TECHNICAL REPORT

ISO/IEC TR 13335-4

First edition
2000-03-01

Information technology — Guidelines for the management of IT Security —

Part 4: Selection of safeguards

Technologies de l'information — Lignes directrices pour la gestion de sécurité IT —

Partie 4: Sélection de sauvegardes

Reference number
ISO/IEC TR 13335-4:2000(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

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 respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

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.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this part of ISO/IEC TR 13335 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 TR 13335-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC TR 13335 consists of the following parts, under the general title *Information technology — Guidelines for the management of IT Security*:

— *Part 1: Concepts and models for IT Security*

— *Part 2: Managing and planning IT Security*

— *Part 3: Techniques for the management of IT Security*

— *Part 4: Selection of safeguards*

— *Part 5: Safeguards for external connections*

Introduction

The purpose of this Technical Report (ISO/IEC TR 13335) is to provide guidance, not solutions, on management aspects of IT security. Those individuals within an organization that are responsible for IT security should be able to adapt the material in this report to meet their specific needs.

The main objectives of this Technical Report are:

- to define and describe the concepts associated with the management of IT security,
- to identify the relationships between the management of IT security and management of IT in general,
- to present several models which can be used to explain IT security, and
- to provide general guidance on the management of IT security.

ISO/IEC TR 13335 is organized into five parts. Part 1 provides an overview of the fundamental concepts and models used to describe the management of IT security. This material is suitable for managers responsible for IT security and for those who are responsible for an organization's overall security programme.

Part 2 describes management and planning aspects. It is relevant to managers with responsibilities relating to an organization's IT systems. They may be:

- IT managers who have responsibility for overseeing the design, implementation, testing, procurement, or operation of IT systems, or
- managers who are responsible for activities that make substantial use of IT systems.

Part 3 describes security techniques relevant to those involved with the management activities during a project life-cycle, such as planning, designing, implementing, testing, acquisition, or operations.

Part 4 provides guidance for the selection of safeguards, and how this can be supported by the use of baseline models and controls. It also describes how this complements the security techniques described in part 3, and how additional assessment methods can be used for the selection of safeguards.

Information technology — Guidelines for the management of IT Security —

Part 4:
Selection of safeguards

1 Scope

This part of ISO/IEC TR 13335 provides guidance on the selection of safeguards, taking into account business needs and security concerns. It describes a process for the selection of safeguards according to security risks and concerns and the specific environment of an organization. It shows how to achieve appropriate protection, and how this can be supported by the application of baseline security. An explanation is provided on how the approach outlined in this part of ISO/IEC TR 13335 supports the techniques for the management of IT security laid out in ISO/IEC TR 13335-3.

2 References

ISO/IEC 13335-1: 1997	Guidelines for the Management of IT Security - Part 1: Concepts and Models
ISO/IEC 13335-2: 1997	Guidelines for the Management of IT Security - Part 2: Managing and Planning IT Security
ISO/IEC 13335-3: 1997	Guidelines for the Management of IT Security - Part 3: Techniques for the Management of IT Security
ISO/IEC 10181-2: 1996	Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework
ISO/IEC 11770-1: 1996	Key Management - Part 1: Framework

3 Terms and definitions

For the purposes of this part of ISO/IEC TR 13335, the terms defined in ISO/IEC TR 13335-1 apply: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, IT security, IT security policy, reliability, residual risk, risk, risk analysis, risk management, safeguard, system integrity, threat, and vulnerability. In addition, the following terms are used:

3.1
authentication
provision of assurance of the claimed identity of an entity (ISO/IEC 10181-2)

3.2
identification
process of uniquely determining the unique identity of an entity

4 Aim

The aim of this part of ISO/IEC TR 13335 is to provide guidance on the selection of safeguards. This guidance is provided for the situations where, for an IT system, a decision is taken to select safeguards:

- according to the type and characteristics of the IT system,
- according to broad assessments of security concerns and threats,
- in accordance with the results of a detailed risk analysis review.

In addition to this guidance, cross references are provided to indicate where safeguard selection can be supported by the use of publicly available manuals containing safeguards.

This part of ISO/IEC TR 13335 also shows how an organization (or part of the organization) - wide baseline security manual can be produced. Detailed network security safeguards are mainly dealt with in the documents referenced in the annexes A - H; ISO is currently developing several other documents on network security.

5 Overview

Clause 6 provides an introduction to safeguard selection and to the concept of baseline security. Clauses 7 to 10 deal with the establishment of baseline security for an IT system. In order to select the appropriate safeguards, it is necessary to make some basic assessments, no matter whether more detailed risk analyses will follow later. These assessments are described in clause 7 which includes the consideration of:

- what type of IT system is involved (e.g. a standalone PC, or connected to a network),
- what are the IT 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 IT system?

Clause 8 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 IT 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 which are referenced in annexes A to H of this document. 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 the type of assessment described in clause 7 is detailed enough for the selection of safeguards, clause 9 provides a list of applicable safeguards for each of the typical IT systems described in 7.1. If safeguards are selected based on the type of IT 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, clause 10 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 relevant threats, and finally the type of IT system is considered. The Figure 1 gives an overview of the ways to select safeguards described in clauses 7, 9, and 10.

