundamental concepts and models used to describe the management of ICT security.

Part 2 (ISO/IEC 13335-2 Management of information and communications technology security - Part 2: Techniques for ICT security risk management, to be published) describes security risk management techniques appropriate for use by those involved with management activities.

As noted in the Foreword, ISO/IEC 13335 Part 1 supersedes ISO/IEC TR 13335 Part 1 and Part 2. ISO/IEC 13335 Part 2 supersedes ISO/IEC TR 13335 Part 3 and Part 4.

Note that Part 5 is a Technical Report. Part 5 (ISO/IEC TR 13335-5: 2002 Guidelines for the management of IT security – Part 5: Management guidance on network security) provides guidance with respect to networks and communications to those responsible for the management of IT security. This guidance supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements. It also contains a brief introduction to the possible safeguard areas.

Information technology –Management of information and communications technology security –

Part 2:
Techniques for information and communications technology security risk management

1 Scope

Part 2 of ISO/IEC 13335 provides techniques information and communications technology (ICT) security risk management. The techniques are based on the general concepts, models, and management and planning guidelines laid out in Part 1 of this International Standard. These guidelines are designed to assist the implementation of ICT security. Familiarity with the concepts and models, and the material concerning the management and planning of ICT security in Part 1, is important for a complete understanding of Part 2.

2 Normative References

The normative references identified in Clause 2 of Part 1 of this International Standard apply equally to this part.

3 Definitions

The definitions given in Clause 3 of Part 1 of this International Standard apply equally to this part.

4 Risk management framework

4.1 Overview of the ICT security management process

[formerly Clause 6; Figure 1 deleted]
The process of the managing ICT security is based on the principles set out in ISO/IEC 13335 Part 1, Clause x. The process can be applied to the whole organization as well as to selected parts of it. ICT security management consists of all the activities to achieve and maintain appropriate levels of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability. A systematic approach based on risk management is necessary for the identification of requirements for ICT security within an organization. This also is true for the implementation of ICT security, and its ongoing administration.

The management of ICT security includes: analyzing the requirements for security, establishing a

plan for satisfying these requirements, documenting and implementing this plan, and maintaining and administering the implemented security. This process starts with establishing the organization's ICT security objectives and strategy, and developing a corporate ICT security policy.

The ICT security management process can be structured by/within the risk management paradigm. An important part of the ICT security management process is the assessment of risks, and how risks can attain an acceptable level. It is necessary to take into account the business objectives, as well as organizational and environmental aspects, and applicable laws and regulations, and each ICT system's specific needs and risks.

After assessing the security requirements of the ICT systems and services, it is advisable to select a corporate risk assessment strategy. The recommended option (the "combined approach") involves conducting a high-level risk assessment for all ICT systems to identify those systems at high risk. These systems are then examined through detailed risk assessment, while a baseline approach is applied for the remaining systems. For the high risk systems, the detailed consideration of assets, threats and vulnerabilities will lead to a detailed risk assessment which facilitates the selection of effective safeguards commensurate with the assessed risks. By using this option, the risk management process can be focused on where the significant risks or greatest needs are, and the overall programme can be made more cost and time effective.

Following the risk assessment, appropriate safeguards are identified for each ICT system to reduce the risks to an acceptable level. These safeguards are implemented as outlined in the ICT security plan. The implementation should be supported by an awareness and training programme, which is essential to maximize and maintain the effectiveness of the safeguards. The awareness and training programme should be based on the ICT security policy, guidelines and procedures.

Furthermore, the management of ICT security includes the ongoing task of dealing with various follow up activities, which can lead to changes to earlier results and decisions. Follow-up activities include: maintenance, security compliance checking, change management, monitoring, and information security incident management.

4.2 Risk management process

[formerly 7.1 Corporate risk management strategy] Any 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.

Risk management is an on-going activity. For new systems and systems at the planning stage, it should be part of the design and development process. For existing systems, risk management should be introduced at any appropriate point. When significant changes to systems are planned, risk management should be part of this planning process. It should take into account all systems within the organization and not be applied to one system in isolation.

The main elements of the risk management process are shown in Figure 1. Each of the boxes in the Figure is briefly described below. Note that this graphic representation is intended as illustrative of one methodology. There are a number of risk management methodologies; some of these varied approaches are detailed further in this International Standard. Implementing this methodology may involve combining some of the steps that are shown as separate boxes. The activity of identifying risks is considered an integral part of the risk assessment process, although it may occur as a separate step.

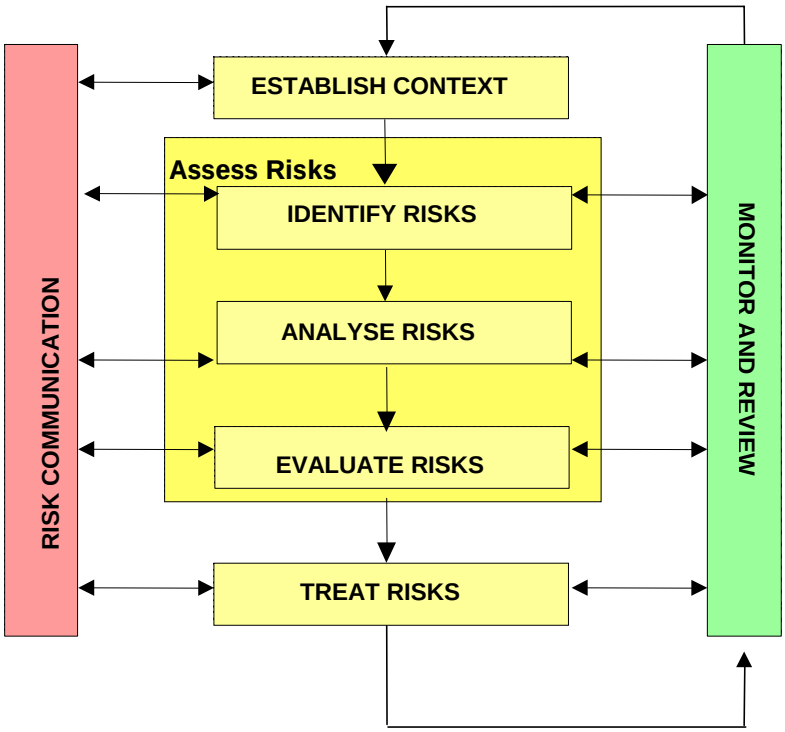

Figure 1 – Risk Management Process Overview

4.2.1 Establish the context

7.2.1 + 8.1 Establish the context.

(old 8.2) Risk evaluation criteria

Establish the strategic, organizational and risk management context in which the rest of the process will take place. Criteria against which risk will be evaluated should be established and the structure of the risk assessment defined.

[8.1]

The risk management process occurs within the framework of an organizational and risk management context. This process needs to be established to define the basic parameters within which risks must be managed and to provide guidance for decisions within more detailed risk management studies. This sets the scope for the rest of the risk management process. It must be remembered that few risks remain static. On-going monitoring and review is necessary to ensure

that the context, identified risks, risk assessment, risk evaluation and risk treatment remains appropriate to the circumstances.

A careful definition of boundaries 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 for the considered information asset:

- ICT assets (e.g. hardware, software, information);
- people (e.g. staff, subcontractors, other external personnel);
- environment (e.g. buildings, facilities), or geographical location; and
- activities (operations).

The strategic context concerns the environment in which the organization operates. The organization should seek to determine the crucial elements that might support or impair its ability to manage the information security risks it faces.

The organizational context concerns the organization and its capabilities, as well as its goals and objectives and the strategies that are in place to achieve them. The context will have an impact on the ICT security policy for ICT systems, on the risk assessment approaches chosen, and on the selection of, and implementation priorities for, safeguards.

The risk management context concerns the goals, objectives, strategies, scope and parameters of the activity, or part of the organization, to which the risk management process is being applied, should be established. The process should be undertaken with full consideration of the need to balance costs of safeguards and risk reduction benefits. The resources required and the records to be kept should also be specified.

Finally, the context establishment phase involves separating the activity of project into a set of elements. Those elements provide a logical framework for identification and analysis that helps ensure significant risks are not overlooked. The structure chosen depends on the nature of the risks and the scope of the project or activity. For example, the structure could be based on different types of assets.

4.2.2 Identify risks

[7.2.2]
Identify what, why and how problems and concerns can arise as the basis for further analysis. Identifying risks involves identifying threats, vulnerabilities, probability and impact.

[8.3.1]
This step is to identify the information security risks to be managed and the most appropriate approach to their treatment. In some cases, risks will be similar to those in other systems or organizations and can be treated using a baseline approach. 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.

Risk identification involves establishing what can happen, and how and why it can happen. Approaches used to identify risks include checklists, judgements based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis and systems engineering techniques.

4.2.3 Analyze risks

[7.2.3]
Determine the existing safeguards and analyze risks in terms of impact and probability in the context of these safeguards. The analysis should consider the range of potential impacts and how likely these impacts are to occur. Impact and probability may be combined to produce a risk estimation.

In the context of ICT security, risk assessment for ICT systems involves the analysis of asset values, threats and vulnerabilities. Impact is assessed in terms of harm that would be caused by a breach of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability. The result of a risk assessment is a statement of the likely risks to assets.

Risk assessment is part of risk management and can be accomplished without an unnecessary investment in time and resources by conducting an initial brief assessment on all systems. This will determine which systems can be adequately protected by a code of practice or baseline controls, and those systems that will benefit from a detailed risk assessment.

[8.3.2]
The objectives of analysis are to separate the minor acceptable risks from the major risks, and to provide data to assist in the evaluation and treatment of risks. Risk analysis involves consideration of the sources of risk, determination of the consequences of realizing these risks and the likelihood that those consequences may occur. Factors that affect the consequences and likelihood may also be identified. Risk is analyzed by combining estimates of consequences and likelihood in the context of existing safeguards.

The risk assessment phase can be made very brief if previous work has established a baseline (or code of practice) for the treatment specific types of risk. Baseline safeguards can be used to treat common risks. Where large or unusual risks are identified, it is necessary to complete risk assessment and evaluation to determine appropriate treatment options.

A preliminary analysis can be carried out so that similar or low-impact risks are excluded from detailed study. Excluded risks should, where possible, be listed to demonstrate the completeness of the risk assessment.

4.2.4 Evaluate risks

[7.2.4]
Compare estimated levels of risk against pre-established criteria. This enables risks to be ranked so as to identify management priorities. Risks assessed as low may be considered as acceptable, and treatment of these low risks may not be required.

[8.3.3]
Risk evaluation involves comparing the level of risk found during the analysis process with previously established risk criteria. Risk analysis and the criteria against which risks are compared in risk evaluation should be considered on the same basis. Thus, qualitative evaluation involves comparison of a qualitative level of risk against qualitative criteria, and quantitative evaluation involves comparison of numerical level of risk against criteria that may be expressed as a specific number, such as frequency, duration of outage, or monetary value.

The result of a risk evaluation is a priority list of risks for further action. Decisions should take into account the wider context of the risk and include consideration of the tolerability of the risks borne by parties other than the organization that benefits from it. If the resulting risk falls into the low or acceptable risk categories they may be accepted with minimal further treatment. Low and accepted risks should be monitored and periodically reviewed to ensure they remain acceptable. 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.

4.2.4.1 Risk evaluation criteria

[8.2]
The context includes the risk evaluation criteria to be used. Decisions concerning risk acceptability and risk treatment may be based on the operational, technical, financial, legal, social, humanitarian or other criteria. These often depend on an organization's internal policy, goals, objectives and the interests of stakeholders. Criteria for evaluation of information security risks are typically (but not limited to) financial consequences associated with:

- customer perceptions and regulatory impacts of breaches of privacy;
- operational and business impacts of unavailability;
- business impacts of loss of confidentiality;
- operational and business impacts of loss of integrity.

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

4.2.5 Treat risks

[7.2.5]
Develop and implement a specific management plan that includes consideration of risk

estimation criteria. Options include risk avoidance, risk reduction risk transference. Any remaining risk may be considered residual risk, and accepted. Low priority risks should be monitored. The selected options for risk treatment should be reviewed periodically.

[8.3.4]
Risk treatment involves identifying the range of options for treating risk, assessing those options, preparing risk treatment plans and implementing them.

4.2.5.1 Identification and assessment of risk treatment options

Options, which are not necessarily mutually exclusive or appropriate in all circumstances, include the following:

- risk avoidance;
- reduction of likelihood;
- reduction of consequences;
- risk transference; and
- risk retention.

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. A number of options may 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 commensurate 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 impacts of risks should be made as low as reasonably practicable, irrespective of any absolute criteria.

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. 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 program.

Where the cumulative costs of implementing all risk treatments exceeds the available budget, the 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 must 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 must be made to secure additional finances.

Risk treatment options should consider how risk is perceived by affected parties and the most appropriate ways to communicate to those parties.

4.2.5.2 Risk Treatment Plans

Plans should document how safeguards should be implemented. The treatment plan should identify responsibilities, schedules, the expected outcome of treatments, budgeting performance measures, and the review process to be set in place. The plan should also include a mechanism for assessing the implementation of the options against performance criteria, individual responsibilities and other objectives, and to monitor critical implementation milestones.

Ideally, responsibility for treatment of risks should be borne by those best able to control the risk. Responsibilities should be agreed between the parties at the earliest possible time. The successful implementation of the risk treatment plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. If after treatment there is a residual risk, a decision should be taken as to whether to retain this risk or repeat the risk treatment process.

4.2.6 Residual Risk

After the implementation of the selected safeguards, there will always be a residual risk. This is because no system can ever be made absolutely secure, and because certain assets may have been left unprotected intentionally (e.g., because of assumed low risk or the high costs of the recommended safeguard relative to the estimated value of the asset to be protected).

The first step of the risk acceptance process is to review the safeguards selected and to identify and assess all residual risks. The next step is to classify the residual risks into those considered "acceptable" and those that are "unacceptable" for the organization.

It is obvious that unacceptable risks cannot be tolerated, thus additional safeguards limiting the impact or consequences of those risks should be considered. In each of these cases, a business decision must be made. Either the risk is to be judged "acceptable", or the expense of additional safeguards must be approved which reduce the risk to an acceptable level.

[8.3.4.3]
There will always be residual risks associated with a risk treatment plan. This is because an organization's information systems can never be made absolutely secure. It may also be that certain assets may have been left unprotected intentionally (e.g., because of assumed low risk or the high costs of safeguard(s)). Risk acceptance involves a review of the safeguards selected in order to identify and assess all residual risks. This involves a judgement of how much the safeguards selected reduce the risks, for example, by reducing the threats and/or vulnerabilities. These residual risks are categorized according to those that are considered 'acceptable' and those that are considered 'unacceptable' to the organization. It is generally good practice that unacceptable risks should not be tolerated, thus additional safeguards reducing those risks should be considered. For each of these unacceptable risks, a business decision must be made. Either the risk is finally accepted, or the expense of additional safeguards must be approved to reduce the risk to an acceptable level.

[9.6]
After choosing the safeguards and identifying the reduction of risks these safeguards will achieve, there will always be residual risks - no system can be made absolutely secure. These residual risks should be categorized as 'acceptable' or 'unacceptable' for the organization. This categorization can be accomplished by reviewing the potential adverse business impacts associated with those risks. Obviously, the unacceptable risks cannot be tolerated without further considerations. 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 safeguards are selected to reduce the unacceptable risks.

4.2.7 Risk communication

[7.2.6]
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.

[8.3.6]
Risk communication is an important consideration at each step of the risk management process. It is important to 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. Communication and consultation involve a two-way dialogue between stakeholders with efforts focused on consultation rather than a one-way flow of information from the decision-maker to other stakeholders.

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 judgements 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.

4.2.8 Risk monitoring and review

[7.2.7]
The use of safeguards should be monitored to ensure they function appropriately, that changes in the environment have not rendered them ineffective and that accountability is enforced.

[8.3.5]
Ongoing review is essential to ensure that the management plan remains relevant. Factors that may affect the likelihood and consequences of an outcome may change, as may the factors that affect the suitability or cost of the various treatment options. It is therefore necessary to regularly repeat the risk management cycle. Review is an integral part of the risk management treatment plan. Results of monitoring and review activities should be fed back into the risk management system.

4.3 Risk management recommendations

The risk assessment approach should provide a number of recommendations to reduce the security risks to an acceptable level. In producing these recommendations for approval, the following should be considered:

- Detailed risk assessment (criteria for determining acceptable levels)
    - establishment of a review boundary
    - identification of assets
    - valuation of assets and establishment of dependencies between assets
    - threat assessment
    - vulnerability assessment
    - identification of existing/planned safeguards
    - assessment of risks
- Risk acceptance
- Selection of safeguards (which reduce risks to an acceptable level)
    - identification of safeguards
    - cost / benefit assessment of safeguards
    - relationship to risk acceptance
    - ICT Security architecture
    - identification review of constraints

- ICT system security policy
- ICT security plan

4.4 Risk management paradigm in ICT security management processes

Risk management approaches should be applied in all ICT Security management processes as described in Clauses 4 and 5. Relationships between ICT security management processes and relevant risk management activities are shown in the following table.

Sec mgmt process	Part 1 Reference	Part 2 Reference	Risk activities related to sec mgmt processes	Part 2 Reference (Risk activities)
Planning				
Corporate ICT sec policy development			Establish context Risk identification	
ICT security organizational planning			Establish context	
Risk assessment			Risk assessment (detailed)	
ICT system security policy development			Risk assessment Risk treatment	
Development of ICT security plan			Risk treatment	
Implementation				
Implementing safeguards			Risk treatment	
Security awareness and training			Risk treatment Risk communication	
Approval of ICT systems			Risk treatment	
Follow- up				
Maintenance			Monitor and review	
Security compliance checking			Risk treatment Monitor and review	
Configuration control and change management			Monitor and review	
Business continuity planning			Risk treatment	
Incident management			Risk treatment Risk communications	
Monitoring and review			Monitor and review	

[Editors' Note: The table above has been added pursuant to Polish comment # 5 in N3668. References need to be added, as the references originally supplied by the Polish NB are no longer valid following reorganization of both Parts 1 and 2.]

5 Risk Management Approaches

5.1 High-level risk assessment

[Belgian Appendix 3, with modification (remove baseline approach)]
[Move text from Annex G, Clause 6]

The high-level risk assessment approach is a high level study allowing to define large domains requesting distinct approaches, e.g. baseline for development environment and detailed risk management for production environment, and a group of systems to specifically protect to comply with external standards.

The high-level approach also allows definition of the priorities and chronology in the actions. For budgetary reasons, it may not be possible to implement all safeguards simultaneously. Besides, it is premature to begin detailed risk management if implementation is only envisaged within one or two years. To reach this objective, a high-level approach frequently begins with a high-level impact assessment instead of starting with a systematic analysis of threats, vulnerabilities, assets and impacts.

Another reason to start with the high-level approach is to synchronise 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 three months later.

The high-level risk management approach derives from the detailed risk management approach in several ways:

- It addresses more the global/generic view of the ICT system, considering the 'technology' aspects as dependent from the business issues. By doing this the context analysed concentrates more on the business and operational environment than the boundaries and ICT components.
- It addresses a limited and generic list of threats and vulnerabilities grouped in defined domains or, to fasten the process, sometimes analyses risk or attack scenarios instead of their elements.
- It realises an evaluation of the analysed risks to decide on the acceptance or treatment of the risks.
- Risks presented in a high-level risk management approach 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 safeguards in this domain. The risk treatment activities tries then first to propose and select common safeguards that are valid across the whole system.
- However, the high-level risk assessment approach, because it seldom addresses technology details, is more appropriate to provide organisational and non-technical safeguards, besides generic management aspects of the technical safeguards.
- For these reasons, the high-level risk assessment approach is to be positioned between the detailed and the baseline approaches and can pick-up here and there steps and ideas from both. As a consequence it can easily be mistaken as a baseline or a combined approach.

Examples: Most of the risk management methods designed to implement the high-level approach are manual. Simple methods (or self-assessment methods) proposed by governmental agencies are of this type.