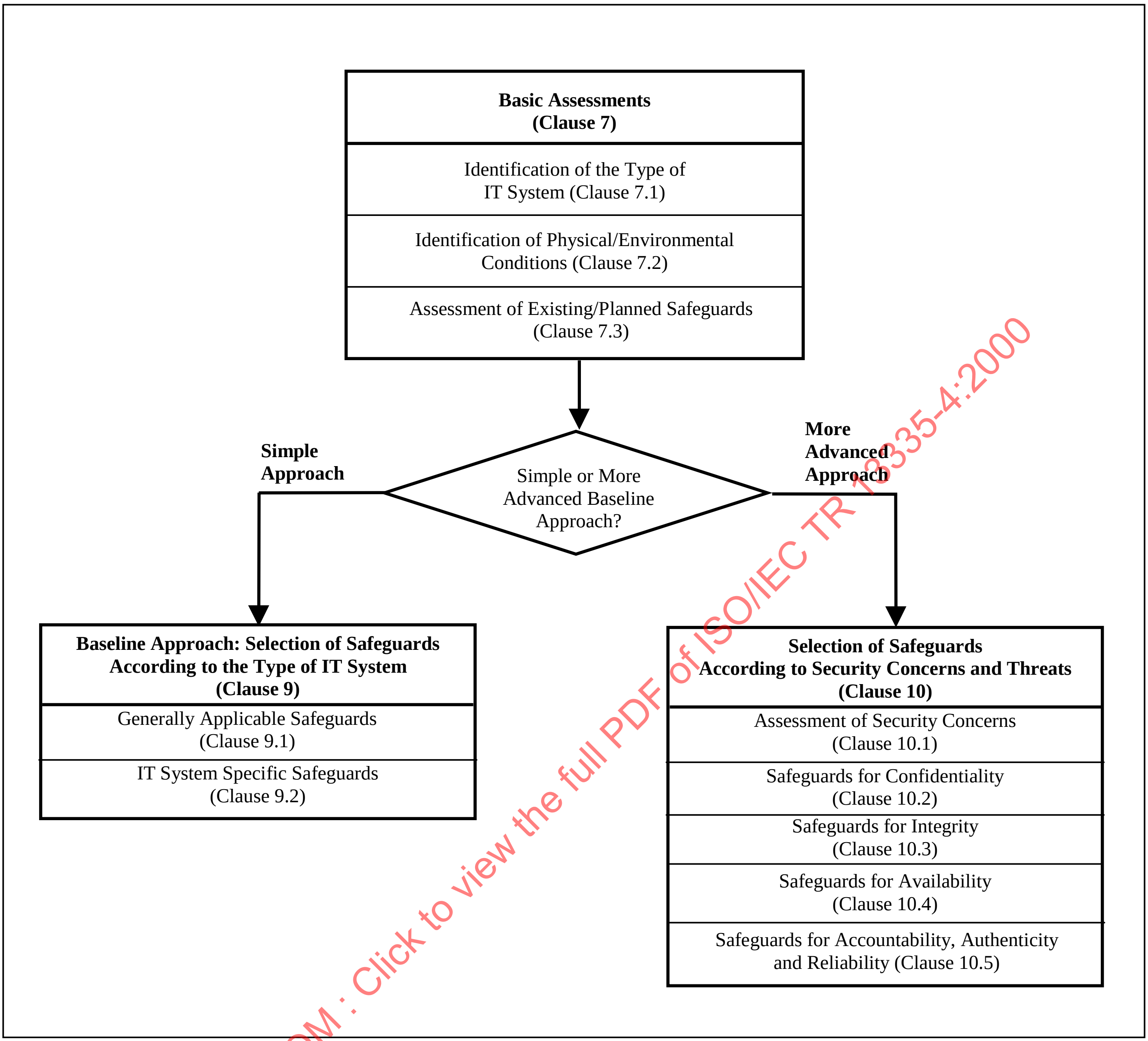
Basic Assessments
(Clause 7)
Identification of the Type of IT System (Clause 7.1)
Identification of Physical/Environmental Conditions (Clause 7.2)
Assessment of Existing/Planned Safeguards (Clause 7.3)
Simple Approach
Simple or More Advanced Baseline Approach?
More Advanced Approach
Baseline Approach: Selection of Safeguards According to the Type of IT System (Clause 9)
Generally Applicable Safeguards (Clause 9.1)
IT System Specific Safeguards (Clause 9.2)
Selection of Safeguards According to Security Concerns and Threats (Clause 10)
Assessment of Security Concerns (Clause 10.1)
Safeguards for Confidentiality (Clause 10.2)
Safeguards for Integrity (Clause 10.3)
Safeguards for Availability (Clause 10.4)
Safeguards for Accountability, Authenticity and Reliability (Clause 10.5)

Figure 1 — Selection of Safeguards According to the Type of IT System or According to Security Concerns and Threats

Clauses 9 and 10 both describe a way to select safeguards from baseline security safeguard documents, which can be applied either for an IT system, or to form a set of safeguards applicable to a range of IT systems in defined circumstances. By focusing on the type of IT system considered, the approach proposed in clause 9 yields the possibility that some risks are not adequately managed, and that some safeguards are selected which are not necessary or not appropriate. The approach suggested in clause 10 to focus on security concerns and associated threats is likely to produce a more optimised set of safeguards. Clauses 9 and 10 can be used to support safeguard selection without more detailed assessments in all instances that fall within the scope of baseline protection. However, if a more detailed assessment, i.e. detailed risk analysis, is used, clauses 9 and 10 can still support the safeguard selection.

Clause 11 deals with the situation where it is decided that detailed risk analysis is necessary because of high security concerns and needs. Guidance on risk analysis is provided in ISO/IEC TR 13335-3. Clause 11 describes the relationships between parts 3 and 4 of ISO/IEC TR 13335 and how the results of the techniques described in part 3 can be used to support safeguard selection. It also describes other 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. The approach considered in clause 11 is different from the approaches described in clauses 9 and 10 in that it gives guidance for selecting a set of safeguards that is optimised to a particular situation. 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.

Clause 12 deals with the establishment of a baseline security manual (or catalogue) for the whole organization or for parts of the organization. For the establishment of a baseline security manual (or catalogue), the safeguards previously identified for IT systems or groups of IT 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 are discussed in order to facilitate a suitable decision for each organization.

Finally, this part of ISO/IEC TR 13335 is summarized in clause 13 and a bibliography and annexes A to H give an overview of the safeguard manuals referenced in clause 8.

6 Introduction to Safeguard Selection and the Concept of Baseline Security

The following clause 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 ISO/IEC TR 13335-3 and is called detailed risk analysis. Part 3 also discusses the advantages and disadvantages of the different approaches to risk analysis, and thus safeguard selection.

Conducting a detailed risk analysis has the advantage that a comprehensive view of the risks is achieved. This can be used to select safeguards which 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 IT 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 IT 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 IT system considered, and
- using a baseline approach where safeguards are recommended according to security concerns and threats, as well as taking into account the IT system considered.

In order to have an overview of the different parallel ways of safeguard selection this document provides, it helps to view Figure 1 as part of a bigger picture (shown in Figure 2) which also gives an idea of the relation between parts 3 and 4 of ISO IEC TR 13335.

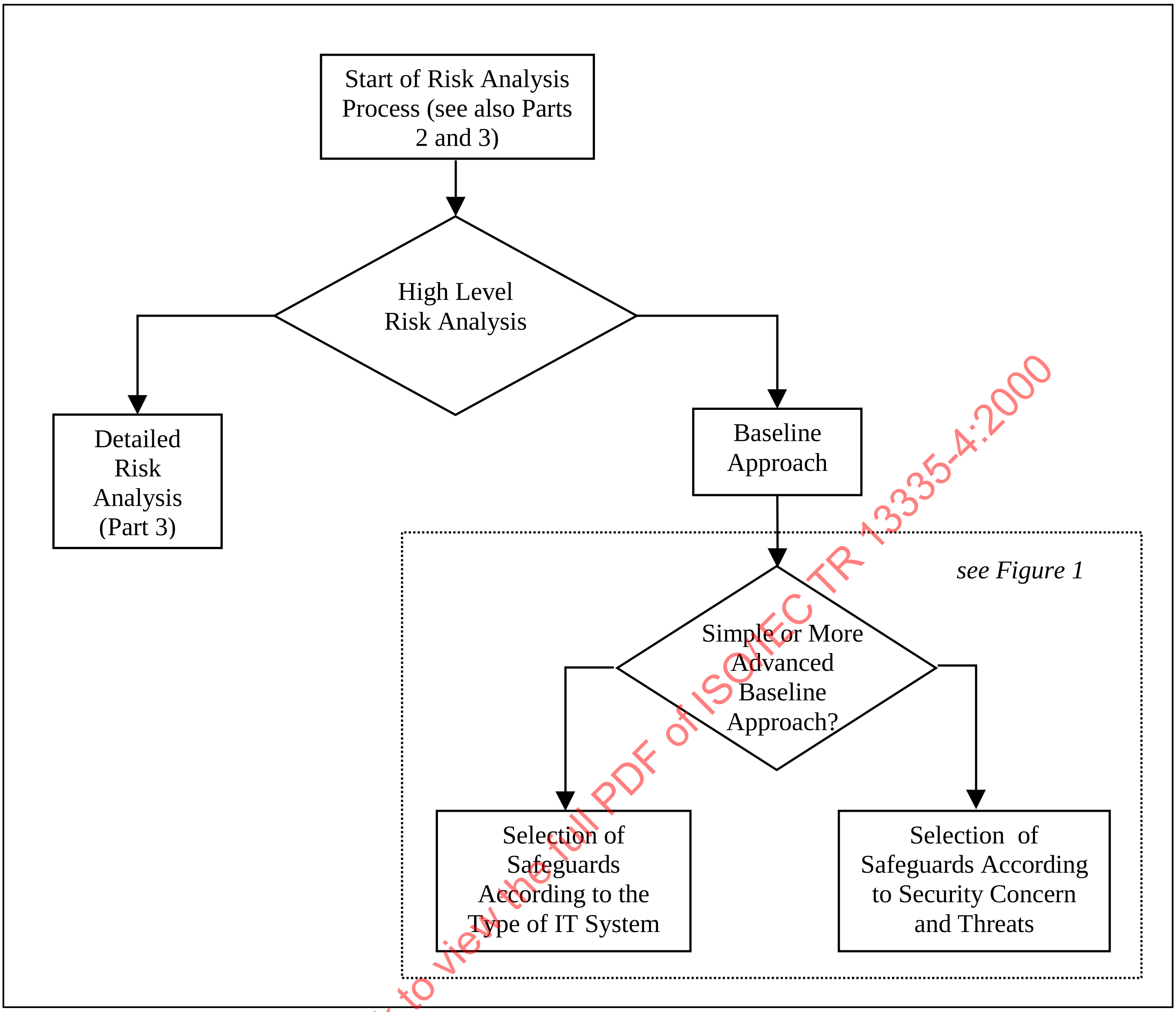
Start of Risk Analysis Process (see also Parts 2 and 3)
High Level Risk Analysis
Detailed Risk Analysis (Part 3)
Baseline Approach
see Figure 1
Simple or More Advanced Baseline Approach?
Selection of Safeguards According to the Type of IT System
Selection of Safeguards According to Security Concern and Threats

Figure 2 — Ways of Safeguard Selection

The baseline approach to be used should be chosen depending on the resources which can be spent on the selection process, the perceived security concerns, and the type and characteristics of the IT 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 IT 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 the safeguards needed to protect the IT system most effectively. If the organization's business operations are heavily dependent on the IT system or service, and/or the information handled is 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 IT 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 IT 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 IT 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 analysis strategy (see ISO/IEC TR 13335-3). 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 IT systems, could be reasons for deciding to follow a baseline approach on its own.

Baseline protection for an IT system can be achieved through the identification and application of a set of relevant safeguards which are appropriate in a variety of low risk circumstances, i.e. they fulfil 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 IT 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) IT systems are very similar in nature and service provided, that safeguards selected through a baseline approach could apply to all IT systems. Figure 3 shows the different ways of using a baseline approach discussed in this part of ISO/IEC TR 13335.