[9.1]
First it is necessary to conduct an initial high-level risk assessment to identify which approach (baseline or detailed risk assessment) is appropriate for each ICT system. This high-level risk

assessment considers the business values of the ICT systems and the information handled, and the risks from the organization's business point of view. Input for the decision as to which approach is suitable for which ICT system can be obtained from consideration of the following:

- the business objectives to be achieved by using the ICT system,
- the degree to which the organization's business depends on the ICT system, i.e. whether functions that the organization considers critical to its survival or the effective conduct of business are dependent on this 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 this ICT system, in terms of developing, maintaining, or replacing the system, and
- the assets of the ICT system, for which the organization directly assigns value.

The criteria established should also be considered when deciding which approach to adopt for each ICT system. When these items are assessed, the decision is generally easy. 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 detailed risk analysis is necessary for the system or part thereof. Either these conditions may be enough to justify conducting a detailed risk assessment.

A general rule to apply is: if the lack of ICT system security can result in significant harm or damage to an organization, its business processes or its assets, then a detailed risk assessment is necessary to identify potential risks.

[Annex G]
TBD

5.2 Combined risk assessment

Some organizations consider the combined approach as the most complex one. It should not be the case as it is frequently a simplification of the detailed approach taking benefits from the advantages of the other approaches.

The combined approach is to conduct an initial high-level risk assessment for all ICT systems, in each case concentrating on the business values of the ICT system and the serious risks to which it is exposed. For the ICT systems identified as being important for the organization’s business and/or exposed to high risks, a detailed risk assessment should be conducted in a priority order. For all other ICT systems, a baseline approach should be chosen. This option provides a good balance between minimizing the time and effort spent in identifying safeguards, while still ensuring that the high-risk systems are appropriately protected.

It is generally articulated as follows:

- A high-level risk assessment approach is performed, on business processes, functions and activities;
- The Risk evaluation step is the key activity:
    - It decides which risk domains or processes or systems that support these processes will follow the baseline approach for the risk treatment steps;
    - It decides which domains, processes or systems will undergo a new detailed risk management process, possibly after a baseline is first step;
    - It decides which risks will benefit of a detailed and narrow risk treatment;
    - It decides on risks that will be accepted and the way that these will be monitored to allow to later on decide which of the baseline or detailed approach will be adopted.

No published methodologies are available that implement this approach. However this approach is really performed in large or medium organizations and combines methodologies and tools from all three approaches depending on predetermined criteria. These organizations had first to prepare a coherent risk management strategy and policy.

5.3 Detailed risk assessment

[Editors' recommendation: High-level introductory paragraph, leading into Clause 6 – TBD]

6 Detailed risk assessment

6.1 General

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

The risk assessment is done by an identification of potential business impacts of incidents and the probability of their occurrence. Incidents can impact the business, people or any asset of the organization. The impact of an incident is a composite of possible damages related to the value of the assets at risk. The probability 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 and selection of safeguards that can be used to reduce the identified risks to an acceptable level.

Detailed risk assessment involves in-depth reviews at each of the steps shown in the following figure. It leads to the selection of justified safeguards as part of the risk

management process. The requirements for these safeguards are documented in the ICT system security policy and the related ICT security plan. 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 incidents that need to be dealt with.

A variety of methods exist for the performance of a risk assessment ranging from checklist-based approaches to structured analysis based techniques. Automated (computer assisted) or manual based products can be used. Whatever method or product is used by the organization, it should at least address the topics identified in the following clauses. It is also important that the methods used fit with the organization's culture.

Once a detailed risk assessment review for a system has been completed for the first time, the results of the review - assets and their values, threat, vulnerability, probability and impact, risk levels, and safeguards identified - should be saved, for example, in a database. Methods with software support tools make this activity much easier. This representation can be utilized to significant effect as changes occur over time, such as configuration, information types stored and processed, threat scenarios, new vulnerabilities, etc. Only the changes are needed as input in order to ascertain the effect on the necessary safeguards. Further, such methods can be quickly used to examine different options, for example during the development of a new system, as well as being used for other systems that are similar in nature.

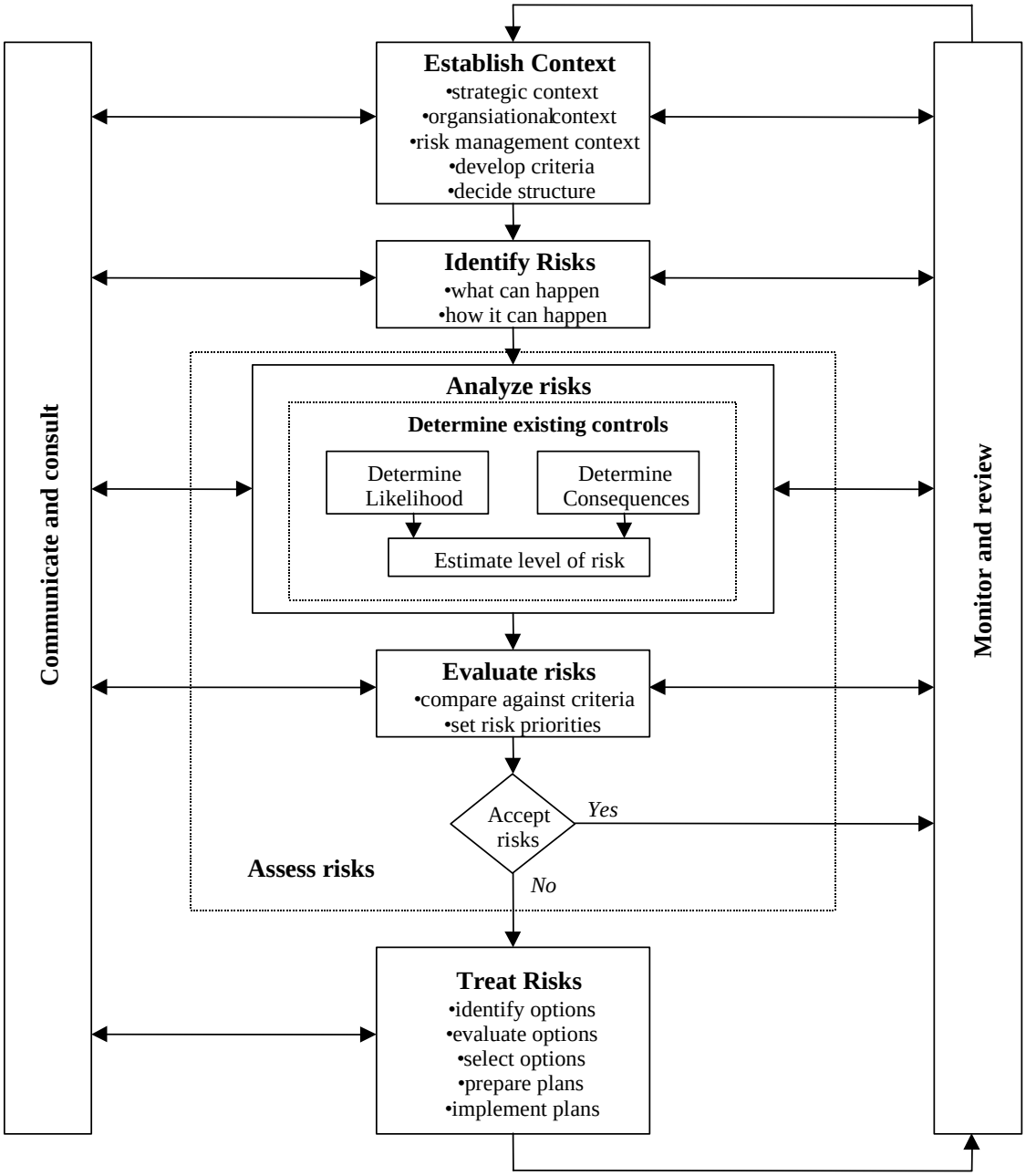

Figure x - Establishing risk management involving detailed risk assessment

6.2 Establishment of review boundary

As shown in Figure x, prior to gathering input for the asset identification and valuation, the boundaries of the review should be defined. A careful definition of boundaries 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 ICT system:

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

6.3 Identification of assets

An asset is a component or part of a total system to which an organization directly assigns value and hence for which the organization requires protection. For the identification of assets it should be borne in mind that an ICT system consists of more than hardware and software. For example, asset types 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 programs, programs developed for special purposes),
- communications equipment (e.g. telephones, copper cable, fibre),
- firmware (e.g. floppy discs, CD ROMs and other removable media),
- documents (e.g. contracts),
- funds (e.g. in Automatic Teller Machines),
- manufactured goods,
- services (e.g. information services, computing resources),
- confidence and trust in services (e.g. payment services),
- environmental equipment,
- personnel,
- image of the organization.

All assets within the review boundary established must be identified. 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.

6.4 Valuation of assets and establishment of dependencies between assets

After fulfilling the objective of asset identification by listing all assets of the ICT system under review, values should be assigned to these assets. These values represent the importance of the assets to the organization. This may be expressed in terms of security concerns such as the potential adverse business impacts from the disclosure, modification, non-availability and/or destruction of information, and other ICT system assets. Thus asset identification and valuation,

based on the business needs of an organization, are major factors in the determination of risks.

The input for the valuation of assets 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 impacts 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 also necessary to establish the value or extent of importance in non-financial, i.e. qualitative, terms to the organization. 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.

In Annex C, more detail is given of possible scales for use in assigning values to assets by considering possible damages. Regardless of which scale is used, issues to be considered in this valuation could be the possible damages resulting from:

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

An organization might need to think of other criteria important for its business, to be added to the criteria used in Annex B. Also, an organization has to define its own limits for damages like ‘low’ or ‘high’. For example, financial damage, which might be disastrous for a small company, might be low or even negligible for a very big company.

It should be emphasized at this stage that the method for assessment must allow not only quantitative valuation, but also qualitative valuation 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 other assets should also be identified, since this might influence the

values of the assets. For example, the confidentiality of data should be kept throughout its storage and processing, i.e. the security needs of data storage and processing programs 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 program, the input data of this program 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 the air conditioning. Thus information about dependencies will assist in the identification of threats and particularly vulnerabilities. It will also 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 programs or the same type of PC 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, so care must 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), non-availability and destruction (preservation of availability), and replacement cost.

6.5 Threat assessment

A threat has the potential to harm the ICT system and its assets under review. If a threat occurred, it could impinge on the ICT system in some way to cause incidents. 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 no threat be overlooked, since this could result in failure or weaknesses in the ICT system security.

Input to the threat assessment should be obtained from the asset owners or users, from personnel department staff, from facility planning 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. An example is given in Annex C. Nevertheless it might be worthwhile to consult other threat catalogues (maybe specific to your organization or business) since no list can be exhaustive. Some of the most common manifestations of threats are:

- errors and omissions,
- fraud and theft,
- employee sabotage,
- loss of physical and infrastructure support,
- malicious hacking, e.g. through masquerading,
- malicious code, and
- industrial espionage.

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. It is also interesting to note that the implementation of safeguards such as virus checking software always seem to lead to the development of new viruses which are resistant to current safeguards.

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, statistics, etc.), if statistics etc. can be applied,
- the motivation, the capabilities (perceived and necessary), resources available to possible attackers, and the perception of attractiveness and vulnerability of ICT system assets for the possible attacker, for deliberate threat sources, and
- geographical factors such as proximity to chemical or petroleum factories, 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 instance, a physical asset might initially be considered to be 'central data servers', but when it is identified that these servers are in different geographic locations, it would be split into 'central data server 1' and 'central data server 2' because some threats may be different, and others at different levels. Similarly, a software asset might first be regarded as 'application software' but later broken down into two or more instances of 'application software'. An example with regard to a data asset could be where it is first determined as 'criminal record' but later split into 'criminal record text' and 'criminal record image'.

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 on a scale

such as high, medium, or low.

6.6 Vulnerability assessment

This assessment includes identifying weaknesses in the physical environment, organization, procedures, personnel, management, administration, hardware, software or communications equipment, and full operational context, that may be exploited by a threat source to cause harm to the assets, and the business they support. The presence of a vulnerability does not cause harm in itself, as there must be a threat present to exploit it. A vulnerability that has no corresponding threat may not require the implementation of a safeguard, but should be recognized and monitored for changes. It should be noted that an incorrectly implemented or malfunctioning safeguard, or safeguard being used incorrectly, could in itself be a vulnerability.

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 also means that the unauthorized destruction of information stored on the EEPROM is possible. This can be a vulnerability.

This assessment identifies vulnerabilities that may be exploited by threats and assesses their likely level of weakness, i.e. ease of exploitation. For example, some assets are easily disposed of, concealed or transported - all of these properties can relate to vulnerabilities. Input for the vulnerability assessment should be obtained from the asset owners or users, facility specialists, and ICT systems experts on hardware and software. Examples of vulnerabilities are:

- unprotected connections (for example to the Internet),
- untrained users,
- incorrect selection and use of passwords,
- no proper access control (logical and/or physical),
- no back-up copies of information or software, and
- location in an area susceptible to flooding.

More examples of vulnerabilities can be found in Annex E.

Ii is important to assess how severe the vulnerabilities are, in other words how easily they may be exploited. A vulnerability should be assessed in relation to each threat that might exploit it in a particular situation. For instance, a 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.

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, e.g. on a scale of high, medium, or low.

6.7 Identification of existing/planned safeguards

The safeguards identified following a risk assessment review should be additional to any already existing and planned safeguards. It is important that such existing and planned safeguards are identified as part of this process to avoid unnecessary work or cost, e.g. in the duplication of safeguards. It might also be identified that an existing or planned safeguard is either not sufficient or not justified. In this case, it should be checked whether the safeguard should be removed, replaced by another, more suitable, safeguard, or whether it should stay in place (for example, for cost reasons).

In addition, a check needs to be made to determine whether the safeguards selected following the risk assessment review are compatible with existing and planned safeguards, i.e. that the safeguards being selected and existing safeguards should not hinder each other.

While identifying the existing safeguards, a check should be made to ensure that the safeguards are working correctly. The organization may rely upon the safeguard to work correctly, but, if it does not, then this will create vulnerabilities.

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

NEW CLAUSE 10 [now 7] Selection of Safeguards/ Risk Treatment

7 Risk treatment options - Selection of safeguards

Appropriate and justified safeguards should be identified and selected to reduce the assessed risks to an acceptable level. Existing and planned safeguards, the ICT security architecture, and constraints of various types have to be taken into account to allow a proper selection.

7.1 Identification of Safeguards

There are several types of safeguards: those that prevent, deter, detect, limit or correct incidents; those that enable recovery from incidents, and those that provide monitoring and awareness. Prevention can include the deterrence of actions and activities that enhance security awareness. Management responsibilities include assessing the costs of individual safeguards relative to the benefits they will provide, and relative to the level of residual risk deemed acceptable. Annex G provides additional guidance on selection of safeguards

The measures of risks determined in the previous step should be used as the basis for identifying all safeguards that are necessary for appropriate protection.

In order to select safeguards that effectively protect against the assessed risks, the results of the risk assessment should be considered. The vulnerabilities to associated threats indicate where additional protection may be needed, and what form it should take.

Areas where safeguards are applicable include:

- physical environment,
- personnel,
- administration,
- hardware/software, and
- communications.

The existing and planned safeguards 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 safeguard than to leave it in place, and maybe add another safeguard. It is possible as well that a safeguard may provide protection to assets outside of the current review boundary.

For the identification of safeguards it is useful to consider the vulnerabilities that are to be removed or reduced, and the associated threats that might exploit these vulnerabilities. In general, there are a number of possibilities to lessen the risks:

- avoid the risk,
- transfer the risk (e.g. insurance),
- reduce the threats,
- reduce the vulnerabilities,
- reduce the possible impacts, and
- detect incidents, react to, and recover from, them.

Which of these possibilities (or a combination of them) is most appropriate depends on the circumstances. Safeguard catalogues also might be helpful. However, in selecting safeguards from a catalogue it is also important to tailor them to the specific needs of an organization.

Another important aspect of safeguard selection is the cost factor. It would be inappropriate to recommend safeguards that are more expensive to implement and maintain than the value of the assets they are designed to protect. It may also be inappropriate to recommend safeguards that are more expensive than the budget that the organization has assigned for security. However, great care should be taken if the budget reduces the number or quality of safeguards to be implemented since this can lead to the implicit acceptance of greater risk than planned. The established budget for safeguards should only be used as a limiting factor with considerable care.

Where a baseline approach is selected to protect the ICT system, the selection of safeguards is relatively simple. Safeguard catalogues suggest a set of safeguards to protect the ICT system against the most common threats. These recommended safeguards are compared with the existing or planned safeguards, and the ones not already in place or planned form a list of safeguards to be implemented to obtain baseline protection.

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

Physical security safeguards 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 must include the steps required to safeguard 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 safeguards. These safeguards 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 safeguards, 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 also 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 safeguards 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 safeguards,
- capital, operating and maintenance costs of the safeguards,
- the help provided to the users to perform their function, and
- ease of use of the safeguard for the user.

Generally, a safeguard will fulfill more than one of these functions - the more it can fulfill the better. When examining the overall security, or set of safeguards 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).

7.2 Implementation of safeguards

For the implementation of safeguards, all the necessary steps described in the ICT security plan should be carried out. The person responsible for the plan (normally is the ICT system security officer) should ensure that the priorities and the schedule outlined in the ICT security plan are followed.

To ensure continuity and consistency, documentation of safeguards is an important part of the ICT security documentation. This process can be accomplished in a number of different ways. It should be part of a number of security documents, i.e. the security plan, business continuity plan, risk assessment documents, and security policies and procedures. It should be designed to fulfill the needs of managers, users, system administrators, maintenance personnel, and those involved in configuration and change management, monitoring, control and audit of systems, and security processes/activities. It needs to be current and in sufficient detail to help eliminate security lapses and oversights, as well as provide information which will ensure that security operations will be performed correctly and efficiently. Much of the documentation, particularly on threats, vulnerabilities and risks, can be very sensitive and must be protected against unauthorized disclosure. As a result, most organizations will need to handle this documentation very carefully and may want to use ‘trusted’ distribution procedures.

If such procedures are used, they should also be documented in a manner that describes how the sensitive parts of the safeguard information will be stored, accessed, and used. Moreover, the procedures should identify who is accountable for deciding how the safeguarded information will

be stored and who will be able to access and use it. In the design of the distribution procedures, safeguard information accessibility should take into account special factors such as the need to find and use a business continuity, including contingency planning/disaster recovery, strategy and plan(s), during a disaster or other unforeseen event where time is critical. Finally, strict configuration control of the safeguard documentation is also needed in order to ensure that no unauthorized changes are made which will diminish the effectiveness of the safeguards.

Once the ICT security plan is completed and signed-off by the responsible functions, safeguards must be implemented, security compliance checked, and tested. A security compliance check review should be conducted to ascertain that the security safeguards 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 and a standard test report used. The objective is to perform implementation and testing in a manner that ensures that the requirements from the ICT security plan are met and the risk is reduced as specified.

7.3 ICT security architecture

An ICT security architecture describes how the requirements for security are to be satisfied for an ICT system, as part of the overall system's architecture. Therefore, it is important to consider the ICT security architecture during the process of safeguard selection.

An ICT security architecture can be used in the development of new systems and when major changes are made to existing systems. Based on the results of the risk assessment or baseline approach, it takes the requirements for security and refines them into a set of technical security services for the system that will satisfy those requirements. In some cases, particularly when changes are being made to existing systems, some of the requirements may be in the form of specific safeguards that are to be used.

An ICT security architecture focuses on technical security services and how they will fulfill the security objectives. In doing this, related non-technical security safeguards are taken into account. Even though the architecture can be built from a number of different perspectives and approaches, one fundamental principle should be taken into account. A security problem in a unique security domain (an area of the same or similar security requirements and safeguards) must not be permitted to adversely impact the security of another unique security domain. An ICT security architecture will normally consist of one or more security domains. The security domains should follow the business domains that the organization is using and has established, as closely as practical. These business domains may follow particular business functional divisions such as payroll, manufacturing, or customer service, or they may follow business services divisions such as e-mail services or office services.