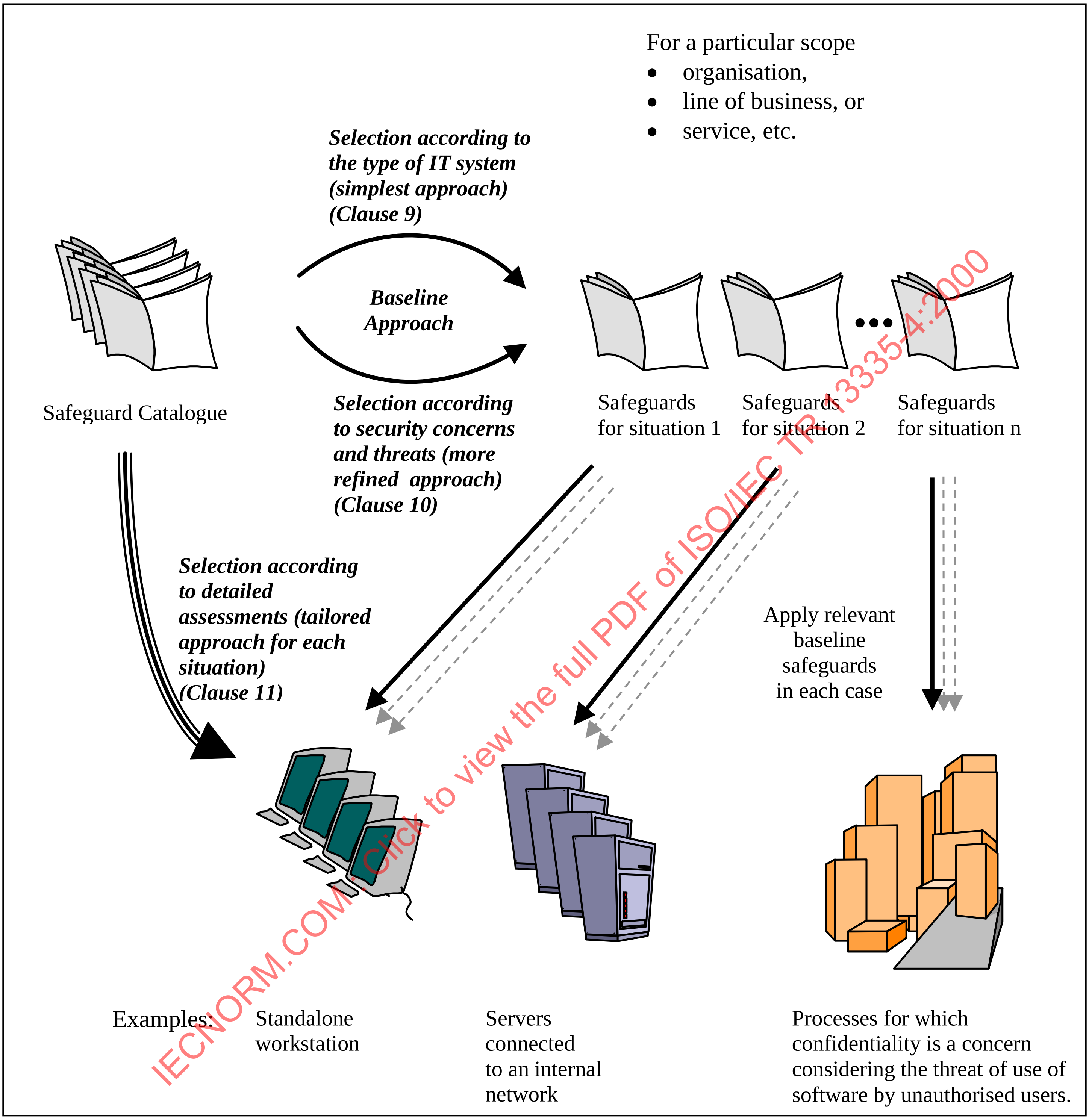
For a particular scope
• organisation,
• line of business, or
• service, etc.
Selection according to the type of IT system (simplest approach) (Clause 9)
Baseline Approach
Selection according to security concerns and threats (more refined approach) (Clause 10)
Safeguard Catalogue
Safeguards for situation 1
Safeguards for situation 2
Safeguards for situation n
Selection according to detailed assessments (tailored approach for each situation) (Clause 11)
Apply relevant baseline safeguards in each case
Examples:
Standalone workstation
Servers connected to an internal network
Processes for which confidentiality is a concern considering the threat of use of software by unauthorised users.

Figure 3 — Approaches to Safeguard Selection

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 lesser 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.

One of the benefits of baseline security is that if it is applied to a group of IT 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.

7 Basic Assessments

The process of safeguard selection always requires some knowledge of the type and characteristic of the IT system considered (for example, a standalone 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 always are 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 (see also ISO/IEC TR 13335-2). Finally, it is necessary to determine whether these assessments provide enough information for the selection of baseline safeguards, or whether a more detailed assessment (as described in clause 10) or a detailed risk analysis (as covered in clause 11) is necessary.

7.1 Identification of the Type of IT System

For the assessment of an existing or planned IT system, the IT system considered should be compared with the following components, and the components representing the system should be identified. In clause 9, safeguards are suggested for each of the components listed below. Components to choose from are:

- standalone workstation,
- workstation (client without shared resources) connected to a network,
- server or workstation with shared resources connected to a network,

7.2 Identification of Physical/Environmental Conditions

The assessment of the environment includes the identification of the physical infrastructure supporting the existing and planned IT 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?
- Access control
  - Who has access to the building?
  - Is there a physical access control system in place?
  - How robust is the structure of the building?
  - How robust are the doors, windows etc. and what protection is afforded to them?
  - Is the building guarded and if so is it for 24 hours per day or only during working hours?