Security domains are differentiated by one or more of the following attributes:

- levels, categories or types of information accessible within the domain,
- operations applicable to the domain,
- communities of interest (COI) associated within the domain,
- relationships to other domains and environments, and
- types of functions or information access required by COI within the domain.

In constructing an ICT security architecture, the issues that should be addressed include:

- interrelationships and interdependencies between unique security domains,
- impacts or implications of interrelationships and interdependencies weakening security services, and
- extra services or precautions required to correct, control or counter any weakness.

An ICT security architecture does not stand alone; rather it relies on and interfaces with other documents. The most important of these is the system architecture and the other associated architectures such as hardware, communications and applications. An ICT security architecture will not contain a complete description of the system; it will address technical aspects and elements related to the security only. An ICT security architecture should aim to minimize any adverse impact on users and business operations, while ensuring that the environment has the optimum protection in place.

A number of other documents are related to the ICT security architecture or are dependent on it. These include the:

- ICT security design,
- ICT security operational concept,
- ICT security plan,
- ICT system security policy, and
- ICT system certification and accreditation documentation, if required.

7.4 Identification and review of constraints

There are many constraints which can affect the selection of safeguards. These constraints must 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, safeguards should be implemented within a time period acceptable for management. Another type of time constraint is whether a safeguard can be implemented within the lifetime of the system. A third type of time constraint

may be the period of time management decides is an acceptable period to leave the system exposed to a particular risk.

Financial constraints:
Safeguards should not be more expensive to implement or to maintain than the value of assets they are designed to protect. 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.

Technical constraints:
Technical problems, like the compatibility of programs or hardware, can easily be avoided if account is taken of them during the selection of safeguards. Also, the retrospective implementation of safeguards to an existing system is often hindered by technical constraints. These difficulties may move the balance of safeguards towards the procedural and physical aspects of security.

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

Environmental constraints:
Environmental factors may influence the selection of safeguards, 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 safeguards. Non-ICT specific laws and regulations such as labour relations and privacy legislation, fire department, health and safety, and economic sector regulations, etc. could also affect safeguard selection.

7.5 ICT system security policy

The ICT system security policy should contain details of safeguards required and describe why they are necessary. The ICT security plan for the system deals with how to implement them.

Many systems require their own security policies, which should be based on risk assessment reviews. This is normally the case with large and complex systems, or with systems that introduce unique and special considerations not found in other systems of the organization. The ICT system security policy should be compatible with the corporate ICT security policy, and any conflict should be avoided. It should address issues at a level lower than that of the corporate ICT security policy. The ICT system security policy is based on the results of a detailed risk

management process. These safeguards ensure that an adequate level of protection is achieved for the system.

The ICT system security policy should be based on the following information regardless of the corporate risk assessment strategy used, and should contain safeguards (including procedures) necessary to achieve the appropriate security level for the considered system. The ICT system security policy and all relevant supporting documents should deal with:

- a definition of the ICT system, a description of its components and boundaries (this description should encompass all the hardware, software, people, environment and activities which comprise the system),
- the definition of the business objectives of the ICT system,
- the identification of the security objectives for the system,
- the broad degree of dependence on the ICT system, in terms of how much the organization's business could be jeopardized by loss or compromise of the ICT system, the tasks this ICT system is meant to fulfill, and the information stored and processed,
- the level of investment in ICT, in terms of the cost of developing, maintaining and replacing the ICT system, together with the capital, running and replacement accommodation costs,
- the risk assessment approach selected for the ICT system,
- the assets of the ICT system the organization wants to protect,
- the valuation of these assets, in terms of what happens to the organization if these assets are compromised (the value of the information held should be described in terms of the potential adverse business impacts from disclosure, modification, non-availability and destruction of this information),
- the threats to the ICT system and the information handled, including the relationship between the assets and the threats, and the likelihood of those threats occurring,
- the vulnerabilities of the ICT system, including a description of the inherent weaknesses, which could be exploited by threats,
- the security risks for this ICT system as a result of:
    - the potential adverse impacts on the business of the organization,
    - the likelihood of threats occurring, and
    - the ease of exploitation of vulnerabilities.
- a list of the safeguards identified to protect this ICT system, and
- the estimated cost of ICT security.

In the case of a system justified as only requiring baseline protection, it should still be possible to provide information under the above headings, even though in some cases there will be less detail than for systems for which a detailed risk assessment was conducted.

7.6 ICT security plan

The ICT security plan is a co-ordination document defining the actions to be undertaken to implement the required safeguards for an ICT system. This plan should contain the results of the review described above, the actions to be undertaken within short, medium and long time-frames to achieve and maintain the appropriate security level, the costs, and an implementation schedule. It should include for each system:

- the security objectives in terms of confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability,
- the risk assessment option decided on for this ICT system,
- an assessment of the residual risks expected and accepted after implementing the safeguards identified ,
- a list of the selected safeguards to be implemented, and a list of existing and planned safeguards, including a determination of their effectiveness and the safeguard upgrades needed; this list should include:
    - priorities for the implementation of the selected safeguards and the upgrading of existing safeguards, and
    - how these safeguards should work in practice,
    - the estimation of the installation and running costs for these safeguards,
    - the estimation of man-power resources for the implementation of these safeguards, and for follow-up actions, and
    - a detailed workplan for the implementation, containing:
        - priorities,
        - an implementation schedule in relation to priorities,
        - the budget needed,
        - responsibilities,
        - the security awareness and training procedures for ICT staff and end users which is needed to ensure the effectiveness of the safeguards,
        - a schedule for approval processes to take place where needed, and
        - a schedule for follow-up procedures.

Moreover, the ICT security plan should describe the mechanisms to control the process of correct implementation of safeguards, like

- the definition of progress reporting procedures,
- procedures to identify possible difficulties, and
- procedures to validate each of the points listed above, including procedures related to the possible modification of single parts or the plan itself, when needed.

The result of this step should be a detailed ICT security plan for each system, based on the ICT system security policy. It should ensure that the safeguards are implemented in time, according

to the priorities derived from the risks to the ICT system, and in line with a description of how to implement the safeguards and how to reach the security level which is appropriate. It also should contain a schedule for follow-up procedures to maintain this security level. These follow-up procedures are described in detail in Clause 10.

7.7 Security awareness and training

7.7.1 Security awareness

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 the effectiveness of safeguards. 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 program. The aim of a security awareness program is to explain 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 program should be designed to motivate employees, partners, contractors, and suppliers, and ensure acceptance of their responsibilities for security.

A security awareness program 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 program 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.

Security awareness programs within an organization may include a variety of activities. One such activity is the development and distribution of security awareness material (e.g., posters, bulletins, pamphlets, or briefings). 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 programs. Finally, courses are required which provide education at a professional level in very specific security topics.

To develop a security awareness program 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,
- program delivery,
- monitoring, and
- awareness program content.

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 ICT staff and the end users have enough knowledge of the ICT systems (hardware and software), and that they understand why safeguards are necessary and how to use them correctly. Only safeguards accepted by the ICT 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 ICT security policy and it should cover all objectives of the organizational ICT 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 the ICT 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 the ICT systems, including hardware and software,
- the objectives behind, and an explanation of, the corporate ICT security policy, any security guidelines and directives, and the risk management strategy, leading into an understanding of risks and safeguards,
- the necessary protection for and the risks to the ICT systems,
- restricted access to ICT 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 ICT staff and end users must not do because of security factors,
- the consequences if staff are responsible for security breaches,
- the ICT system security plans to implement and check safeguards,
- why these safeguards 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 must determine the breakdown of requirements in accordance with the corporate ICT security policy. This should be combined with overall security (i.e. not just ICT) 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 modern information technology.

The responsibility for determining the objectives and content of the awareness programme should be allocated at the senior management level to the ICT security forum (see Part 1 of ISO/IEC 13335). The responsibility for its development and implementation should be allocated to the corporate ICT 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 successfully develop a security awareness programme, the following components should be incorporated:

7.7.2 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.

7.7.3 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 ICT assets 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.

7.7.4 Monitoring of Security Awareness Programmes

There are two 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, and
- 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.), there will be a need to alter the security awareness programme to update the existing knowledge and skill levels to reflect those changes.

7.7.5 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 ICT security. The degree of depth of security training should be dependent on the overall importance ICT 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 also be provided. An ICT security training programme should be developed to cover all security needs relevant for the organization.

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

- personnel with key responsibilities for the ICT system design and development,
- personnel with key responsibilities for ICT system operations,
- corporate, ICT project, 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 impacts, for the organization or the individual, and
    - information sensitivity categorization scheme,
- the overall security process,
    - a description of the overall process, and
    - risk assessment components,
- safeguards, and the training necessary to comply with the safeguards,
- roles and responsibilities, and
- ICT system security policy.

The correct implementation and use of safeguards 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 safeguards. The following are examples of safeguard related topics that should be covered, with an emphasis on the need for balance between non-technical and technical safeguards:

- security infrastructure,
    - roles and responsibilities,
    - security policy,
    - regular security compliance checking, and
    - information security incident management,
- physical security,
    - buildings,
    - office areas, equipment rooms, and
    - equipment,
- personnel security,
- media security,
- hardware/software security,
    - identification and authentication,
    - logical access control,
    - accounting and security audit, and
    - actual storage clearance,
- communications security,
    - network infrastructure,
    - bridges, routers, gateways, firewalls, and
    - Internet and other external connections, and
- business continuity, including contingency planning/disaster recovery, strategy and plan(s).

7.8 Approval of ICT Systems

Organizations should ensure that approval takes place for all or selected ICT systems that they meet the requirements of the ICT system security policy and the ICT security plan. This approval process should be based on techniques such as security compliance checking, security testing, system evaluation and/or audit. Procedures may be according to internal or external standards, and the body carrying out the approval process may be internal or external to the organization.

The approval process should aim at ascertaining that the security safeguards implemented and maintained for an ICT system provide an appropriate level of protection. This approval should be valid for a defined operational environment, and for a defined period of time stated in the ICT system security policy or plan. Any significant changes to the security safeguards implemented, or changes of security relevant operational procedures, may require re-approval. Criteria for stimulating a re-approval should be included in the ICT system security policy.

The approval process consists mainly of document reviews, physical inspections and technical assessments (i.e. security compliance checking). For this to be achieved, the following key issues need to be addressed:

- the approval process has to be planned, thus tailoring the approach to the particular ICT system; this first step also helps to define the schedule, the resources needed and the responsibilities,
- the documents used during this process should be collected,
- a document review should be conducted to check their completeness and internal consistency with other documents,
- a review and testing against criteria described in the ICT security plan should be completed,
- a report should be produced which summarizes the results of the approval process and states whether the system's security has a full, partial, limited or no approval, any waivers and their duration of validity, and any limitations on processing, and
- re-approval should take place if the ICT system or its environment changes; it should also occur at the end of an approval period.

Once the approval process has been conducted, follow-up procedures will be implemented. Follow-up will help to detect and investigate changes in the system, its security and its environment. Upgrades will need to be implemented, following the detection, in which case re-approval will take place.

Approval of trading partner’s ICT systems might be needed against an agreed baseline security or code of practice for an organization that:

- wishes to establish its own tailored version of baseline security or a code of practice and issue it to its suppliers/trading partners for compliance and approval purposes prior to allowing connection to its ICT facilities,
- trades with a number of other companies and wishes to be connected, but to do so needs

to demonstrate an acceptable security profile against baseline security or code of practice as a whole, or

- wishes to establish the levels of security risks associated with other companies connecting to its ICT facilities, and the security profile it will expect other companies to meet. This will enable the company to enforce approval on the basis of a security compliance check review indicating compliance with those parts of the baseline security or code of practice consistent with its security profile.

8 Follow-up

[This Clause remains unchanged.]
Follow-up, even though often neglected, is one of the most important aspects of ICT security. The implemented safeguards can only work effectively if they are selected and checked in real business life and operational context. It must 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 safeguards 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 clause form the basis of an effective follow-up programme. The management of ICT security is an ongoing process that does not stop after the implementation of the ICT security plan.

8.1 Maintenance

The majority of safeguards 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 safeguards preserved.

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

Maintenance activities include:

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

The cost of maintenance and administration should always be factored in when assessing and selecting between different safeguards. This is because maintenance and administrative costs can differ widely between one safeguard and the next. Hence, this can often become a significant

determinant in the selection of safeguards. 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.

8.2 Security Compliance Checking

Security compliance checking is the review and analysis of the implemented safeguards. It is used to check whether ICT systems or services conform to the security requirements documented in the ICT system security policy and ICT system security plan. Security compliance checks may be used to check the conformance of:

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

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

The safeguards protecting the ICT system 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 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.

Security compliance checking, for approval and regular checks thereafter, must be based on the agreed safeguard lists from the last risk assessment results, on the ICT system security policy, as well as security operating procedures which the ICT management has signed up to, including for incident reporting. The objectives are to ascertain whether safeguards are implemented, implemented correctly, used correctly, and where relevant, tested.

A security compliance checker/inspector should walk through the building on a normal working day and look at the way security safeguards are used. Interviews are of course important - but the results should be cross-checked as much as possible. What somebody says may be what is believed, but not what it is: cross-check with the persons he/she works with.

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?

In summary, security compliance checking is not a small task and does need good experience and knowledge to be successfully completed. It is a separate activity from internal audit review.

8.3 Configuration management

Configuration management or control is the process of maintaining system configuration and can be done formally or informally. The primary security goal of configuration management is to ensure that up-to-date system configuration documentation is maintained, and that approved changes to the system are managed in such a manner that such changes do not reduce the effectiveness of safeguards and the overall security of the organization.

Configuration management is intended to manage approved changes. It is not intended to prevent changes to ICT systems on the basis of security. 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. If the change is a major one, it may be necessary to analyze some or all of the system safeguards again.

8.4 Change Management

Change management is the process used to help identify whether different security safeguards are required when changes to ICT systems occur. ICT systems and the environment in which they operate are constantly changing. These changes are a result of the availability of new ICT features and services, or the discovery of new threats and vulnerabilities. Changes to ICT systems include:

- new procedures,
- new features,
- software updates,
- hardware revisions,
- new business objectives, processes, functions, tasks, applications or constraints,
- new users to include external groups or anonymous groups, and
- additional networking and interconnection.

When a change to an ICT system occurs or is planned, it is important to determine what, if any, impact the change will have on the security of the system. If the system has a configuration control board or other organizational structure to manage technical system changes, the ICT security officer should be assigned to the board and be given the responsibility to make decisions about whether the change will impact 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 must 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.

8.5 Monitoring and audit

The effectiveness of security safeguards should be verified periodically. This is achieved by monitoring and compliance checking to ensure that the safeguards are functioning and being used in the manner expected. Many safeguards 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. These tools can also 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 program.

Monitoring is an ongoing activity which checks whether the system, its users, and the environment maintain the level of security as laid out by the ICT security plan. A plan for day to day monitoring should be prepared to provide additional guidance and procedures for ensuring ongoing secure operation. Users, operations personnel and system designers should periodically be consulted to ensure that all security issues are fully addressed and the ICT security plan remains up to date.

One of the reasons why monitoring is an important part of the maintenance of ICT security is that it is a way to detect security relevant changes. Some aspects that should be monitored are assets and their values, threats to and vulnerabilities of the assets, and the safeguards protecting the assets.

Assets are monitored to detect changes in their values, and to detect changes of the security objectives of the ICT system. Possible reasons for these variations are changes of:

- the business objectives of the organization,
- the applications running on the ICT system,
- the information stored or processed on the ICT system, and
- the ICT equipment.

Threats and vulnerabilities are monitored to detect changes in their impact (for example, caused by changes of the environment, the infrastructure or of technical possibilities), and to detect the appearance of other threats or vulnerabilities at an early stage. The changes of threats and vulnerabilities might be influenced by changes of the assets.

Safeguards are monitored to check their performance and effectiveness over time. It should be ensured that they are adequate and protect the ICT system according to the necessary level of protection. It is possible that the changes of assets, threats and vulnerabilities affect the effectiveness and adequacy of safeguards.

In addition, when new ICT systems are introduced or when changes are made to existing systems, there will be a need to ensure that such changes do not affect the status of existing safeguards, and that new systems are introduced with adequate security safeguards in place.

When security anomalies are found, there will be a need to investigate and report findings to management for possible review of safeguards, or, in serious circumstances, to investigate reviews of the ICT system security policy and initiate risk assessment activity.

To ensure adherence with the ICT system security policy, appropriate resources will have to be committed to maintain an appropriate level of day-to-day monitoring of:

- existing safeguards,
- the introduction of new systems or services, and
- planned changes to existing systems or services.

Many safeguards produce output in the form of logs of the occurrence of events. These logs should be analyzed using statistical techniques 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 management technique for controlling day-to-day monitoring is to prepare a security operating procedures document for the necessary activities. This document describes all the actions required to ensure that the level of security for all systems and services is maintained and not compromised as systems and services evolve over time.

The procedures for updating the security configuration should be documented. They should include coverage of adjusted security parameters and updating any security management information. These changes must be recorded and approved by the configuration management process. Procedures for performing routine maintenance should be established to ensure that security is not compromised. Trusted distribution procedures should be described for each security component where applicable.

The procedure for monitoring security safeguards 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.

8.6 Information security incident management

No security policies or safeguards will guarantee total protection of an information and communications system, service or network and related data. After safeguards have been implemented, residual weaknesses can remain that make information security incidents possible. Insufficient preparation by an organization to deal with such incidents and weaknesses will make any actual response chaotic and thus ineffective. Therefore a methodical and planned approach for the reporting and handling of ICT security incidents and weaknesses is essential for any organization that is serious about security.

A good scheme for the reporting and handling of ICT incidents can be used for addressing security weaknesses. The reporting and handling of ICT weaknesses is an important adjunct to that of ICT incidents, to aid the prevention of such incidents occurring in the first place. Thus, ICT incident management consists of the following processes:

- planning for and preparing a fully documented and accepted scheme, and related procedures, for the reporting and handling of ICT incidents and weaknesses, with all relevant personnel made fully aware of how to use, manage and support that scheme, and, importantly, senior corporate management and those personnel who will report to and receive feedback from the scheme fully ‘sold’ on its introduction and use;
- detection of the occurrence of suspected or actual ICT incidents and weaknesses;
- reporting of the occurrence of suspected or actual ICT incidents and weaknesses;
- analysis of suspected or actual ICT incidents and weaknesses;
- responding to confirmed ICT incidents;
- learning from suspected or actual ICT incidents and weaknesses.

To identify the risks and to measure their impact, it has been emphasized that risk assessment is required. To support risk assessment and enhance the results, information is required on security incidents. This information has to be gathered and analyzed in a secure way, and be seen to provide benefit. Thus it is important that any organization has a properly constructed and organized ICT incident analysis scheme (IAS) in operation, and that the information received and processed should be available to support risk assessment and management and other security related activities.

In order to be successful and to meet the needs of users and potential users, IAS have to be constructed based on the requirements of the users. Further, prior to any live operation there needs to be significant coverage of information security incident management in the security awareness programme to ensure that all likely to be involved understand what an IAS constitutes, the benefit offered, and how results obtained can be used to:

- improve risk assessment and management reviews,
- assist in the prevention of incidents,
- raise the level of awareness of ICT security related issues, and
- provide 'alert' information for use by such as information security incident response teams.

Related to these, key aspects that should be addressed by any IAS are:

- the establishment of pre-determined plans for the handling of unwanted incidents when they occur, whether caused by external or internal logical and physical attack, or by accident, equipment malfunction or people error,
- the training of nominated personnel in incident investigation, for instance to form information security incident response teams.

An information security incident response team may be more or less formalized as a defined group of persons who investigate the causes of ICT incidents, study potential future occurrences or carry out periodic studies and analyses of historical data. Its conclusions could give rise to remedial actions. An information security incident response team could be internal to an organization, or external (e.g. contracted).

With a plan and trained personnel in place, when an incident is in progress, hasty decisions will be avoided, evidence that can be used in tracking down and identifying the source of an incident will be preserved, protection for valuable assets will be more quickly established, and the costs not only of an incident but also of responding will be reduced. Further, any negative publicity will be minimized.

Any organization should prepare and plan for incidents with an efficient IAS in place, encompassing:

- preparation - pre-documented preventive measures, information security incident management guidelines and procedures (including for the protection of evidence, maintenance of event logs, and handling public relations), documentation required, and business continuity plans,
- notification - the procedures, means and responsibilities for reporting incidents, and to whom,
- assessment - the procedures and responsibilities for investigating incidents and determining their seriousness,
- management - the procedures and responsibilities for dealing with, limiting the damage from, and eradicating incidents, and notifying higher management,
- recovery - the procedures and responsibilities for re-establishment of normal service,
- review - the procedures and responsibilities for post-incident actions, including investigation of legal implications and trend analysis.

It is emphasized that while there is benefit to individual organizations from the use of IAS, some organizations may consider that even more benefit could be accrued from sharing some incident information with others to provide a wider base from which to gain 'alerts', quickly identify trends and enable prevention. To facilitate this an IAS database structure should be used which is flexible enough to cover the range of requirements for total (all sectors, threat types and impacts) and sectoral / threat / impact specific needs. Whether intra- or inter-organizational, each connecting IAS would use similar typology, metrics and structure to record information on incidents. This would allow for comparison and analysis. The use of a common structure is key to the enablement of more comprehensive results, and particularly a more solid base for the rapid

identification of 'alerts', in some cases that may not have been identified through individual IAS.

As implied above, the achievement of interfaces between IAS and risk assessment and management methods may significantly improve results, thereby increasing the benefit to be gained from IAS.

Information on threat occurrences will greatly aid the quality of threat assessment, and thus the risk assessment. Further, during the investigation of an incident or incidents it is likely that new and additional information will be gathered with regard to vulnerabilities and the manner in which they may be exploited. The exploitation of an IAS enables the user to identify and assess vulnerabilities, and thus provide valuable input to risk assessment approaches. This will be based partly upon the information introduced with regard to threats and partly with regard to the results of incident investigations, say by information security incident response teams. As an example, the threat of logical infiltration (the presence of an attacker and the attractiveness of the information stored or processed) can combine with vulnerability to logical infiltration (inadequacies or absence of appropriate logical access control mechanisms), and thereby create a risk. Therefore, the use of an IAS for the identification and assessment of vulnerabilities can take place via the use of threat information which is input into the database from incidents which have already been reported, combined with information from other sources, particularly information security incident response team investigations and studies, which may uncover previously unidentified vulnerabilities.

It should be noted that an IAS functions according to data reported concerning incidents that have occurred. Therefore, an IAS cannot provide information directly on those vulnerabilities that may be present but which have not been yet implicated in ICT incidents. Furthermore, IAS data should be used with caution for statistical and trend analysis because inputs may be incomplete or erroneously identified. Nevertheless, the result of information security incident response team investigations may provide some views on previously unforeseen vulnerabilities. Overall, regular IAS input to a risk assessment and management review may help to improve the quality of threat, risk, as well as vulnerability, assessment.

8.7 Business continuity management

There should be a managed process in place for developing and maintaining business continuity throughout an organization. Business continuity management provides for the availability of processes and resources in order to ensure the continued achievement of critical business objectives. It includes planning for contingencies and recovery from disasters.

Before being able to produce business continuity plans, an organization should ensure that a strategy is developed for the overall approach to business continuity. This strategy should be based on business impact analysis results and related agreed minimum resource, accommodation, ICT infrastructure and communications requirements, and agreed recovery time periods.

Business continuity plans are business oriented and contain information about how to operate a business when the support processes, including ICT systems, are degraded or unavailable.

Disaster recovery plans, in contrast, are primarily technology oriented and describe how to restore to operation ICT systems affected by an incident. Both business continuity and disaster recovery plans should include:

- criteria that constitute a disaster,
- responsibility for activating the recovery plans,
- responsibilities for various recovery activities,
- descriptions of recovery activities and resources, with scenarios for critical resource unavailability, and
- responsibility for testing that the recovery plan is effective.

These plans should address a number of scenarios including:

- various lengths of interruption,
- loss of different types of facilities,
- total loss of physical access to premises,
- the need to return to the state that would have existed if the disruption had not occurred, and
- the need to cope with service demands in excess of what can be handled with available resources.

Organizations should also consider crisis management plans. Unforeseen incidents may result in a crisis, either within the organization or in the external environment in which the organization operates. To manage during crisis conditions, organizations should have crisis management plans in place that include:

- crisis preparation,
- crisis organization and management, and
- crisis communication.

Annex A An example contents list for a corporate ICT security policy

(informative)

Contents

Annex B Risk assessment strategies

Before starting any risk assessment activity, an organization should have a strategy in place for this analysis, and its constituent parts (methods, techniques, etc.) should be documented in the corporate ICT security policy. The means and criteria for the selection of the risk assessment method should be agreed for the organization. The risk assessment strategy should ensure that the approach chosen is suitable for the environment and that ICT focuses the security efforts where they are really needed. The options presented below describe four different risk assessment approaches. The basic difference between each of these options is the depth of the risk assessment. Since it is generally too costly to conduct a detailed risk assessment for all ICT systems, and it is also not effective to give only peripheral attention to serious risks, a balance between these options is needed.

Apart from the possibility of doing nothing, and accepting that there will be exposure to a number of risks of unknown magnitude and impact, there are four basic options for a corporate risk assessment strategy:

- use the same baseline approach for all ICT systems, irrespective of risks facing the systems, and accept that the level of security may not always be appropriate,
- use an informal approach to perform risk assessment and concentrate on ICT systems which are perceived as being exposed to high risks,
- conduct detailed risk assessment using a formal approach for all ICT systems, or
- carry out an initial 'high level' risk assessment to identify ICT systems exposed to high risks and those which are critical for the business, followed by a detailed risk assessment for these systems, and applying baseline security to all other systems.

These different possibilities for addressing security risks are discussed below, and then a recommendation is made as to the preferred approach.

If an organization decides to do nothing about security, or to postpone the implementation of safeguards, management should be aware of the possible implications of this decision. While this requires no time, money, personnel or other resources, it has a number of disadvantages. Unless an organization is confident about the non-critical nature of its ICT systems, it may be leaving itself open to serious consequences. An organization may not be in compliance with legislation and regulation, and its reputation may suffer if it is subject to breaches in security, and it is shown that no preventive action has been taken. If an organization has very few concerns about ICT security, or does not have any business-critical systems, then this may be a viable strategy. However, the organization is left in a position of not knowing how good or bad the situation really is, and for most organizations this is unlikely to be a good solution.

Baseline Approach

For the first option, an organization could apply baseline security to all ICT systems by selecting

standard safeguards. A variety of standard safeguards are suggested in baseline documents and codes of practice.

There are a number of advantages with this approach such as:

- only a minimum amount of resources is needed for risk assessment and management for each safeguard implementation, and thus less time and effort is spent on selecting security safeguards,
- baseline safeguards may offer a cost-effective solution, as the same or similar baseline safeguards can be adopted for many systems without great effort if a large number of the organization's systems operate in a common environment and if the security needs are comparable.

The disadvantages of this option are:

- if the baseline level is set too high, there might be an excessive level of security on some ICT systems,
- if the level is set too low there may be a lack of security on some ICT systems, resulting in a higher level of exposure, and
- 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 safeguards are still sufficient.

If all of an organization’s ICT systems have only a low level of security requirements then this might be the most cost-effective strategy. In this case, the baseline has to be chosen such that ICT reflects the degree of protection required by the majority of ICT systems. Most organizations will always need to meet some minimum standards to protect sensitive data and to comply 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 a common standard to all systems.

[9.2]
The objective of baseline protection is to establish a minimum set of safeguards to protect all or some ICT systems of an organization. Using this approach, it is possible to apply baseline protection organization-wide, and, as reflected above, additionally use detailed risk assessment reviews to protect ICT systems at high risk or systems critical to the business. The use of the baseline approach reduces the investment that the organization has to make in the performance of risk assessment reviews.

The appropriate baseline protection can be achieved through the use of safeguard catalogues, which suggest a set of safeguards to protect an ICT system against the most common threats. The level of baseline security can be adjusted to the needs of the organization. A detailed assessment of threats, vulnerabilities and risks is not necessary. All that has to be done to apply baseline protection is to select those parts of the safeguard catalogue that are relevant for the ICT system considered. After identifying the safeguards already in place, a comparison is made with those safeguards listed in the baseline catalogue. Those that are not already in place, and are

applicable, should be implemented.

Baseline catalogues may specify safeguards to be used in detail, or they may suggest a set of security requirements to be addressed with whatever safeguards appropriate to the system under consideration. Both approaches have advantages. One of the objectives of the baseline approach is consistency of security safeguards throughout the organization, which can be achieved by both approaches.
Several documents are already available which provide sets of baseline safeguards. 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 safeguard catalogues to be used by a number of different organizations. For example, catalogues of baseline safeguards could be obtained from:

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

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

[from Annex G Clause 6]
The following gives a brief overview of the topic of safeguard selection, and how and when the concept of baseline security can be used in that process. There are two main approaches to safeguard selection, i.e. using a baseline approach and carrying out detailed risk analyses. There are several different ways of conducting detailed risk analyses, one of which is described in detail in Clauses 6 and 7, and is called detailed risk analysis.

Conducting a detailed risk analysis has the advantage that a comprehensive view of the risks is achieved. This can be used to select safeguards that are justified by the risks, and thus should be implemented. This avoids the provision of too much or too little protection. As this can require a considerable amount of time, effort and expertise, it may be most suitable for ICT systems at high risk, whereas a simpler approach can be considered to be sufficient for lower risk systems. Using a high-level risk analysis can identify the lower risk systems. This high-level risk analysis does not need to be a formalized or complex process. Safeguards for low risk systems can be selected by applying baseline security. Baseline security is at least the minimum level of security defined by an organization for each type of ICT system. This level of baseline security is achieved by implementing a minimum set of safeguards known as baseline safeguards.
Because of differences in the safeguard selection process, two different ways of applying the baseline approach are considered in this document:

- using a baseline approach where safeguards are recommended according to the type and characteristics of the ICT system considered, and
- using a baseline approach where safeguards are recommended according to security concerns and threats, as well as taking into account the ICT system considered.

If an organization decides to apply baseline security to either the whole organization or parts of it, it is necessary to decide which parts of the organization are suitable to be protected by the

same baseline, and what level of security this baseline should be aimed at. In most cases when using baseline security, a lower level of security should not be allowed, whilst additional safeguards should be implemented where justified and necessary to manage medium and high risks. Alternatively, the baseline could reflect an average level for the organization, i.e. exceptions would be permitted above and below the baseline if they were justified, for example, by the results of risk analysis.

A baseline security manual (or catalogue) for the whole organization or for parts of the organization may be developed. For the establishment of a baseline security manual (or catalogue), the safeguards previously identified for ICT systems or groups of ICT systems are considered and a common set of safeguards is identified. Depending on security needs, concerns, and constraints, different levels of baseline security can be chosen. The advantages and disadvantages must be considered in order to facilitate a suitable decision for each organization.

One of the benefits of baseline security is that if it is applied to a group of ICT systems, a certain security level can be relied on throughout that group. In these circumstances, it is usually most beneficial to develop and document an organization or department-wide baseline catalogue of security safeguards.

[from Annex G, Clause 9]
There are two different sets of safeguards, mechanisms and/or procedures, which can be applied to protect ICT systems. On one hand, there are quite a few organizational safeguard categories that are generally applicable for each ICT system if the specific circumstances make them necessary, irrespective of the individual components. Because of their general applicability, safeguards 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 safeguards; the selection of these safeguards 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 safeguards 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. Again, a more detailed selection can only be made by considering further information. After all safeguard types applicable for the ICT system considered are identified, further information on these safeguard types and on specific safeguards can be obtained by using one or more of the documents summarized in the Annexes G-A to G-H. Before implementing the safeguards selected, they should be checked carefully against the safeguards already in place and/or planned. The use of a more detailed analysis should be considered to select additional safeguards. If safeguards are selected according to different criteria (e.g. baseline safeguards and additional safeguards), the final set of safeguards 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 safeguards without a detailed consideration is to apply application-specific baselines. For example, there are baseline manuals available for telecommunications, health care, banking, (see Annexes G-B, G-E, and G-F), and many more. When using these manuals, it is, for example, possible to check the existing or planned safeguards against the ones recommended. But before choosing which safeguards are to be

implemented, it is still helpful to have a closer look at security needs or concerns.

Informal Approach

This option is to conduct informal pragmatic risk analyses. An informal approach is not based on structured methods, but exploits the knowledge and experience of individuals.
The advantage of this option is:

- it usually does not require a lot of resources or time. No additional skills need to be learned to do this informal analysis, and it is performed quicker than a detailed risk assessment.

However, there are a number of disadvantages:

- without some sort of formal approach or comprehensive checklists, the likelihood of missing some important details increases,
- justifying the implementation of safeguards against risks assessed in this way will be difficult,
- individuals who have minimum previous experience in analysing risks may have little guidance to assist them in this task,
- some approaches in the past have been vulnerability driven, i.e. security safeguards were implemented based on identified vulnerabilities, without considering whether there were any threats likely to exploit these vulnerabilities, i.e. whether there was a real need for the safeguards,
- a degree of subjectivity may be introduced; the particular prejudices of the reviewer may influence the results, and
- problems may arise if the person who carried out the informal risk assessment leaves the organization.

The informal approach is based on collection of objective information (incidents, identified important asset, etc.) and should not be confused with arbitrary actions based on unconfirmed information and sources. Arbitrary security measures are too often ineffective and expensive.

Based upon the above disadvantages, this option is not an effective approach to risk assessment for many organizations.

Detailed risk assessment

The third option is to conduct detailed risk assessment reviews for all ICT systems in the organization. Detailed risk assessment 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 thence identify justified security safeguards. This approach is described in detail in Clause 7.

The advantages with this approach are:

- it is likely that appropriate safeguards are identified for all systems, and
- the results of the detailed analysis can be used in the management of security changes.

The disadvantages of this option are:

- it requires a considerable amount of time and effort, and expertise, to obtain results.
- there is the possibility that the security needs of a critical system are addressed too late, since all ICT systems would be considered in the same detail and a considerable amount of time is required to complete the analyses.

Therefore, it is not advisable to use detailed risk assessment for all ICT systems. If this approach is chosen, there are a number of possible implementations:

- use of a standard approach, that meets the criteria reflected in this International Standard,
- use a standard approach in different ways appropriate to the organization; the use of 'risk modeling techniques' could be of advantage to some organizations.

Combined approach

The combined approach involves, first, the conduct of a high-level risk assessment for all ICT systems. Then, once those at highest risk have been identified, a detailed risk assessment is conducted on those systems. For lower risk systems, a baseline approach is selected. Additional advantages of this option are:

- the incorporation of an initial quick and simple approach is likely to gain acceptance of the risk assessment programme,
- it should be possible to quickly 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, and
- the follow up actions will be more successful.

The only potential disadvantage is:

- as the initial risk analyses are at a high level, and potentially less accurate, some systems may not be identified as requiring detailed risk assessment. However, these systems would still be covered by baseline security. Also, these systems can be re-visited whenever necessary to check whether more than a baseline approach is needed.

The adoption of a high-level risk assessment approach, combined with the baseline approach, and detailed risk assessment where appropriate, offers the majority of organizations the most effective way forward.

Annex C Valuation of assets

(informative)

The valuation of an organization's assets is an essential step in the overall 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. To perform the asset valuation, an organization first needs to identify all of its assets. To assure that all assets are accounted for, it is often helpful to group them by type, such as:

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

This is also valuable to assign an asset owner who will be responsible for determining the asset's value.

The next step is to agree upon the scale to be used and the criteria for assigning a particular valuation to an asset. 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 a company's good name or 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 potential damage or adverse business impact which would result from security incidents with an assumed set of circumstances. It is emphasized that this approach accounts for damage and other impact costs 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 must 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 damages 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 commercial 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 a 'low' or a 'high' damage - a damage that might be disastrous for a small organization could be low or even negligible for a very large organization.

Annex D List of possible threat types

(informative)

The following list gives examples of typical threats. The list can be used during the threat assessment process. Threats can be caused by one or more of deliberate, accidental or environmental (natural) incidents. 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 ICT assets, A is used for all human actions which accidentally can damage ICT 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.

Earthquake	E
Flooding	A, D, E
Hurricane	E
Lightning	E
Industrial Action	A, D
Bomb attack	A, D
Use of arms	A, D
Fire	A, D
Wilful Damage	D
Failure of power supply	A, D, E
Failure of water supply	A, D, E
Air conditioning failure	A, D, E
Hardware failures	A
Power fluctuation	A, E
Extremes of temperature and humidity	A, D, E
Dust	E
Electromagnetic radiation	A, D, E
Electrostatic charging	E
Theft	D
Unauthorized use of storage media	D
Deterioration of storage media	E
Operational staff error	A, D
Maintenance error	A, D
Software Failure	A, D
Use of software by unauthorized users	A, D
Use of software in an unauthorized way	A, D
Masquerading of user identity	D
Illegal use of software	A, D
Malicious software	A, D
Illegal import/export of software	A, D
Network access by unauthorized users	D
Use of network facilities in an unauthorized way	D
Technical failure of network components	A

Transmission errors	A
Damage to lines	A, D
Traffic overloading	A, D
Eavesdropping	D
Communications infiltration	D
Traffic analysis	D
Misrouting of messages	A
Rerouting of messages	D
Repudiation	D
Failure of communications services (i.e. network services)	A, D
Staff shortage	A, D
User errors	A, D
Misuse of resources	A, D

Annex E Examples of common vulnerabilities

(informative)

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 also exploit these vulnerabilities.

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, 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)

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)

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. 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)

Annex F Types of risk assessment methodologies

(informative)

Risk assessment has a number of stages that have been discussed in this and the other parts of this International Standard. Those stages are:

- asset identification and valuation (potential adverse business impact assessment),
- threat assessment,
- vulnerability assessment,
- existing/planned safeguard assessment, and
- risk assessment.

The final stage 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 impacts 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 unwanted impacts, and
- the existing or planned safeguards, which might reduce the severity of vulnerabilities, threats and impacts.

The objective of risk assessment is to identify and assess the risks to which the ICT system and its assets are exposed, in order to identify and select appropriate and justified security safeguards. When assessing the risks, several aspects are considered including impact and likelihood.

The impact 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 probability 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;
- 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. Currently, there is no right or wrong method to use. 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 data assets (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 data assets. 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 data assets.

The values for data assets 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 data assets in terms of the worst case scenarios that could be reasonably expected to happen from adverse business impacts due to unauthorised disclosure, unauthorised modification, repudiation, non-availability for varying time periods, and destruction.

The valuation is accomplished using data asset 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 impact). 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 impact types 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, acts of god, errors by people, and equipment/software/line failure.

The asset values, and the threat and vulnerability levels, relevant to each impact type, 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 impact 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 impact (asset value) and likelihood of threat occurrence (taking account of vulnerability aspects). The first step is to evaluate the impact (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 impact and the lowest probability of occurrence.

Threat descriptor (a)	Impact (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 impact and probability 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 frequency and the possible damage of risks:

In this example, the emphasis is placed on the impact of 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 damage 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 frequency 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

Frequency 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 frequency 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
Frequency 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 frequency 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 frequency 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 also different assets within one system.

Example 4 Distinction between tolerable and intolerable risks:

Another way of measuring the risks is to only distinguish between tolerable and non-tolerable risks. The background of this is that the measures 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
Frequency 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 G: Selection of safeguards

[formerly TR 13335-4, with modification]

General

Annex G provides additional information on safeguard selection. The decision on which risk assessment approach to use depends in part on consideration of:

- what type of ICT system is involved (e.g. a stand-alone PC, or connected to a network),
- what are the ICT system's location(s) and surrounding environmental conditions like,
- what safeguards are already in place and/or planned, and
- whether the assessments made provide enough information to select baseline safeguards for the ICT system?