  - Is the building and/or room housing critical IT equipment fitted with intruder alarms?
- Protection in place
  - How is (are) the room(s) containing the IT 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.

7.3 Assessment of Existing/Planned Safeguards

After assessing the physical environment conditions and the components of the IT system, all other safeguards already in place or planned for 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:

- have a look at documents containing information about the safeguards (for example, IT 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. IT system security officer, building manager or operations manager) and the users as to which safeguards are really implemented for the IT 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 other, removing a redundant safeguards might reduce the overall security in place. In addition, it can be cheaper to leave safeguards in place then to remove them, or, especially if the safeguards have high maintenance costs, it can be cheaper to remove them.

8 Safeguards

The following clause 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 and physical safeguards which could be applicable for IT systems are summarized in 8.1. Safeguards specific to an IT system are considered in 8.2. 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 analysis.

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 A to H (for references [A] to [H] see the bibliography at the end of this document) are provided, pointing to where more detailed information can be found about the safeguards mentioned here.

8.1 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.

8.1.1 IT Security Management and Policies

This safeguard category contains all those safeguards dealing with the management of IT 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 in parts 1 to 3 of ISO/IEC TR 13335. 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.

1. Corporate IT 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 IT system security policy documents.
2. IT System Security Policy
   For each IT system, an IT system security policy should be developed which describes the safeguards which 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.
3. IT Security Management
   The management of IT security should be formalized and co-ordinated within the organization in a manner appropriate to its size, for example by establishing an IT security committee and nominating a person (often an IT security officer) being responsible for the security of each IT system.
4. Allocation of Responsibilities
   The responsibilities for organization-wide IT security should be clearly documented and allocated according to the corporate IT security policy and IT system security policies.
5. Organization of IT Security
   All business processes which can support IT security (e.g. procurement, co-operation with other organizations) should be organized to provide that support in a secure manner.
6. Asset Identification and Valuation
   All assets within an organization and for each IT system should be identified, and their value to the conduct of business should be assessed.
7. Approval of IT Systems
   Approval of IT systems should take place according to the IT security policy. The approval process should aim at ascertaining that the safeguards implemented provide an appropriate level of protection. It should taken into account that an IT system might include networks and underlying communications.

8.1.2 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.

1. Compliance with IT Security Policies and Safeguards
   Regular checks should be conducted to ensure that all safeguards that should be in place, as listed in the corporate IT security policy and the relevant IT 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.

2. 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 IT 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 IT systems or cryptography.

8.1.3 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 which makes that possible. Incident handling includes:

1. 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.
2. Reporting of Security Weaknesses
   If users are noting any security relevant weaknesses, they should report them to the person responsible as soon as possible.
3. 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.
4. 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.

8.1.4 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.

1. 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.
2. 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 IT facilities.
3. Security Awareness and Training
   All personnel who use, develop, support and have access to IT 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 IT facilities correctly, to avoid errors. For selected personnel, e.g. IT security officers, security administrators, more specific security training might be necessary.
4. Disciplinary Process
   All employees should be aware of the consequences of an (intentional or unintentional) violation of the organization-wide and specific IT system security policies or any other documented security agreement.

8.1.5 Operational Issues

Safeguards in this area aim at all procedures maintaining the secure, correct and reliable functioning of the IT 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.

1. Configuration and Change Management
   Configuration management is the process of keeping track of changes to IT systems. Its primary security goal is to ensure that changes to IT 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 IT systems.
2. 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 IT system.
3. Documentation
   All aspects of IT configurations and operations should be documented to ensure continuity and consistency. The security of an IT system also needs to be documented in the IT system security policy, security operating procedures document, and business continuity strategy report(s) and plan(s). The documentation should be current and accessible.
4. Maintenance
   IT 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.
5. 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.
6. 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 security relevant events. This includes details of readily identifiable unauthorized or error events and details of 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 events which 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.
7. Security Testing
   Security testing should be used in order to ensure that all IT equipment and all related software components are operating in a secure manner. Security testing should encompass the security requirements defined in the IT system security policy and test plans, and acceptance criteria should be established to demonstrate that the required level of security is achieved.
8. 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.

9. 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 IT security officer) should be available for the users to be used for complete and secure deletion.
10. 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 which, in combination, can lead to the circumvention of safeguards or audits, or to an undue advantage for the employee, should be kept separate.
11. Correct Software Use
    It should be ensured that no copyrighted material is copied, and that the license agreements are obeyed for proprietary software.
12. 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 IT 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.

8.1.6 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 events, an effective business continuity, including contingency planning/disaster recovery, strategy and plan(s) should be in place. This includes the following safeguards.

1. Business Continuity Strategy
   A business continuity, including contingency planning/disaster recovery, strategy should be formulated and documented related to the IT system considered, based on the identified potential adverse business impacts from unavailability, modification and destruction.
2. 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.
3. Testing and Updating the Business Continuity Plan
   Before being accepted, a business continuity plan should be thoroughly tested to ensure that 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.
4. 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.

8.1.7 Physical Security

Safeguards in this area deal with physical protection. They should be considered in combination with the identification of the environment discussed in 7.2. 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.

1. 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 IT 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.
2. 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 IT systems from water or other extinguishing means.
3. 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.
4. 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.
5. Protection against Theft
   To achieve stock control, all items of equipment should be uniquely identifiable and an inventory maintained. Security guards/receptionists should be encouraged to check for 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.
6. Power and Air-conditioning
   All IT equipment should be protected from power failures, if necessary. A suitable power supply should be provided, and an uninterruptable power supply should be introduced, if necessary. Another aim of protection should be to ensure admissible temperature and humidity.
7. Cabling
   Power and communication cabling carrying data or supporting IT 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.