Annex G provides an overview of safeguards to be selected, divided into organizational and physical safeguards (which are selected according to security relevant needs, concerns and constraints) and ICT system specific safeguards, both grouped into safeguard categories. For each safeguard category, the most typical types of safeguards are described, including a brief explanation about the protection they are aimed at providing. Specific safeguards within these categories, and their detailed description, can be found in baseline security documents that are referenced in Annexes G-A to G-H. In order to facilitate the use of these documents, a cross-reference between the safeguard categories of this document and the chapters of the various documents in the Annexes is provided in a table for each safeguard category.

If it is decided that baseline assessment is detailed enough for the selection of safeguards, a list of applicable safeguards for each of the typical ICT systems is described in Clause x. If safeguards are selected based on the type of ICT system, separate baselines might be necessary for standalone workstations, networked workstations or servers. To achieve the required level of security, all that is necessary to select the safeguards applicable under the specific circumstances, is to compare these with the safeguards already existing (or planned), and to implement those which are not already implemented.

If it is decided that a more in-depth assessment is necessary for the selection of effective and suitable safeguards, a high level assessment provides support for that selection taking into account the high level view of security concerns (according to the importance of the information) and likely threats. Hence, in this section, the safeguards are suggested according to the security concerns identified, taking into account the threats, and finally the type of ICT system is considered. The following figure gives an overview of the ways to select safeguards described in this Annex and in previous clauses:

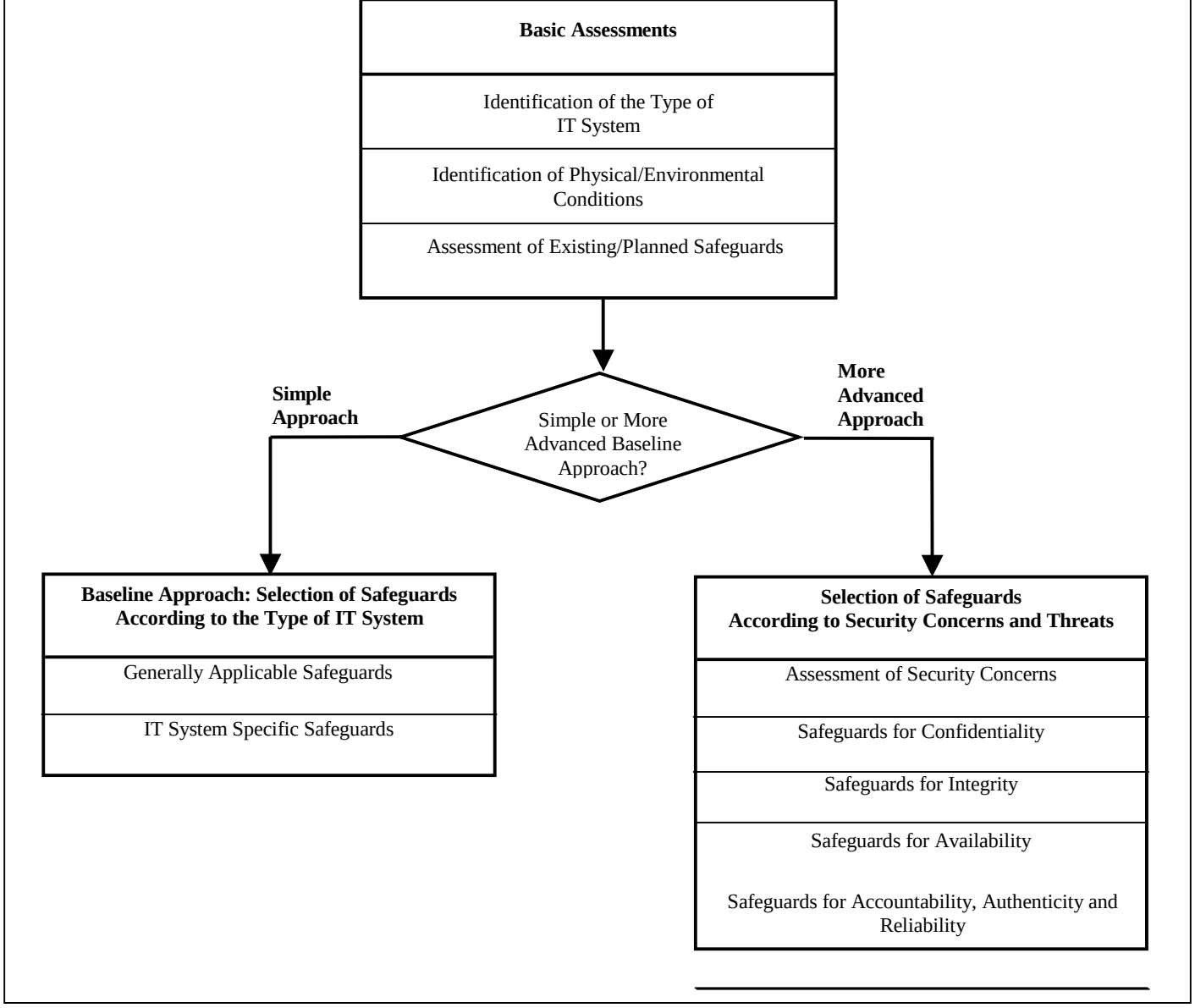

Figure G-1 - Selection of Safeguards According to the Type of ICT System or According to Security Concerns and Threats

Annex B, above, describes a way to select safeguards from baseline security safeguard documents, which can be applied either for an ICT system, or to form a set of safeguards applicable to a range of ICT systems in defined circumstances. By focusing on the type of ICT system considered, the baseline approach yields the possibility that some risks are not adequately managed, and that some safeguards are selected which are not necessary or not appropriate. The high-level approach to focus

The baseline approach can be used to support safeguard selection without more detailed assessments.

It may be determined that a detailed risk assessment is necessary because of high security concerns and needs. Factors which might influence the safeguard selection, like any constraints that have to be considered, any legal or other requirements which have to be fulfilled, etc, are addressed below. This approach is not a baseline approach, but might nevertheless be used to select safeguards to complement (i.e. add to) baseline safeguards in some circumstances. Alternatively, this approach might be used without any relation to baseline protection.

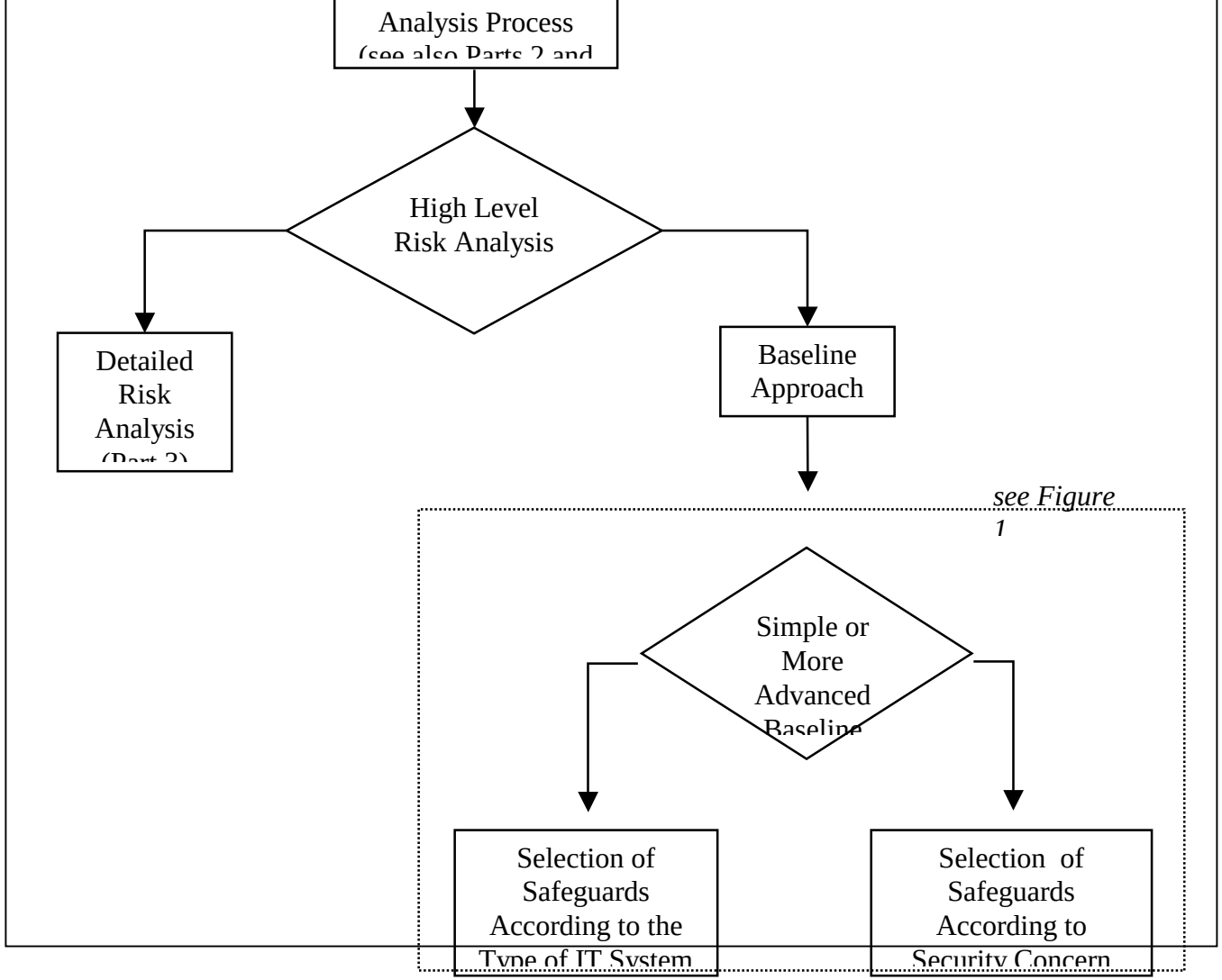

Figure G-2 - Ways of Safeguard Selection

The baseline approach to be used should be chosen depending on the resources that can be spent on the selection process, the perceived security concerns, and the type and characteristics of the ICT system considered. If an organization does not wish to spend a lot of time and effort on the selection of safeguards (for whatever reason), a baseline approach suggesting safeguards without further assessments may be suitable. However, if the organization's business operations are moderately dependent on the ICT system or service, and/or the information handled is sensitive, it is very likely that additional safeguards will be required. In this case, it is highly recommended that at least a high level view is taken of the importance of the information and likely threats to gain a better focus of

very sensitive, the risks may be high, and a detailed risk analysis is the best way to identify appropriate safeguards.

Specific safeguards should be identified based on detailed risk analysis where

- the type of ICT system considered is not represented appropriately by the types considered in this report,
- it is felt that the business or the security needs are not commensurate with the solutions suggested in these clauses, or
- a more detailed assessment is warranted anyway due to potential high risks or the significance of the ICT system to the business.

It should be noted that even when a detailed risk analysis is undertaken, it may still be useful to apply baseline safeguards to an ICT system.

The first decision an organization has to make is whether to use a baseline approach on its own, or as part of a more comprehensive risk assessment strategy. In taking this decision, it should be noted that in using the baseline approach on its own the resultant process for the selection of safeguards may result in less optimised security than if a wider risk analysis strategy was adopted. However, the lower costs and less resources needed for the selection of security safeguards, and the achievement of at least a minimum level of security for all ICT systems, could be reasons for deciding to follow a baseline approach on its own.

Baseline protection for an ICT system can be achieved through the identification and application of a set of relevant safeguards that are appropriate in a variety of low risk circumstances, i.e. they fulfill at least the minimum security needs. For example, the appropriate baseline security safeguards can be identified through the use of catalogues which suggest sets of safeguards for types of ICT systems to protect them against the most common threats. These catalogues of safeguards contain information on safeguard categories or detailed safeguards, or both, but generally do not indicate which safeguards should be applied in particular circumstances. It is possible that if an organization’s (or part of an organization’s) ICT systems are very similar in nature and service provided, that safeguards selected through a baseline approach could apply to all ICT systems. The following figure shows the different ways of using a baseline approach discussed in this document.

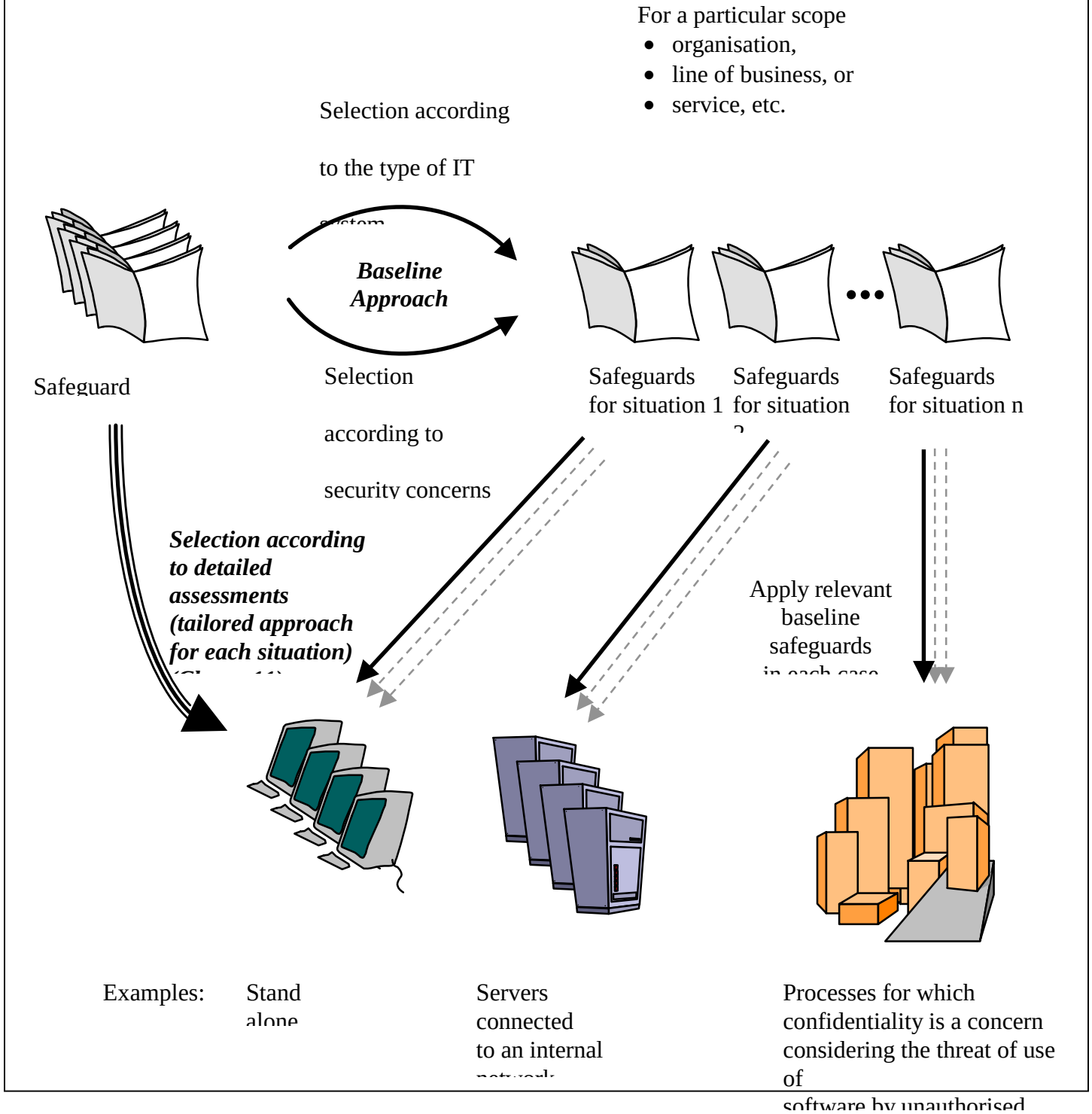

Figure G-x – Approaches to Safeguard Selection

Basic Assessments

The process of safeguard selection always requires some knowledge of the type and characteristic of the ICT system considered (for example, a stand-alone workstation, or a workstation connected to a network), since this has significant influence on the safeguards 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 safeguards is the assessment of existing and/or planned safeguards. This avoids unnecessary work, and waste of time, effort, and money. Hence, it is highly recommended that the assessments described in Clause 7 be always used as a basis for the selection of safeguards. When selecting safeguards, business requirements and the organization's approach to security should be taken into account. Finally, it is necessary to determine whether these assessments provide enough information for the selection of baseline safeguards, or whether a more detailed assessment or a detailed risk analysis is necessary.

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, safeguards 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,
- 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 safeguards. Since all safeguards 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. The reader should also 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?

- 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 safeguards 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.

Assessment of Existing/Planned Safeguards

After assessing the physical environment conditions and the components of the ICT system, all other safeguards already in place or planned should be identified. This is necessary to avoid an already existing or planned safeguard being reselected, and the knowledge of the safeguards implemented or planned helps to select further safeguards acting in combination with them. When selecting safeguards, the compatibility of the existing safeguards with the selected ones should also be considered. A safeguard may conflict with another or hinder its successful operation and the protection provided.

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

- review documents containing information about the safeguards (for example, ICT security plans or concepts) - if the security process is well documented, all existing or planned safeguards and the status of their implementation should be listed there,
- check with the persons responsible (e.g. ICT system security officer, building manager or operations manager) and the users as to which safeguards are really implemented for the ICT system under consideration, and
- walk through the building viewing the safeguards, compare those implemented with the list of what safeguards should be there, and check those implemented as to whether they are working correctly and effectively.

It may be determined that existing safeguards exceed current needs. In this case, consideration should be given to removing these safeguards. If removing redundant or unnecessary safeguards is considered, security and cost factors should be taken into account. Since safeguards influence each

high maintenance costs, it can be cheaper to remove them.

Safeguards

This section provides an overview of possible safeguards to be implemented to improve security. Some of these safeguards are mechanisms, others can be considered as procedures, which ought to be in place. Organizational, physical and information technology safeguards that could be applicable for ICT systems are considered. It should be noted that safeguards are described regardless of the way by which they might be selected, i.e. some of these safeguards might be selected using any way; others might only be identified carrying out detailed risk assessment.

To make it easier to describe the various types of safeguards, safeguard categories have been introduced. The following subclauses contain a brief description of these safeguard categories, and which types of safeguards are relevant to them. Also, references to the manuals listed in Annexes G-A to G-H are provided, pointing to where more detailed information can be found about the safeguards mentioned here.

Organizational and Physical Safeguards

At the end of this clause tables relating to each subsection show where to find additional information about the safeguard categories mentioned.

ICT Security Management and Policies
This safeguard category contains all those safeguards dealing with the management of ICT security, the planning of what should be done, assignment of responsibilities for these processes, and all other relevant activities. These safeguards have already been introduced earlier in this document. The aim of these safeguards is to achieve an appropriate and consistent level of security throughout an organization. Safeguards in this area are listed below.

- Corporate ICT Security Policy
  A written document should be developed which contains rules, directives and practices describing how assets are managed, protected and distributed within an organization. It should indicate the need for, and provide guidance on the content of the ICT system security policy documents.
- ICT System Security Policy
  For each ICT system, an ICT system security policy should be developed which describes the safeguards that are in place or should be implemented. The procedures to be followed to secure this system, and where possible a summary of the security concerns and/or risks which justify the safeguards.
- ICT Security Management
  The management of ICT security should be formalized and co-coordinated within the organization in a manner appropriate to its size, for example by establishing an ICT security

- Allocation of Responsibilities
  The responsibilities for organization-wide ICT security should be clearly documented and allocated according to the corporate ICT security policy and ICT system security policies.
- Organization of ICT Security
  All business processes that can support ICT security (e.g. procurement, co-operation with other organizations) should be organized to provide that support in a secure manner.
- Asset Identification and Valuation
  All assets within an organization and for each ICT system should be identified, and their value to the conduct of business should be assessed.
- Approval of ICT Systems
  Approval of ICT systems should take place according to the ICT security policy. The approval process should aim at ascertaining that the safeguards implemented provide an appropriate level of protection. It should take into account that an ICT system might include networks and underlying communications.

Security Compliance Checking

It is important that compliance is maintained with all required safeguards, and relevant laws, regulations and policies, since any safeguard, regulation or policy can only be working as long as users comply, and systems conform, with them. Safeguards in this area are listed below.

- Compliance with ICT Security Policies and Safeguards

  Regular checks should be conducted to ensure that all safeguards that should be in place, as listed in the corporate ICT 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 ensuring that all legal and regulatory requirements related to the country or countries in which the ICT system is located, are met. Where this legislation exists, this includes legislation on data protection and privacy, software copying, safeguarding of organizational records, misuse of ICT systems or cryptography.

Incident Handling

Everybody in the organization should be aware of the need to report security incidents, including software malfunctions, and identified weaknesses, as quickly as possible. The organization should provide a reporting scheme that makes that possible. Incident handling includes:

- Reporting of Security Incidents
  Each employee should be aware of the commitment to report security incidents. Incidents can also be identified and reported by tools. In order to facilitate effective incident handling, a reporting scheme and contact points within the organization should be provided by the organization.
- Reporting of Security Weaknesses

responsible as soon as possible.

- Reporting of Software Malfunctions
  If users are noting any security relevant software malfunctions, they should report them to the person responsible as soon as possible.
- Incident Management
  A management process should be in place that supports the protection against incidents, their detection and reporting, and appropriate reaction to the incident. Information about incidents should be collected and evaluated to avoid incidents in the future and limit the damage, if they occur.

Personnel

Safeguards in this category should reduce the security risks resulting from errors or intentional or unintentional breaking of security rules by personnel (permanent or contracted). Safeguards in this area are listed below.

- Safeguards for Permanent and Temporary Staff
  All employees should be aware of their security roles and responsibilities. All security relevant procedures, which should be followed by the personnel, should be stated in a document. Employees should be subject to recruitment checks before employment, and a confidentiality agreement should be signed if that is necessary.
- Safeguards for Contracted Personnel
  Contracted personnel (e.g. cleaning or maintenance staff) should be controlled, as well as any other visitor. Contracted, certainly long-term, personnel should sign a confidentiality agreement before having access (physical or logical) to the organization's ICT facilities.
- Security Awareness and Training
  All personnel who use, develop, support and have access to ICT equipment should receive regular security awareness briefings and material. This should ensure that the personnel are aware of the importance of the information processed to the business, associated threats, vulnerabilities and risks, and thus understand why safeguards are needed. Users should also be trained to use ICT facilities correctly, to avoid errors. For selected personnel, e.g. ICT security officers, security administrators, more specific security training might be necessary.
- Disciplinary Process
  All employees should be aware of the consequences of intentional or unintentional violations of the organization-wide and specific ICT system security policies or any other documented security agreement.

Operational Issues

Safeguards in this area aim at all procedures maintaining the secure, correct and reliable functioning of the ICT equipment and related system(s) used. Most of these safeguards can be realized by implementing organizational procedures. Operational safeguards are necessary in combination with other, for example, physical and technical, safeguards. Safeguards in the area of operational issues are listed below.

primary security goal is to ensure that changes to ICT systems do not reduce the effectiveness of safeguards and the overall security provided. Change management can contribute to the identification of new security implications when changes occur to ICT systems.

- Capacity Management
  Capacity management should be used to avoid failures due to inadequate capacity. Future capacity requirements and current trends should be taken into account when assessing the capacity necessary for an ICT system.
- Documentation
  All aspects of ICT configurations and operations should be documented to ensure continuity and consistency. The security of an ICT system also needs to be documented in the ICT system security policy, security operating procedures document, and business continuity strategy report(s) and plan(s). The documentation should be current and accessible.
- Maintenance
  ICT equipment should be correctly maintained to ensure its continued reliability, availability and integrity. All security requirements that have to be met by the maintenance providers should be fully documented in the maintenance contracts. Maintenance should take place in accordance with the supplier's contract, and should only be done by authorized personnel.
- Monitoring Security Relevant Changes
  Changes to the impacts, threats, vulnerabilities, and risks and their associated characteristics should be monitored. The monitoring should include both existing and new aspects. The environment within which the system is located should also be monitored.
- Audit Trails and Logging
  Auditing and logging capabilities of servers (for example, audit trail recording and analysis facilities), networks (for example, the auditing facilities of firewalls or routers) and applications (for example, the auditing facilities of messaging applications or transaction processing applications) should be utilised to record details of incidents. The details that should be recorded include readily identifiable unauthorized or error events, as well as apparently normal events that may need to be analysed at a later date. Audit trails and logs should be regularly reviewed to detect unauthorized activities and allow appropriate corrective measures to be taken. Events in logs should also be analysed for repetition of similar events that may indicate the presence of vulnerabilities or threats for which inadequate safeguards are present. Such analysis may also reveal patterns in apparently unrelated incidents that may allow identification of people performing unauthorized activity or the root cause of a security problem.
  [Note. In this text ‘auditing capabilities’ of systems and applications and ‘logging capabilities’ are used to mean the same thing. Whilst such capabilities can be used to support broader audits of financial integrity they only meet part of the requirements for such activity and the reader should be aware of this terminology usage.]
- Security Testing
  Security testing should be used in order to ensure that all ICT equipment and all related software components are operating in a secure manner. Security testing should encompass the security requirements defined in the ICT system security policy and test plans, and

- Media Controls
  Media controls include a variety of safeguards to provide physical and environmental protection and accountability for tapes, discs, printouts, and other media. This includes marking, logging, integrity verification, physical access protection, environmental protection, transmittal, and secure disposal.
- Assured Storage Deletion
  The confidentiality of information previously written to a storage device should be preserved if the information is no longer required. It should be ensured that files containing confidential material are erased and physically overwritten or otherwise destroyed – the activation of delete functions does not always do that. Facilities approved by the responsible personnel (e.g. the ICT security officer) should be available for the users to be used for complete and secure deletion.
- Segregation of Duties
  In order to minimize the risks and the possibilities of misuse of privileges, segregation of duties should be applied where required and possible. In particular duties and functions that, in combination, can lead to the circumvention of safeguards or audits, or to an undue advantage for the employee, should be kept separate.
- Correct Software Use
  It should be ensured that no copyrighted material is copied, and that the license agreements are obeyed for proprietary software.
- Software Change Control
  Software change control should be applied to maintain the integrity of software when changes are made (software change controls applies only to software, whereas configuration and change management described in safeguard area 1. of this clause applies to ICT systems and their environment as a whole). Change control procedures for software that manage all changes and ensure that security is maintained throughout the whole process should be established. This includes authorization for changes, security consideration for intermediate solutions, and security checks of the final solution.

Business Continuity Planning

In order to protect business, especially critical business processes, from the effects of major failures or disasters and to minimize the damage caused by such incidents, an effective business continuity, including contingency planning/disaster recovery, strategy and plan(s) should be in place. This includes the following safeguards.

- Business Continuity Strategy
  A business continuity, including contingency planning/disaster recovery, strategy should be formulated and documented related to the ICT system considered, based on the identified potential adverse business impacts from unavailability, modification and destruction.
- Business Continuity Plan
  Based on the business continuity strategy, business continuity plan(s), including plans for contingency and disaster recovery, should be developed and documented.

it is working under 'real life' circumstances, and that it is known to all relevant members of the staff. Since business continuity plans can become out-of-date quickly, it is important that they are updated regularly. The business continuity strategy should also be updated whenever necessary.

- Back-ups
  Back-ups should be made of all important files and other business data and of important system programs and documentation. The frequency of back-ups should be in line with the importance of the information and the business continuity plan. Back-ups should be stored securely and remotely, and recovery checked regularly for reliability.

Physical Security

Safeguards in this area deal with physical protection. They should be considered in combination with the identification of the environment. Several of the following items apply to buildings, secure areas, computer rooms and offices. The safeguard selection depends on which part of the building is considered. Safeguards in this area are listed below.

- Material Protection
  Physical safeguards to protect a building include fences, physical access control, strong walls, doors, and windows. Secure areas within a building should be protected from unauthorized access by physical access controls, guards, etc. Secure areas might be necessary for ICT equipment, such as servers, and associated software and data, supporting important business activities. Access to such secure areas should be limited to the minimum number of personnel necessary, and details recorded in a log. All diagnostic and control equipment should be securely stored and the use should be strictly controlled.
- Fire Protection
  Equipment and surrounding areas, including access to them, should be protected against the spread of fire from elsewhere in the building or adjacent buildings. Fire hazards in the vicinity of rooms/areas containing equipment should be minimized. There also should be protection against fires starting within and/or affecting all rooms/areas containing key equipment. Safeguards should include fire and smoke detection, alarms and suppression. Care should be taken that the fire protection does not lead to damage of ICT systems from water or other extinguishing means.
- Water/Liquid Protection
  Essential facilities should not be sited in any area where serious flooding or water, or other liquid, leakage is likely to occur. Appropriate protection should be provided where a significant threat of flooding exists.
- Natural Disaster Protection
  Buildings containing key equipment should be protected against the effects of lightning. Also, the key equipment itself should be protected against the effects of lightning. Protection against other natural disasters can be achieved by avoiding areas where these are likely to happen (if possible) and by having business continuity strategy and planning in place.
- Protection against Theft

equipment or media leaving rooms/areas or the building without authorization. Sensitive information and proprietary software held on portable media (e.g. floppy discs) should be protected appropriately.

- Power and Air-conditioning
  All ICT equipment should be protected from power failures, if necessary. A suitable power supply should be provided, and an uninterruptible power supply should be introduced, if necessary. Another aim of protection should be to ensure admissible temperature and humidity.
- Cabling
  Power and communication cabling carrying data or supporting ICT services should be protected from interception, damage and overloading. Cabling should be physically protected against accidental or deliberate damage, and selected and laid appropriate for its purpose; careful planning taking into account future developments can avoid a lot of problems. Wherever justified and possible, cables should be protected against wiretapping.

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommend-ations for computer workstations	Canadian Handbook on Information Technology Security
1. Corporate IT Security Policy	3.1	--	1.1, 1.2	5.1	*.3.1.1	3	--	5.1, 5.2
2. IT System Security Policy	--	--	1.1, 1.2	5.2, 5.3	*.3.1.1	3	--	5.2, 5.3
3. IT Security Management	4.1.1, 4.1.2	--	1.1, 1.2	6	*.3.1.1	4	2.1	6
4. Allocation of Responsibilities	4.1.3	--	1.3	2.4, 2.5, 3	*.3.1.1	4	2.1	2.4, 2.5, 3
5. Organization of IT Security	4.1	--	1.2	3.5	--	4	2.2	3.5
6. Asset Identification and Valuation	5	--	2.2	7.1	--	5.6, 7.1	5.1	7.1
7. Approval of IT Systems	4.1.4	--	--	8	5	--	6.7	8, 9

* stands for any number between 6 and 11.

Table G-1 – ICT security management and policies

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Compliance with IT Security Policies and Safeguards	12.2	--	1.2	10.2.3	--	10.2	7.1, 7.2	9.4, 10.2.3
2. Compliance with Legal and Regulatory Requirements	12.1	--	3.1, 3.2	6.3, 10.2.3	6.3.11	8.18, 10.2	8.1	1.5, 2.9, 6.3, 10.2.3

Table G-2 – Security compliance checking

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Reporting of Security Incidents	6.3.1	--	M2	12	--	10.4	--	12
2. Reporting of Security Weaknesses	6.3.2	--	M2	12	--	10.4	--	12
3. Reporting of Software Malfunctions	6.3.3	--	M2	12	--	10.4	--	12
4. Incident Management	8.1.3	--	M2	12	--	10.4	--	18.1.3

Table G-3 – Incident management

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Safeguards for Permanent and Temporary Staff	6.1	--	3.2, M3	10.1	*.3.9	9.2	4.1, 2.2	10.1
2. Safeguards for Contracted Personnel	6.1	--	--	10.3	*.3.9	9.2	4.1, 2.2	10.3
3. Security Awareness and Training	6.2	--	1.2, M3	13, 10.1.4	*.3.9	9.1	4.2, 2.2	13, 10.1.4
4. Disciplinary Process	6.3.4	--	3.2, M3	--	*.3.9	9.2.6	2.2.1	13.1

[1] * stands for any number between 6 and 11.

Table G-4 - Personnel

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Configuration and Change Management	8.2, 10.5	--	--	14.3, 8.4.1	--	7.4	9	14.3, 8.4.1, 8.4.4
2. Capacity Management	8.2.1	--	--	--	--	--	--	--
3. Documentation	8.1.1, 8.6.3	--	M2	14.6	--	8.4.6, 8.5.7, 8.7	--	14.6
4. Maintenance	7.2.4	--	M2	14.7	*.3.6	8.1.4, 8.10,5, 10.1	6.5	14.7
5. Monitoring Security Relevant Changes	--	--	1.2	7.3.3	--	7.4, 8.1.3, 8.2.5, 8.3.7	6.7	7.3.3, 8.4.4
6. Audit Trails and Logging	8.4	--	M2	18	--	7.3, 8.1.8, 8.2.10, 8.9.5	6.7	(18)
7. Security Testing	--	--	M2	8.4.3	--	8.3.5	6.7, 3	8.4.3
8. Media Controls	8.6	--	8, M2	14.5	*.3.5	8.4 – 8.14	5	14.5
9. Assured Storage Deletion	--	--	M4	--	--	8.1.9	6.3, 5	14.5.7
10. Segregation of Duties	8.1.4	--	M2	--	--	--	--	10.1.1
11. Correct Software Use	12.1.2	--	M2	--	*.3.8	8.3	6.3	14.2
12. Software Change Control	10.5.1, 10.5.3	--	M2	--	*.3.8	8.3.7	6.3	8.4.4, 14.2

* stands for any number between 6 and 11.

Table G-5 – Operational issues

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Business Continuity Strategy	11.1.1, 11.1.2	--	3.3, M6	11.2, 11.3, 11.4	*.3.3	8.19, 8.1.7, 8.4.5, 8.5.5, 8.6.5, 8.7.5, 8.8.3, 8.19 8.19	7.3, 7.4, 7.5	11.2, 11.3, 11.4
2. Business Continuity Plan	11.1.3, 11.1.4	--	3.3, M6	11.5	*.3.3		--	11.5
3. Testing and Updating the Business Continuity Plan	11.1.5	--	3.3, M6	11.6	*.3.3		--	11.6
4. Back-ups	8.4.1	--	3.4	14.4	*.3.2.4	--	7.1, 7.2	14.4

[1] * stands for any number between 6 and 11.

Table G-6 – Business continuity planning

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Material Protection	7.1	--	4.1, 4.3, M1	15.1	*.3.1.2	8.1.1, 8.6.2, 8.9.1	3.1, 3.4, 4	15.1
2. Fire Protection	7.2.1	--	--	15.2	*.3.1.4	8.1.1, 8.6.2, 8.9.1	3.1, 3.2, 7.5	15.2
3. Water/Liquid Protection	7.2.1	--	M2	15.5	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.5
4. Natural Disaster Protection	7.2.1	--	M2	15.4	*.3.1.4	8.1.1, 8.6.2, 8.9.1	7.5	15.4
5. Protection against Theft	7.1	--	1.2	15.1	*.3.1.3	8.1.1, 8.6.2, 8.9.1	3.3, 3.4, 4	15.1
6. Power and Air-conditioning	7.2.2	--	M2	15.6	*.3.4	8.1.1, 8.6.2, 8.9.1	3.2, 7.3	15.6
7. Cabling	7.2.3	--	4.2, M1	--	--	8.1.1, 8.6.2, 8.9.1	8.2	15, 15.1, 15.7

[1] * stands for any number between 6 and 11.

Table G-7 – Physical security

ICT System Specific Safeguards

At the end of this clause tables relating to each subsection show where to find additional information about the safeguard categories mentioned.

Identification and Authentication (I&A)

Identification is the means by which a user provides a claimed identity to a system. Authentication is the means of establishing the validity of this claim. The following ways are examples of how to achieve I&A (other ways of classifying I&A mechanisms are possible).

- I&A Based on Something the User Knows
  Passwords are the most typical way to provide I&A based on something the user knows linked with a user identification process. The allocation of passwords and their regular change should be controlled. If users are choosing the passwords themselves, they should be aware of the common rules for password design and handling. Software can be used to support this, for example by limiting the use of common passwords or patterns and characters. If it is necessary or wanted, copies of passwords should be stored securely to allow authorized access if the user is not available or has forgotten the password. I&A based on something the user knows can also make use of cryptographic means and authentication protocols. This type of identification and authentication can also be used for remote I&A.
- I&A Based on Something the User Possesses
  Objects that users possess for the purpose of I&A can be memory tokens (e.g., magnetic stripe cards) and smart tokens (e.g., smart cards, USBs, PC cards). Authentication is provided based on something the user possesses (the token) and something the user knows (the PIN).
- I&A Based on Something the User Is
  Biometric authentication technologies use the unique characteristics or attributes of an individual to authenticate the person’s identity. These characteristics could be fingerprints, hand geometry, retina pattern, voice pattern and hand-written signatures. Relevant details can be securely stored on smart cards, or a system.

Logical Access Control and Audit

Safeguards in this area are implemented to

- restrict access to information, computers, networks, applications, system resources, files and programs, and
- record details of error and user actions in audit trails and analyse the details recorded, in order to detect and handle security breaches in an appropriate manner.

A common means to enforce access control is to use the I&A details linked to access control lists defining what files, resources, etc. a user is permitted to access, and what form that access can take. Safeguards in the area of logical access control and audit are listed below.

- Access Control Policy
  For each user or group of users, there should be a clearly defined access control policy. This policy should grant access rights according to the business requirements, such as availability, productivity and the 'need to know' principle. The general idea should be: 'as many rights as necessary, as few rights as possible'. The allocation of access rights should take into account the organization’s approach to security (for example, open or restrictive)

and culture to fulfill business needs and gain user acceptance.

- User Access to Computers
  Access control to computers is applied to prevent any unauthorized access to a computer. It should be possible to identify and verify the identity of each authorized user, with both successful and unsuccessful attempts logged. Computer access control can be aided by passwords, or by any other I&A method.
- User Access to Data, Services and Applications
  Access control should be applied to protect the data and services on a computer or within a network from unauthorized access. This can be done with help of appropriate I&A mechanisms (see Clause 8.2.1 above), the appropriate interfaces between networked services, and the configuration of the network which ensures that only authorized access to ICT services can take place (restrictive allocation of rights). To prevent unauthorized access to applications, role-based access control that allows access according to the business functions of the users, should be introduced.
- Reviewing and Updating Access Rights
  All access rights given to users should be reviewed regularly and updated if the security or business needs for access have changed. Privileged access rights should be reviewed more frequently to ensure that they are not misused. Access rights should be withdrawn immediately if they are no longer necessary.
- Audit Logs
  All work done with ICT support should be logged and these logs should be inspected regularly; this includes successful and unsuccessful attempts to log into a system, logging of access to data, functions of the system used, etc. Faults should also be logged, and these logs should be reviewed regularly. These data should be used in accordance with data protection and privacy legislation, for example, they may only be stored for a restricted duration and only be used for the detection of security violations.

Protection against Malicious Code

Malicious code may be introduced into systems through external connections and through files and software introduced from portable disks. Malicious code may not be detected before damage is done unless suitable safeguards are implemented. Malicious code may result in compromise of security safeguards (e.g. capture and disclosure of passwords), unintended disclosure of information, unintended changes to information, loss of system integrity, destruction of information, and/or unauthorised use of system resources.

Malicious code is normally one of three types: viruses, worms, and Trojan horses.

Malicious code carriers are:

- executable software,
- data files (containing executable macros, e.g. word processing documents or spreadsheets),
- active contents of World Wide Web pages.

Malicious code can propagate via:

- floppy discs,

- other removable media,
- electronic mail,
- networks,
- downloads.

Malicious code may be introduced as a result of a deliberate action by a user, or by system level interactions that may not be visible to users. Protection against malicious code can be achieved by the use of the safeguards listed below.