Table 8.1.1 - IT 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	Recommendations 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

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

Table 8.1.2 - 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[1]	TC 68 Information Security Guidelines	Recommendations 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 8.1.3 - Incident Handling

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categori-zation 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 8.1.4 - Personnel

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categori-zation 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	6.3.5	--	3.2, M3	--	*.3.9	9.2.6	2.2.1	13.1

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

Table 8.1.5 - 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 Categori-zation 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

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

Table 8.1.6 - 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 Categori-zation 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 8.1.7 - Physical Security

	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	Recommendations 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.

8.2 IT 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.

8.2.1 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).

1. 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.
2. I&A Based on Something the User Possesses
   Objects that users possess for the purpose of I&A can be memory tokens and smart tokens. A common application of memory tokens is the magnetic material on the back of a credit card. Authentication is provided based on something the user possesses (the card) and something the user knows (the PIN). Typical examples of smart tokens are smart cards.
3. I&A Based on Something the User Is
   Biometric authentication technologies use the unique characteristics or attributes of an individual to authenticate the persons identity. This could be fingerprints, hand geometry, retina pattern, as well as voice patterns or hand-written signatures. Relevant details can be securely stored on smart cards, or a system.

8.2.2 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.

1. 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 fulfil business needs and gain user acceptance.
2. 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.
3. 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 8.2.1), the appropriate interfaces between networked services, and the configuration of the network which ensures that only authorized access to IT 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.
4. 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.
5. Audit Logs
   All work done with IT 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.

8.2.3 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 can be of the following 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.

1. 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 IT 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.
2. 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.
3. 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 IT systems. Control of circulation of media can be achieved by the use of:
   - special software,
   - procedural safeguards (see below).
4. 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 type 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.

8.2.4 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.

1. 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 security relevant incidents (see also 8.1.3).

2. 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 and reacted to (see also 8.1.5).
3. 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.
4. 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.
5. 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.
6. 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.

8.2.5 Cryptography

Cryptography is a mathematical means of transforming data to provide security. It can be used for many different purposes in IT 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. The use of cryptography for I&A is discussed in 8.2.1. Time stamping services can be used to support several applications of cryptographic safeguards. The different ways of using cryptography are discussed below.

1. 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.
2. 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.

3. 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.
4. 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.
5. Key Management
   Key management includes technical, organizational and procedural aspects that is 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.

Table 8.2.1 - 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	Recommendations 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 8.2.2 - Logical Access Control and Audit

	Code of Practice for Information Security Management	ETSI Baseline Security Standard - Features and Mechanisms	IT Baseline Protection Manual	NIST Computer Security Handbook	Security Categori-zation 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 8.2.3 - 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 Categori-zation 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 8.2.4 - 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 Categori-zation 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 8.2.5 - Cryptography

	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. 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

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

As discussed in clause 8, there are two different sets of safeguards, mechanisms and/or procedures, which can be applied to protect IT systems. On one hand, there are quite a few organizational safeguard categories which are generally applicable for each IT system if the specific circumstances make them necessary (as considered in 8.1), irrespective of the individual components. The selection of these safeguards are considered in 9.1. Because of their general applicability, safeguards from these categories should always be considered. Furthermore, a lot of them are not expensive to implement, since they are based on introducing organizational structures and procedures.

On the other hand, there are IT system specific safeguards (as considered in 8.2) - the selection of these safeguards depends on the type and characteristics of the IT system under review. The selection of these safeguards is discussed in 9.2.

Of course, it is always possible that one or more of these categories or specific safeguards are not applicable for an IT 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 (see clauses 10 and 11).

After all safeguard types applicable for the IT system considered are identified, further information on these safeguard types and on specific safeguards can be obtained by using clause 8 and one or more of the documents summarized in the annexes A to H (links to clause 8 are provided in the table at the end of clause 9). Before implementing the safeguards selected, they should be checked carefully against the safeguards already in place and/or planned (see 7.3).

The use of a more detailed analysis should be considered (clauses 10 and/or 11) 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 IT systems, it should be considered whether an organization-wide baseline could be established (clause 12).

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 B, E, and 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.

9.1 Generally Applicable Safeguards

Generally applicable safeguard categories are:

- IT Security Management and Policies (8.1.1),
- Security Compliance Checking (8.1.2),
- Incident Handling (8.1.3),
- Personnel (8.1.4),
- Operational Issues (8.1.5),
- Business Continuity Planning (8.1.6), and
- Physical Security (8.1.7).

The safeguards of these categories form the basis for successful IT 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 (see clause 10), 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 IT 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.

9.2 IT System Specific Safeguards

In addition to generally applicable safeguards, IT 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 IT system specific safeguards. In this example, ‘X’ refers to safeguards which should be implemented under normal circumstances and ‘(X)’ notes safeguards which might be necessary in some circumstances. The safeguard selection process would be continued by considering the safeguard descriptions presented in 8.2, and, as necessary, further information obtained from the baseline safeguard documents listed in annexes A to 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)

10 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 IT system considered. The different types of IT systems are introduced in 7.1 and an overview of possible safeguards is given in the subclauses of clause 8. In this way, it is possible to fulfil specific security needs and to aim the protection at where it is really needed.

10.1 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 IT system considered. With the help of the identification of the security concerns, taking into account relevant threats that might realize these concerns, safeguards can be selected, as described in 10.2 to 10.5.

If an assessment according to this clause proves very high security concerns, a more detailed approach is recommended in order to achieve appropriate protection. Support for that can be found in clause 11. 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 IT 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 IT 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 IT 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 is processed on the IT system, unauthorised disclosure would not cause any damage at all. Consideration of possible threats (see 10.2 to 10.5) 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 IT system, the different types may need to be considered separately. The protection afforded an IT 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 worth while 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, the approach described from 10.2 onwards should provide sufficient security for the IT 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 in 10.2 to 10.5 should be selected. Suggestions for more detailed assessments and safeguard selection according to the results of these assessments are given in ISO/IEC TR 13335-3 and in clause 11. Nevertheless, the safeguards suggested from 10.2 onwards can be used as a basis for a refined selection.

10.1.1 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.

10.1.2 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.

10.1.3 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.

10.1.4 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.

10.1.5 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.

10.1.6 Loss of reliability

Consider what damage could arise from the loss of reliability of systems. This is also important to address functionality which 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.

10.2 Safeguards for Confidentiality

The threat types which 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 IT system should be taken into account.

It should be noted that most of the safeguards listed in 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 IT 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.

10.2.1 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. This type of protection is not explicitly covered in clause 8. In case of telephones, appropriate cabling can provide some protection against eavesdropping. This protection is not covered here, but in ISO/IEC TR 13335-5.
- IT 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. More information about that can be found in 8.2.5.

10.2.2 Electromagnetic radiation

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

- Physical safeguards: These can be cladding for rooms, walls etc. which does not permit electromagnetic radiation to go beyond the cladding; this type of protection is not explicitly covered in 8.1.7 (this is not the cheapest way to protect from electromagnetic radiation).
- Data confidentiality protection: For detailed discussion, see 8.2.5. 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 IT equipment with low radiation: Again, this is not covered explicitly in clause 8, but equipment with built-in protection can be obtained.

10.2.3 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: For a detailed description of malicious code protection, see 8.2.3.
- Incident Handling: 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. More information about that can be found in 8.1.3.

10.2.4 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 (see 8.2.1).
- 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 (see 8.2.2). 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 (see 8.2.3).
- 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 (see 8.2.5).

10.2.5 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 mis- or re-routing taking place, the messages can be encrypted. More information about that can be found in 8.2.5.

10.2.6 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 handling: Everybody noticing a malfunction of software should report that to the responsible person so action can be taken as soon as possible. More information about that can be found in 8.1.3.
- Operational issues: Some software failures can be avoided by thorough testing of the software before it is used, and through software change control (see 8.1.5).

10.2.7 Theft

Theft can endanger confidentiality if the IT component stolen has any sensitive information on it which 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 IT equipment more difficult, or specific safeguards against theft (both described in 8.1.7).
- Personnel: Safeguards for personnel (controlling outside personnel, confidentiality agreements, etc.) should be in place making theft difficult (see 8.1.4).
- Data confidentiality protection: This safeguard should be implemented if theft of IT equipment containing sensitive information seems likely, e.g. laptops. For detailed discussion, see 8.2.5.
- Media controls: Any media containing sensitive material should be protected against theft (see 8.1.5).

10.2.8 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 IT 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 described in 8.2.2 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 (see 8.2.4) should be in place.
- Physical access control: Beside logical access control, protection can be provided by physical access control (see 8.1.7).
- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls (8.1.5) 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 (see 8.2.5).

10.2.9 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 (see 8.1.5). 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 (see 8.1.7).
- 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 (see 8.2.5).

10.3 Safeguards for Integrity

The threat types which might endanger integrity 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 IT system should be taken into account.

It should be noted that most of the safeguards listed in 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 IT 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.

10.3.1 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 (see 8.1.5), 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. More about back-ups can be found in 8.1.6.
- Data integrity protection: Cryptographic means can be used to protect the integrity of data in storage. More information can be found in 8.2.5.

10.3.2 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 (see 8.1.5). 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 (see 8.1.6).
- Data integrity protection: Cryptographic means can be used to protect the integrity of information. More information can be found in 8.2.5.

10.3.3 Malicious code

Malicious code can lead to a loss of integrity, e.g. if data or files are altered 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: For a detailed description of malicious code protection, see 8.2.3.
- Incident Handling: 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. More information about that can be found in 8.1.3.

10.3.4 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 (see 8.2.1).

- 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 (see 8.2.2). 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 (see 8.2.3).
- 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 (see 8.2.5).

10.3.5 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 mis- or re-routing taking place, hash functions and digital signatures can be used. More information about that can be found in 8.2.5.

10.3.6 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 which are described in 8.2.5 (data integrity and non-repudiation).

10.3.7 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 (see 8.1.3).
- 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 (see 8.1.5).
- 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 (see 8.1.6).
- Data integrity protection: Cryptographic means can be used to protect the integrity of information. More information can be found in 8.2.5.

10.3.8 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 (see 8.1.7).
- Back-ups: Back-ups should be used to restore any information that has been damaged (see 8.1.6).

10.3.9 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 IT system or network. Documentation and maintenance are used to ensure the trouble-free running of the system or network (see 8.1.5).
- Network management: Operational procedures, system planning and proper network configuration should be used to minimise the risks of technical failures (see 8.2.4).
- 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 (see 8.1.7).
- Back-ups: Back-ups should be used to restore any information that has been damaged (see 8.1.6).

10.3.10 Transmission errors

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

- Cabling: Careful planning and laying of cables can avoid transmission errors, for example, if the error is caused by overloading (see also 8.1.7).
- 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. More information can be found in 8.2.5.

10.3.11 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 IT 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 described in 8.2.2 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 (see 8.2.4) should be in place.
- Physical access control: Beside logical access control, protection can be provided by physical access control (see 8.1.7).
- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls (8.1.5) 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. More information can be found in 8.2.5.

10.3.12 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 IT system security manager - or whoever might be responsible for the security of the system (see also 8.1.4).
- Back-ups: Back-ups should be used to restore any information that has been damaged (see 8.1.6).
- 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 as described in 8.2.2 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 (see 8.2.3).

10.3.13 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 (see 8.1.5). 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 (see 8.1.7).
- Data integrity: Cryptographic means can be used to protect the integrity of information stored on the media. More information can be found in 8.2.5.

10.3.14 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 (see also 8.1.4). 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 (see 8.1.6).

10.4 Safeguards for Availability

The threat types which 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 IT system should be taken into account.