- Scanners
  Different forms of malicious code can be detected and removed by special scanning software and integrity checkers. Scanners can work in off-line or on-line modes. On-line operation of a scanner provides active protection, i.e. detection (and possible removal) of malicious code before any infection takes place and damage is done to the ICT system. Scanners are available for stand-alone computers, workstations, file servers, electronic mail servers and firewalls. However, users and administrators should be made aware that scanners cannot be relied upon to detect all malicious code (or even all malicious code of a particular type) because new forms of malicious code are continually arising.
- Integrity Checkers
  Typically, other forms of safeguard are required to augment the protection provided by scanners. For example, checksums can be used to check whether a program has been modified. Integrity checking software should be an integral part of technical safeguards providing protection against malicious code. This technique can only be used for data files and programs that do not keep status information for further use.
- Removable Media Circulation Control
  Uncontrolled circulation of media (especially floppy discs) can lead to an increased risk of introducing malicious code to an organization’s ICT systems. Control of circulation of media can be achieved by the use of special software or procedural safeguards.
- Procedural Safeguards
  Guidelines for users and administrators should be developed outlining procedures and practices to minimise the possibility for introducing malicious code. Such guidelines should cover loading games and other executable software, use of various types of Internet services, and importing files of varying types. Independent reviews of source or executable code should be made when necessary. Security awareness training and disciplinary actions and related procedures should be in place for not following the documented malicious code prevention procedures and practices.

Network Management

This area includes topics of planning, operation and administration of networks. The proper configuration and administration of networks is an effective means to reduce risks. ISO is currently working on several documents containing further information about detailed safeguards for network security. Safeguards in the area of network management are listed below.

- Operational Procedures
  The establishment of operational procedures and responsibilities is necessary to ensure the correct and secure operation of networks. This includes the documentation of the operating procedures and the establishment of procedures to react to incidents.

- System Planning
  In order to ensure reliable functioning and adequate network capacity, advanced planning and preparation, and monitoring (including of loading statistics) is necessary. Acceptance criteria for new systems should be applied and changes should be controlled.
- Network Configuration
  An appropriate network configuration is essential for its reliable functioning. This includes a standardized approach for the configuration of servers throughout the organization, and, very important, good documentation. Furthermore, it should be ensured that servers used for special purposes are only used for these purposes (e.g. no other tasks should run on a firewall), and that sufficient protection from failure is in place.
- Network Segregation
  In order to minimize the risks and the possibilities of misuse in a network in operation, business areas dealing with critical business issues and information should be kept separate, logically or physically. As well, development facilities should be separated from operational facilities.
- Network Monitoring
  Network monitoring should be used to identify the weaknesses within the existing network configuration. It allows for reconfiguration caused by traffic analysis and helps to identify attackers.
- Intrusion Detection
  Attempts to gain entry to systems or networks and successful unauthorized entry should be detected so that the organization can respond in an appropriate and effective manner.

Cryptography

Cryptography is a mathematical means of transforming data to provide security. It can be used for many different purposes in ICT security; for example, cryptography can help to provide confidentiality and/or integrity of data, non-repudiation, and advanced I&A methods. When applying cryptography, care should be taken to comply with all laws and regulations in this area. One of the most important aspects of cryptography is an adequate key management system, which is discussed in more detail in ISO/IEC 11770-1. Further information about classes of cryptographic applications can also be found in Annex C of ISO/IEC 11770-1. Time stamping services can be used to support several applications of cryptographic safeguards. The different ways of using cryptography are discussed below.

- Data Confidentiality Protection
  In circumstances where preservation of confidentiality is important, e.g. where the information is particularly sensitive, safeguards should be considered to encrypt information for storage or communication over networks. The decision to use encryption safeguards should take account of:
    - relevant government laws and regulations,
    - the requirements of key management and the difficulties that need to be overcome to ensure that real security improvements are achieved without creating new vulnerabilities, and
    - the suitability of the encryption mechanisms used for the deployment situation and the degree of protection required.
- Data Integrity Protection

In circumstances where preservation of integrity of stored or processed data is important, hash functions, digital signatures and/or integrity safeguards should be considered to protect stored or communicated information. Integrity safeguards (for example using so called message authentication codes (MACs)) provide protection against accidental or deliberate alteration, addition or deletion of information. Digital signature safeguards can provide similar protection to safeguard message integrity, but also have properties that allow them to enable non-repudiation. The decision to use digital signature or other integrity safeguards should take account of:

- relevant government laws and regulations,
- relevant public key infrastructures,
- the requirements for key management and the difficulties that need to be overcome to ensure that real security improvements are achieved without creating new vulnerabilities.

- Non-Repudiation
  Cryptographic techniques (e.g. based on the use of digital signatures) can be used to prove or otherwise the sending, transmission, submission, delivery, receipt notification, etc. of messages, communications and transactions.
- Data Authenticity
  In situations where the authenticity of data is important a digital signature can be used to attest to the validity of the data. This necessity arises particularly when use is made of reference data from third party sources, or when a large community is dependent upon the reference data to be accurate. Digital signatures can also be used to attest the fact that data is originating from a specific person.
- Key Management
  Key management includes technical, organizational and procedural aspects that are necessary to support the use of any cryptographic mechanism. The objective of key management is the secure administration and management of cryptographic keys and related information. Key management includes the generation, registration, certification, de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material. In addition, it is important to design key management appropriately to reduce the risk of key compromise and use by unauthorized persons. Key management procedures depend on the algorithm used, the intended use of the key and the security policy. For more information on key management, see also ISO/IEC IS 11770-1.

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. I&A Based on Something the User Knows	9.2.3, 9.3.1, 9.4., 9.5.1	4.2.1, 5.2.1, Annex A	M4	16.1	*.3.2.1	7.2.1, 7.2.2	6.2	16.1
2. I&A Based on Something the User Possesses			--	16.2	*.3.2.1		6.2	16.2
3. I&A Based on Something the User Is			--	16.3	*.3.2.1		6.2	16.3

[1] * stands for any number between 6 and 11.

Table G-8 – Identification and authentication (I&A)

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Access Control Policy	9.1	--	M2	17.1, 17.2, 17.3	*.3.2.1	7.2, 8.1.2, 8.2.2, 8.4.1	6.4	17.1, 17.2, 17.3
2. User Access to Computers	9.2, 9.3, 9.5	4.2.4, 5.2.4, Annex A	M4		*.3.2.1		6.2, 3.3	
3. User Access to Data, Services and Applications	9.4, 9.6		M4		*.3.2.1		6.4	
4. Reviewing and Updating Access Rights	9.1, 9.2.4	--	M2	17.4	*.3.2.1		--	17.4
5. Audit Logs	9.7	--	M4	18	*.3.2.2	7.3, 8.2.10	6.7	18

[1] * stands for any number between 6 and 11.

Table G-9 – Logical access control and audit

Table G-xy3 - Protection against Malicious Code

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Scanners	8.3	--	M4	--	*.3.10	8.3.11, 8.3.16	7.4	4.6, 5.2.1, 6.4, 8.4.4, 11
2. Integrity Checkers	8.3	--	M4	--	--	8.3.11, 8.3.16	7.4	--
3. Removable Media Circulation Control	7.3.2	--	--	--	--	--	--	--
4. Procedural Safeguards	8.3	--	M4	--	*.3.10	8.3.11, 8.3.16	7.4	6.2.2, 9.3, 12, 14.2

[1] * stands for any number between 6 and 11.

Table G-10 – Protection against malicious code

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommen-dations for computer workstations	Canadian Handbook on Information Technology Security
1. Operational Procedures	8.5.1	--	M2	--	--	8.2, 8.3	8.2	14.6
2. System Planning	8.2	--	M2, M4	8.4	--		6.1	8.4
3. Network Configuration	--	--	M4	--	--		9, 6.1	14.3
4. Network Segregation	9.4.6	--	M2	--	--	--	3.1	--
5. Network Monitoring	9.7	--	M2	18.1.3	--	8.2.7	--	18.1.3
6. Intrusion Detection	--	--	--	18.1.3	--	--	6	18.1.3

[1] * stands for any number between 6 and 11.

Table G-11 – Network management

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categorization and Protection for Healthcare Information Systems[1]	TC 68 Information Security Guidelines	Recommend-ations for computer workstations	Canadian Handbook on Information Technology Security
1. Data Confidentiality Protection	10.3.2	4.2.2, 5.2.2, Annex A	M4	19.5.1	--	8.23	8.1	19.5.1
2. Data Integrity Protection	10.3.3	4.2.3, 5.2.3, Annex A	M4	19.5.2	--	8.23	8.1	19.5.2
3. Non-Repudiation	10.3.4	4.2.6, 5.2.6, Annex A	--	19.2.3	--	8.23	8.1	19.2.3
4. Data Authenticity	10.3.2	4.2.3, 5.2.3, Annex A	M4	19.5.2	--	8.23	8.1	19.5.2
5. Key Management	10.3.5	4.2.5, 5.2.5, Annex A	--	19.3	--	8.23	8.1	19.3

Table G-12 - Cryptography

[9 Baseline Approach: Selection of Safeguards According to the Type of IT System]

Baseline Approach: Selection of Safeguards According to the Type of ICT System

Generally Applicable Safeguards

Generally applicable safeguard categories are:

- ICT security management and policies (ref. x),
- Security compliance checking (ref. x),
- Incident management (ref. x),
- Personnel (ref. x),
- Operational issues (ref. x),
- Business continuity planning (ref. x), and
- Physical security (ref. x).

The safeguards of these categories form the basis for successful ICT security management, and should not be underestimated. It is also important to ensure the interworking of these safeguards with the more technical ones considered below. How much an organization decides to do in these areas depends on its needs and concerns, and the resources available.

Of course, many of the other safeguard categories are also applicable in most cases, but the manner of implementation is usually specific to the particular circumstances (for example, safeguards providing access control for a network are different from safeguards providing access control for a stand alone computer).

When selecting safeguards from the generally applicable safeguard categories, it is helpful to consider the size of the organization as well as the security needs, since this influences the extent to which these safeguards are implemented. For example, a small organization will neither have the need nor the personnel to establish an ICT security committee, but, nevertheless, somebody fulfilling the functions should be in place. Hence, all safeguards listed in 8.1 should be scaled appropriately whenever necessary.

ICT system specific safeguards

In addition to generally applicable safeguards, ICT system specific safeguards should be selected for each relevant type of system component. The following table gives an example of how to start the process of selection of ICT system specific safeguards. In this example, ‘X’ refers to safeguards that should be implemented under normal circumstances and ‘(X)’ notes safeguards that might be necessary in some circumstances. The safeguard selection process would be continued by considering the safeguard descriptions presented above, and, as necessary, further information obtained from the baseline safeguard documents listed in Annexes G-A to G-H.

	Stand-alone Workstation	Workstation (Client without Shared Resources) Connected to a Network	Server or Workstation with Shared Resources Connected to a Network
I&A			
I&A Based on Something the User Knows	X	X	X
I&A Based on Something the User Possesses	X	X	X
I&A Based on Something the User Is	(X)	(X)	(X)
Logical Access Control and Audit			
Access Control Policy			X
User Access to Computers	X	X	X
User Access to Data, Services and Applications	X	X	X
Reviewing and Updating Access Rights			X
Audit Logs	X	X	X
Malicious code			
Scanners	X	X	X
Integrity Checkers	X	X	X
Removable Media Circulation Control	X	X	X
Procedural Safeguards	X	X	X
Network Management			
Operational Procedures			X
System Planning			X
Network Configuration			X
Network Segregation			X
Network Monitoring			X
Intrusion Detection			X
Cryptography			
Data Confidentiality Protection	(X)	(X)	(X)
Data Integrity Protection	(X)	(X)	(X)
Non-Repudiation		(X)	(X)
Data Authenticity	(X)	(X)	(X)
Key Management	(X)	(X)	(X)

Table G-13 – ICT system specific safeguards

Selection of Safeguards According to Security Concerns and Threats

The selection of safeguards 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 safeguards selected should be appropriate to the assessed security concerns. Second, for each of the security concerns, typical threats are listed and for each threat, safeguards are suggested according to the ICT system considered. The different types of ICT systems are introduced above and an overview of possible safeguards 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 safeguards 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, safeguards 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 safeguards 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 safeguards.

Security concerns can be assessed by considering whether the impact of a failure or breach in security could cause serious damage to business operations, or minor or no damage. For example, if company-confidential information is processed on an ICT system, the unauthorised 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, unauthorised 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 safeguards additional to the ones suggested below should be selected.

Loss of confidentiality
Consider what damage could arise 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, and
- financial loss.

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

Loss of integrity
Consider what damage could arise 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.

According to the answers to the questions above, it should be decided whether the overall damage that could result from a loss of integrity would be serious, minor or none. This decision should be documented.

Loss of availability
Consider what damage could arise 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 also be considered. 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 damage 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 all damages that might occur in such different time periods, and assess the damage for each time period as serious, minor or none (this information should be used in the safeguard selection).

According to the answers to the questions above, it should be decided whether the overall damage that could result from a loss of availability would be serious, minor or none. This decision should be documented.

Loss of accountability
Consider what damage could arise from the loss of accountability of users of systems or subjects (e.g. software) acting on the behalf of the user. This consideration should also 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.

According to the answers to the questions above, it should be decided whether the overall damage that could result from a loss of accountability would be serious, minor or none. This decision should be documented.

Loss of authenticity
Consider what damage could arise 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.

According to the answers to the questions above, it should be decided whether the overall damage that could result from a loss of authenticity would be serious, minor or none. This decision should be documented.

Loss of reliability
Consider what damage could arise from the loss of reliability of systems. This is also important to address functionality that is a sub-characteristic of reliability (see ISO 9126). 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.

According to the answers to the questions above, it should be decided whether the overall damage that could result from a loss of reliability would be serious, minor or none. This decision should be documented.

Safeguards for Confidentiality
The threat types that might endanger confidentiality are listed below, with safeguards to protect against these threats suggested. References to the safeguards described in Clause 8 are given. If relevant for the safeguard selection, the type and characteristics of the ICT system should be taken into account.

It should be noted that most of the safeguards listed in Clause 8.1 provide a more 'general' protection, i.e. they are aimed at a range of threats and provide protection by supporting an overall effective ICT 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. Safeguards against that are listed below.

- Physical Safeguards: 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.

- ICT 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. Safeguards against electromagnetic radiation are listed below.

- Physical safeguards: These can be cladding for rooms, walls etc, and these safeguards 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. Safeguards 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 confidentiality problems whenever this masquerade allows access to sensitive information. Safeguards in this area are listed below.

- I&A: Masquerade becomes more difficult if I&A safeguards 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 is currently working on several documents containing

further information about detailed safeguards 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. Safeguards against that are listed below.

- Network management: Safeguards to protect against misrouting and re-routing can be found in other documents ISO is currently developing containing further information about detailed safeguards 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. Safeguards 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. Safeguards against theft are listed below.

- Physical safeguards: This can be material protection making access to the building, area or room containing the ICT equipment more difficult, or specific safeguards against theft.
- Personnel: Safeguards for personnel (controlling outside personnel, confidentiality agreements, etc.) should be in place making theft difficult.
- Data confidentiality protection: This safeguard 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. Safeguards 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 safeguards 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. Safeguards 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.

<u>Safeguards for Integrity</u>

The threat types that might endanger integrity are listed below, with safeguards to protect against these threats suggested. If relevant for the safeguard 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 safeguards 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. Safeguards 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. Safeguards against that are listed below.

- Protection against malicious code: For a detailed description of malicious code protection, reference Clause x.
- 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. Safeguards in this area are listed below.

- I & A: Masquerade becomes more difficult if I & A safeguards 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 is currently working on several documents containing further information about detailed safeguards 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. Safeguards against that are listed below.

- Network management: Safeguards to protect against misrouting and re-routing can be found in other documents ISO is currently developing containing further information about detailed safeguards 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

Safeguards 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 safeguards 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. Safeguards 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. Safeguards against those specific problems can be found in the respective subsections; safeguards against supply failures are listed below.

- Power and air conditioning: Suitable power supply and air conditioning related safeguards, 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. Safeguards 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 minimise the risks of technical failures.
- Power and air conditioning: Suitable power supply and air conditioning related safeguards, 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. Safeguards 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 is currently working on several documents containing further information about detailed safeguards 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. Safeguards 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 safeguards should be used in combination with logical access control to prevent unauthorized access.
- Logical access control and audit: Safeguards 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). Safeguards 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 safeguards 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. Safeguards 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. Safeguards 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.

Safeguards for Availability

The threat types that might endanger availability are listed below, with safeguards to protect against these threats suggested. References to the safeguards described in Clause 8 are given. If relevant for the safeguard selection, the type and characteristics of the ICT system should be taken into account.

It should be noted that most of the safeguards discussed provide a more 'general' protection, i.e. they are not aiming at specific threats but provide protection by supporting an overall effective ICT 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. Safeguards 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 safeguards 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 safeguards 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. Safeguards to protect the availability are listed below.

- Redundancy and Back-ups: Redundant implementation of communication services components can be used to lower the probability of communication services failures. Depending on the maximal acceptable downtime, standby equipment may also be used 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: ISO is currently working on several documents containing further information about detailed safeguards 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. Safeguards 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. Safeguards 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. Safeguards 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. Safeguards in this area are listed below.

- I & A: Masquerade becomes more difficult if I & A safeguards 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 is currently working on several documents containing further information about detailed safeguards for network security.
- Data back-up: Data back-up cannot protect against masquerading of user identity but reduces the impact 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. Safeguards against that are listed below.

- Network management: Safeguards to protect against misrouting and re-routing can be found in other documents ISO is currently developing containing further information about detailed safeguards 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. Safeguards 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 safeguards should be used in combination with logical access control to prevent unauthorized access.
- Logical access control and audit: Safeguards 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 safeguards 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. Safeguards 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. Safeguards against those specific problems can be found in the respective subsections; safeguards against supply failures are listed below.

- Power and air conditioning: Suitable power supply and air conditioning related safeguards, 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. Safeguards 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 minimise 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. Safeguards against theft are listed below.

- Physical safeguards: This can be material protection making access to the building, area or room containing the ICT equipment and information more difficult, or specific safeguards against theft.
- Personnel: Safeguards 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. Safeguards to protect the availability are listed below.

- Redundancy and Back-ups: Redundant implementation of communication services components can be used to lower the probability of traffic overloading. Depending on the maximal acceptable downtime, standby equipment may also be used 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 is currently developing documents containing further information about detailed safeguards for network security that can be applied to protect against traffic overloading.

Transmission errors
Transmission errors can destroy the availability of the information transmitted. Safeguards 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 is currently developing documents containing further information about detailed safeguards 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. Safeguards 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 safeguards should be used in combination with logical access control to prevent unauthorized access.
- Logical access control and audit: Safeguards 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). Safeguards 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 authorization 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 safeguards 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. Safeguards 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. Safeguards 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.

Safeguards 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 safeguards may be applicable. Therefore, only general guidance can be given below.

The safeguards 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 ICT 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 safeguards can be used to, or can contribute to, enforcing accountability. Safeguards 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 safeguards 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 safeguards can be used to, or can contribute to, enforcing authenticity. Safeguards 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 safeguards 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 safeguards can be used to, or can contribute to, enforcing reliability. Safeguards 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 safeguards will be dependent upon the specific usage of reliability within the domain.

Selection of Safeguards According to Detailed Assessments

The selection of safeguards according to detailed assessments follows the same principles that are applied in the previous clauses. The performance of a detailed risk analysis allows the special requirements and circumstances of the ICT system and its assets to be taken into account. The difference from high-level assessment is the level of effort, and the detail gathered during the assessment process. A qualified justification of the safeguards selected is therefore possible.

Relation between this Annex and the remainder of ISO/IEC 13335-2

Techniques for the management of ICT security are introduced. Besides other issues, possible corporate risk analysis strategy options and the recommended approach for risk analysis are discussed. The main strategy options to be used within an organization are:

- to use a baseline approach for all ICT systems,
- to use detailed risk analysis for all ICT systems, and
- to use the 'recommended approach', i.e. following a high-level risk analysis of all ICT systems, then a baseline approach for the ICT systems at low risk and a detailed risk analysis for ICT systems at high risk.

If it was decided to use detailed risk analysis for all ICT systems to identify safeguards, information about how to select safeguards and how to use the results of the detailed risk analysis effectively is provided. Nevertheless, the information about safeguards, safeguards for specific ICT systems, and the link between security concerns, threats and safeguards, can still be used.

Principles of Selection

There are basically four aspects that a safeguard can address, i.e. impacts, threats, vulnerabilities, and the risks themselves. A risk itself is addressed when the decision is made to reduce or avoid the risk rather than accept it (an example for reducing a risk is taking out insurance, and an example for avoiding a risk is to move sensitive information to another computer). The components that, all together, make the risks, i.e. the impacts, threats and vulnerabilities, are the main target of safeguards. Ways in which safeguards can address these aspects are:

- threats – safeguards can reduce the likelihood of a threat occurring (for example, consider a threat of loss of data because of user errors, then a training course for the users would reduce the amount of these errors), or, in the case of a deliberate attack, can deter by increasing the technical complexity to achieve a successful attack,

- vulnerability – safeguards can remove a vulnerability, or make it less serious (for example, if an internal network connected to an external network is vulnerable to unauthorised access, the implementation of an appropriate firewall would make the connection less vulnerable, and disconnection removes this vulnerability), or
- impact – safeguards can reduce or avoid the impact (if the adverse impact is the non-availability of information, it is reduced by making a copy of the information that is stored safely elsewhere and having a business continuity plan ready for activation). Having good audit trail recording, analysis and alert facilities can help early incident detection and reduction of the adverse business impact.

How and where a safeguard is used can make a big difference to the benefits gained from its implementation. Very often, threats can exploit more than one vulnerability. Therefore, if a safeguard is used that prevents such a threat occurring, several vulnerabilities may have been addressed at one time. The converse is also true – a safeguard protecting a vulnerability can address several threats. These benefits should be considered when possible in the selection of safeguards. These additional benefits should always be documented to have a full view of the security requirements that any safeguard satisfies.

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

Security should always show reasonable balance in addressing the effects mentioned above. If too much emphasis is placed on one type of safeguard, the overall security is unlikely to be effective. For example, if a majority of deterrence safeguards is used without adequate detection safeguards being in place to identify when deterrence has not worked, the overall security will not be effective. Prior to implementation, the proposed safeguards should be compared with the existing safeguards to assess whether there are any that can be extended or upgraded. If this is the case, then this may be less expensive than introducing new safeguards.

During safeguard selection it is important to weigh the cost of implementation of the safeguards against the value of the assets being protected, and the return on investment in terms of risk reduction. The cost of implementation and maintenance of a safeguard can be much higher than the cost of the safeguard itself, hence they should be taken into account during selection.

Technical constraints such as performance requirements, manageability (operational support requirements) and compatibility issues may hamper the use of certain safeguards. In these instances, the system and security managers should work together to identify optimal solutions. It could also be the case that a safeguard 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.

Aspects such as privacy legislation and jurisprudence may demand that certain safeguards be in place, therefore defining unalterable elements of the baseline used or identified.

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 safeguards forming the different (if necessary) baselines be determined?

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

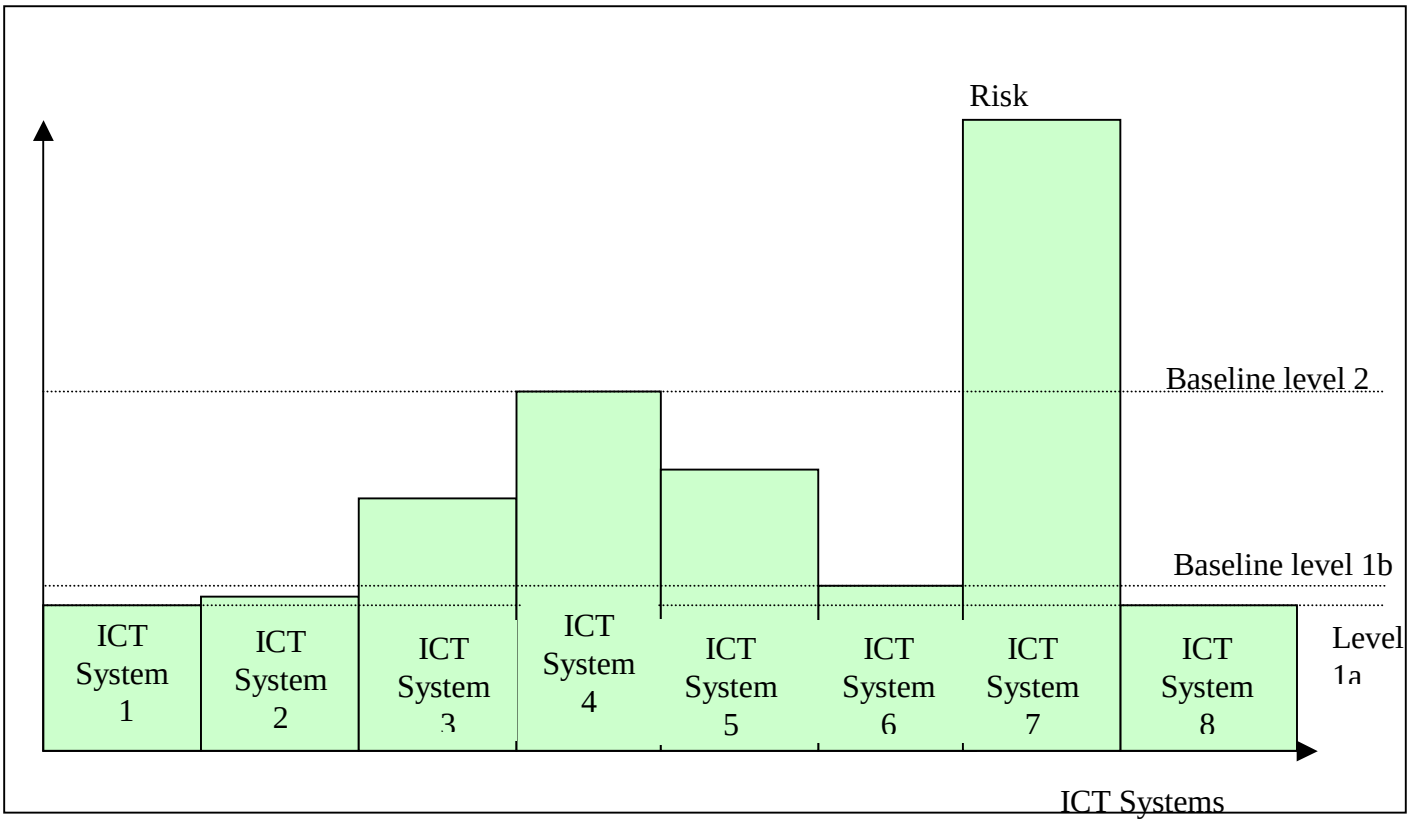

Figure G-x - Different Baseline Levels

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 G-x). If ICT systems with different security requirements are 'really different' (in the sense that most of the safeguards 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 safeguards 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 baseline security should aim at 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 4). It is sensible to aim at a level that is sufficient for most (Baseline level 1a in Figure 4) 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 safeguards 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 safeguards to protect all ICT systems with higher requirements,
- a medium level, adding specific safeguards to protect all ICT systems with higher requirements, or
- a high level, sufficient to protect all ICT 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 ICT systems considered.

Bibliography

[Ed. Note: All of these references need to be updated with specific references.]

[A] Code of Practice for Information Security Management see Annex G-A
[B] ETSI Baseline Security Standard - Features and Mechanisms see Annex G-B
[C] IT Baseline Protection Manual see Annex G-C
[D] NIST Computer Security Handbook see Annex G-D
[E] Medical Informatics: Security Categorization and Protection for Healthcare Information Systems see Annex G-E
[F] TC 68 Banking and Related Financial Services - Information Security Guidelines see Annex G-F
[G] Protection of sensitive information not covered by the Official Secrets Act – Recommendations for computer workstations see Annex G-G
[H] Canadian Handbook on Information Technology Security see Annex G-H

Editors' Note: Annexes need to be updated. Input from the relevant NBs is requested.

Annex G-A Code of Practice for Information Security Management

(Type: generic)
[Ed. Note: To be updated pursuant to publication of ISO/IEC 17799:2000.]
Scope
BS 7799 is issued as a two-part standard

> BS 7799-1: 2000 Code of Practice for Information Security Management;
> BS 7799-2: 2002 Information Security Management Systems -- Specification with Guidance for Use.

These standards are published under the authority of the Standards Board of the British Standards Institution (BSI). BS 7799-1:2000 reproduces verbatim ISO/IEC 17799:2000 and implements it as the UK national standard. BS 7799-1:2000 supersedes the 1999 version, which has now been withdrawn. BS 7799 is intended for use by directors, managers and employees who are responsible for initiating, implementing and maintaining information security in their organization, and may be considered as a basis for developing organizational security standards.

The revised versions of Parts 1 and 2 have been prepared under the supervision of the BSI/DISC committee BDD/2, Information Security Management. These new versions take into account recent developments in the application of information processing technology, particularly in the area of networks and communications. They also give greater emphasis to business involvement in and responsibility for information security. The revision process took account of contributions from organizations from different countries in the world.

These documents provide a comprehensive set of controls comprising best practices in information security and is intended to be as comprehensive as possible. They are intended to serve as a single reference point for identifying the range of controls needed for most situations where information systems are used in industry and commerce, and may therefore be applied by large, medium and small organizations.

Contents of BS 7799-1:2000
1. Scope
2. Terms and definitions
3. Security Policy
    3.1 Information Security Policy
4. Security Organization
    4.1 Information security infrastructure
    4.2 Security of third party access
    4.3 Outsourcing
5. Asset Classification and Control
    5.1 Accountability for assets
    5.2 Information classification
6. Personnel Security

- 6.1 Security in job definition and resourcing
- 6.2 User training
- 6.3 Responding to incidents

7. Physical and Environmental Security
   - 7.1 Secure areas
   - 7.2 Equipment security
   - 7.3 General controls
8. Communications and Operation Management
   - 8.1 Operational procedures and responsibilities
   - 8.2 System planning and acceptance
   - 8.3 Protection against malicious software
   - 8.4 Housekeeping
   - 8.5 Network management
   - 8.6 Media handling and security
   - 8.7 Data and software exchange

9. Access Control
   - 9.1 Business requirements for system access
   - 9.2 User access management
   - 9.3 User responsibilities
   - 9.4 Network access control
   - 9.5 Computer access control
   - 9.6 Application access control
   - 9.7 Monitoring system access and use
   - 9.8 Mobile computing and teleworking
10. System Development and Maintenance
    - 10.1 Security requirements of systems
    - 10.2 Security in application systems
    - 10.3 Cryptographic controls
    - 10.3 Security of application system files
    - 10.4 Security in development and support environments
11. Business Continuity Management
    - 11.1 Aspects of business continuity management
12. Compliance
    - 12.1 Compliance with legal requirements
    - 12.2 Review of security policy and technical compliance
    - 12.3 System audit considerations

Point of Contact
BSI
389 Chiswick High Road
London, W4 4AL
UK
Tel.: +44 181 996 7000
Fax: +44 181 996 7001

BS 7799 is also published in Australia and New Zealand as AS/NZS 4444.

Point of Contact
SAA
P.O.Box 1055
AUS – Strathfield NSW 2135
Australia
Tel.: +61 297 464700
Fax: +61 297 464766

BS 7799 is also published in Sweden as SS 62 77 99.

Point of Contact
STG
S-11289 Stockholm
SWEDEN
Tel.: +46 8136250
Fax: +46 86186128

Annex G-B ETSI Baseline Security Standard Features and Mechanisms

(Type: ICT application specific)

Scope

This document lists all security features and mechanisms that were evaluated and which may be used in ETSI standards. However, this document merely presents guidelines for the selection and application of specific security mechanisms in an annex. If more specific advice is needed, references to relevant sources of information are given. Moreover, the ETSI STAG experts are ready to assist in case of questions and problems. In many cases, the security mechanisms are not officially standardized themselves, but are registered for use. Many of them are not published because of security considerations, but may be used in specific ETSI-applications. Since there is considerable activity in the fields of telecommunication and cryptology, this document is to be revised and updated regularly.

Contents

Point of Contact
ETSI Secretariat
06921 Sophia Antipolis Cedex
France
Tel.: +33 9294 4200
Fax: +33 9365 4716

Annex G-C IT Baseline Protection Manual

(Type: IT system specific)

Scope

It is the aim of IT baseline protection, through the appropriate application of organizational, personnel, infrastructure and technical standard security safeguards, to achieve a security standard for IT systems that is adequate and sufficient as regards medium-level protection requirements and can serve as a basis for IT applications requiring a high degree of protection.

To this end, the IT Baseline Protection Manual recommends countermeasure packages for typical IT configurations, environments and organizational set-ups. For the preparation of this manual, the German Information Security Agency assumed risk assessment estimates on the basis of known threats and vulnerabilities and has developed packages of measures suited for this purpose. Consequently, the users of the IT Baseline Protection Manual do not have to do these involved analyses regarding IT baseline protection over again; they only have to see to it that the recommended safeguards will be consistently and fully implemented.

At the same time, this helps to ensure that IT security as regards medium-level protection requirements can be achieved in a labour-economical way, especially since individual system security policies can refer to the IT Baseline Protection Manual. Thus, IT baseline protection becomes a common basis of agreement on safeguards to meet medium-level protection requirements.

Contents

5. Non-Networked Systems
    - 5.1 DOS PC (single user)
    - 5.2 UNIX systems
    - 5.3 Laptop PC
    - 5.4 DOS PC (several users)
    - 5.5 PC Windows NT
    - 5.6 PC Windows 95
    - 5.99 General non-networked IT system
6. Networked Systems
    - 6.1 Server-based PC network
    - 6.2 UNIX network
    - 6.3 Peer-to-peer network under Windows for Workgroups
    - 6.4 Windows NT network
    - 6.5 Novell Netware 3.x
    - 6.6 Novell Netware 4.x
    - 6.7 Heterogeneous networks
    - 6.8 Network and system management
7. Data Transmission Systems
    - 7.1 Exchange of storage media
    - 7.2 Modem
    - 7.3 Firewall
    - 7.4 Email
    - 7.5 WWW server
8. Telecommunications
    - 8.1 Telecommunications system
    - 8.2 Fax machine
    - 8.3 Answering machine
    - 8.4 LAN connection via ISDN
9. Other IT Components
    - 9.1 Standard software
    - 9.2 Databases
    - 9.3 Teleworking

Safeguard Catalogues
Threat Catalogues
Catalogues of Threat/Safeguard Tables

Standards Body
DIN
Burggrafenstrasse 6
10787 Berlin
Germany
Tel.: +49 30 2601 2652
Fax: +49 30 2601 1723

Point of Contact
BSI
Postfach 20 03 63
53133 Bonn
Germany
Tel.: +49 228 9582 0
Fax: +49 228 9582 400

Annex G-D NIST Computer Security Handbook

(Type: generic)

[Ed. Note: To be updated with specific references to NIST Special Publications.]

Scope

This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.

The handbook provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It does not describe detailed steps necessary to implement a computer security program, provide detailed implementation procedures for security controls, or give guidance for auditing the security of specific systems. General references are provided at the end of each chapter, and references of 'how-to' books and articles are provided at the end of each chapter in Parts II, III, and IV.

The purpose of this handbook is not to specify requirements, rather, to discuss the benefits of various computer security controls and situations in which their application might be appropriate. Some requirements for federal systems are noted in the text. This document provides advice and guidance; no penalties are stipulated.

Contents

V. Example

20. Assessing and Mitigating the Risks to a Hypothetical Computer System

Standards Body

ANSI
11 West 42nd Street
13th floor
USA – New York, N.Y. 10036
USA
Tel.: +1 212 642 4900
Fax: +1 212 840 2298

Point of Contact

Computer systems Laboratory
NIST
Gaithersburg
MD 20899-0001
US

Annex G-E Medical Informatics: Security Categorisation and Protection for Healthcare Information Systems

(Type: IT application specific)

Scope

This European pre-standard specifies a method of categorizing automated healthcare information systems in the context of security. Security has been taken to mean the preservation, to an acceptable level, of data availability, confidentiality, and integrity. For each system category specified a corresponding set of protective requirements is provided which is appropriate to the level of risks inherent in that category.

This European Prestandard applies to all automated information systems which process healthcare data. This includes systems which contribute directly to patient care, for example laboratory test results; but it also includes statistical systems as well as administrative systems which provide operational support for the Healthcare Establishment itself, for example staff payroll, personnel, planning and financial support systems. However, systems where confidentiality is considered to be unimportant, i.e. the information is in the public domain, are not covered by this European Prestandard. The target audiences for this European Prestandard are the consumers/procurers of secure information systems in healthcare and developers/manufacturers of secure information systems in or for healthcare. Implementation of the terms of this European Prestandard is regarded as a responsible management response to the obligations of national and European laws as well as the expectations of the public for a high standard of security of healthcare information.

Contents

Point of Contact
CEN TC 251
Rue de Stassart 36
1050 Brussels
Belgium

Annex G-F TC68 Banking and Related Financial Services - Information Security Guidelines

(Type: IT application specific)
[Ed. Note: To be updated. Reference is ISO TR 13569]
Scope
Financial institutions increasingly rely on Information Technology (IT) for the efficient conduct of business. Management of risk is central to the financial service sector. Financial institutions manage risk through prudent business practice, careful contracting, insurance, and use of appropriate security mechanisms.

There is a need to manage information security within financial institutions in a comprehensive manner. This Technical Report is not intended to provide a generic solution for all situations. Each case must be examined on its own merits and appropriate actions selected. This Technical report is to provide guidance, not solutions.

The objectives of this Technical Report are:

- to present an information security programme structure.
- to present a selection guide to security controls that represent accepted prudent business practice.
- to be consistent with existing standards, as well as emerging work in objective and accreditable security criteria.

This Technical Report is intended for use by financial institutions of all sizes and types that wish to employ a prudent and commercially reasonable information security programme. It is also useful to providers of service to financial institutions. This Technical Report may also serve as a source document for educators and publishers serving the financial industry.

Contents

Point of Contact
Secretariat

Ms. Cynthia Fuller
Accredited Standards Committee X9, Inc.
PO Box 4035
Annapolis, MD 21403 USA
Telephone #: 1-301-879-7988
Fax #: 1-301-879-5124
Email: Isabel.Bailey@X9.org
Web: http://TC68.org

Annex G-G Protection of sensitive information not covered by the Official Secrets Act - Recommendations for computer workstations.

(Type: generic)

Scope

This document recommends all of the measures to be implemented by the various officials of a body in order to ensure the protection of sensitive information not covered by the Official Secrets Act and which is processed, handled or stored by computer means. These recommendations concern in particular:

- software that is expensive or the theft, deterioration or disclosure of which can place the body in difficulty,
- limited circulation or specific confidentiality information which, subject to the obligation of professional secrecy, shall not be disclosed. For information of a higher level of sensitivity like specific secret information, the bodies shall arrange to reinforce the measures recommended in this document.

The bodies shall draw up their internal instructions on the basis of these recommendations.

Contents

Point of Contact
AFNOR
Tour d’ Europe
92049 Paris La Defense Cedex
France
Tel.: +33 1 4291 5555
Fax: +33 1 4291 5656

Annex G-H Canadian Handbook on Information Technology Security

(Type: generic)

Scope

This handbook provides assistance in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. It illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.

The handbook provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It does not describe detailed steps necessary to implement a computer security program, provide detailed implementation procedures for security controls, or give guidance for auditing the security of specific systems. General references are provided at the end of each chapter, and references of 'how-to' books and articles are provided at the end of each chapter in Parts II, III, and IV.

The purpose of this handbook is not to specify requirements, rather, to discuss the benefits of various computer security controls and situations in which their application might be appropriate. Some requirements for federal systems are noted in the text. This document provides advice and guidance; no penalties are stipulated.

Contents

20. Assessing and Mitigating the Risks to a Hypothetical IT System

Standards Body
Standards Council of Canada
270 Albert Street
Suite 200
Ottawa, Ontario K1P 6N7
Canada
Tel.: +1 613 238 3222
Fax: +1 613 995 4564

Point of Contact
Communications Security Establishment
P.O. Box 9703, Terminal
Ottawa, Ontario K1G 3Z4
Canada