It should be noted that most of the safeguards listed in 8.1 provide a more 'general' protection, i.e. they are not aiming at specific threats but provide protection by supporting an overall effective IT 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 IT systems (but the loss of such data and unavailability of such systems is still considered critical) to highly time-critical data or IT 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.

10.4.1 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 (see also 8.1.4).
- Media controls: All media should be appropriately protected from unauthorized access using physical protection and accountability for all media (see 8.1.5).
- 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. More about back-ups can be found in 8.1.6.
- Material protection: Physical access controls should be used to avoid any unauthorized access that would facilitate to unauthorized destruction of IT equipment or information (see 8.1.7).
- 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 as described in 8.2.2 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.

10.4.2 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 (see 8.1.5).
- 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. More about back-ups can be found in 8.1.6.

10.4.3 Failure of communication equipment and services

Failure of equipment and communication services threatens the availability of information communicated via these services. Depending on what caused the failure, it might also be helpful to consider 10.4.11 Software failure, 10.4.12 Supply failure or 10.4.13 Technical failure. 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. General information about back-ups can also be found in 8.1.6.
- 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 and laying of cables can avoid damages; if there is a suspicion that a line might be damaged it should be inspected (see also 8.1.7).
- Non-repudiation: If a proof of network delivery, or sending or receiving of a message is needed, non-repudiation should be applied (see 8.2.5); then communication failures or missing information could be easily detected.

10.4.4 Fire, water

Information and IT 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 IT equipment or media on which important information is stored should be protected appropriately against fire and water (see 8.1.7).
- 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 (see 8.1.6).

10.4.5 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 (see 8.1.5).
- Back-ups: If maintenance errors have taken place, back-ups can be used to restore the availability of the lost information (see 8.1.6).

10.4.6 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: For a detailed description of malicious code protection, see 8.2.3.
- Incident Handling: 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. More information about that can be found in 8.1.3.

10.4.7 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 (see 8.2.1).
- 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 (see 8.2.2). Review and analysis of audit logs can detect unauthorized activities.
- Protection against malicious code are listed below. 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 (see 8.2.3).
- 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 events resulting from that (see 8.1.6).

10.4.8 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 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 (see 8.2.5).

10.4.9 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 (see 8.1.4).
- 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 (see 8.1.5).
- 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 described in 8.2.2 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 (see 8.2.4).

10.4.10 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 (see 8.1.7).
- 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 (see 8.1.6).

10.4.11 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 (see 8.1.3).
- 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 (see 8.1.5).
- 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 (see 8.1.6).

10.4.12 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 (see 8.1.7).
- 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. More about back-ups can be found in 8.1.6.

10.4.13 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 IT system. Documentation and maintenance are used to ensure the trouble-free running of the system (more about that in 8.1.5).
- Network management: Operational procedures, system planning and proper network configuration should be used to minimise the risks of technical failures (see 8.2.4).
- 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 (see 8.1.6).

10.4.14 Theft

Theft obviously endangers the availability of information and IT equipment. Safeguards against theft are listed below.

- Physical safeguards: This can be material protection making access to the building, area or room containing the IT equipment and information more difficult, or specific safeguards against theft (both described in 8.1.7).
- Personnel: Safeguards for personnel (controlling outside personnel, confidentiality agreements, etc.) should be in place making theft difficult (see 8.1.4).
- Media controls: Any media containing important material should be protected against theft (see 8.1.5).

10.4.15 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. General information about back-ups can also be found in 8.1.6.
- Network management: The proper configuration, management and administration of networks and communication services should be used to avoid overloading (see 8.2.4).
- 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.

10.4.16 Transmission errors

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

- Cabling: Careful planning and laying of cables can avoid transmission errors, for example, if the error is caused by overloading (see also 8.1.7).
- 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.

10.4.17 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 IT 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 described in 8.2.2 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 (see 8.2.4) should be in place.
- Physical access control: Besides logical access control, protection can be provided by physical access control (see 8.1.7).
- Media control: If sensitive data are stored on other media (e.g. floppy disc), media controls (8.1.5) should be in place to protect the media from unauthorized access.

10.4.18 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 IT system security manager - or whoever might be responsible for the security of the system (see also 8.1.4).
- Back-ups: Back-ups should be used to restore any information, services or resources that has been damaged or lost (see 8.1.6).
- 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 as described in 8.2.2 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 (see 8.2.3).

10.4.19 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 (see 8.1.5). 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 (see 8.1.7).

10.4.20 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 (see also 8.1.4). 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 (see 8.1.6).

10.5 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 listed in 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 IT 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.

10.5.1 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 IT 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.

10.5.2 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.

10.5.3 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.

11 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 IT system and its assets to be taken into account. The difference from use of the previous clauses is the level of effort, and the detail gathered during the assessment process. A qualified justification of the safeguards selected is therefore possible. 11.1 addresses how ISO/IEC TR 13335-3, which describes a method for risk analysis, can be used in the safeguard selection process of this part of ISO/IEC TR 13335. The principles of selection are addressed in 11.2.

11.1 Relation between part 3 and part 4 of ISO/IEC TR 13335

In ISO/IEC TR 13335-3, techniques for the management of IT 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 IT systems,
- to use detailed risk analysis for all IT systems, and
- to use the 'recommended approach', i.e. following a high level risk analysis of all IT systems, then a baseline approach for the IT systems at low risk and a detailed risk analysis for IT systems at high risk.

If it was decided to use detailed risk analysis for all IT systems to identify safeguards, information about how to select safeguards and how to use the results of the detailed risk analysis effectively is given in 11.2 of this part of ISO/IEC TR 13335. Nevertheless, the information about safeguards, safeguards for specific IT systems, and the link between security concerns, threats and safeguards contained in clauses 8 to 10 of this part of ISO/IEC TR 13335, can still be used.

11.2 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.

12 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:

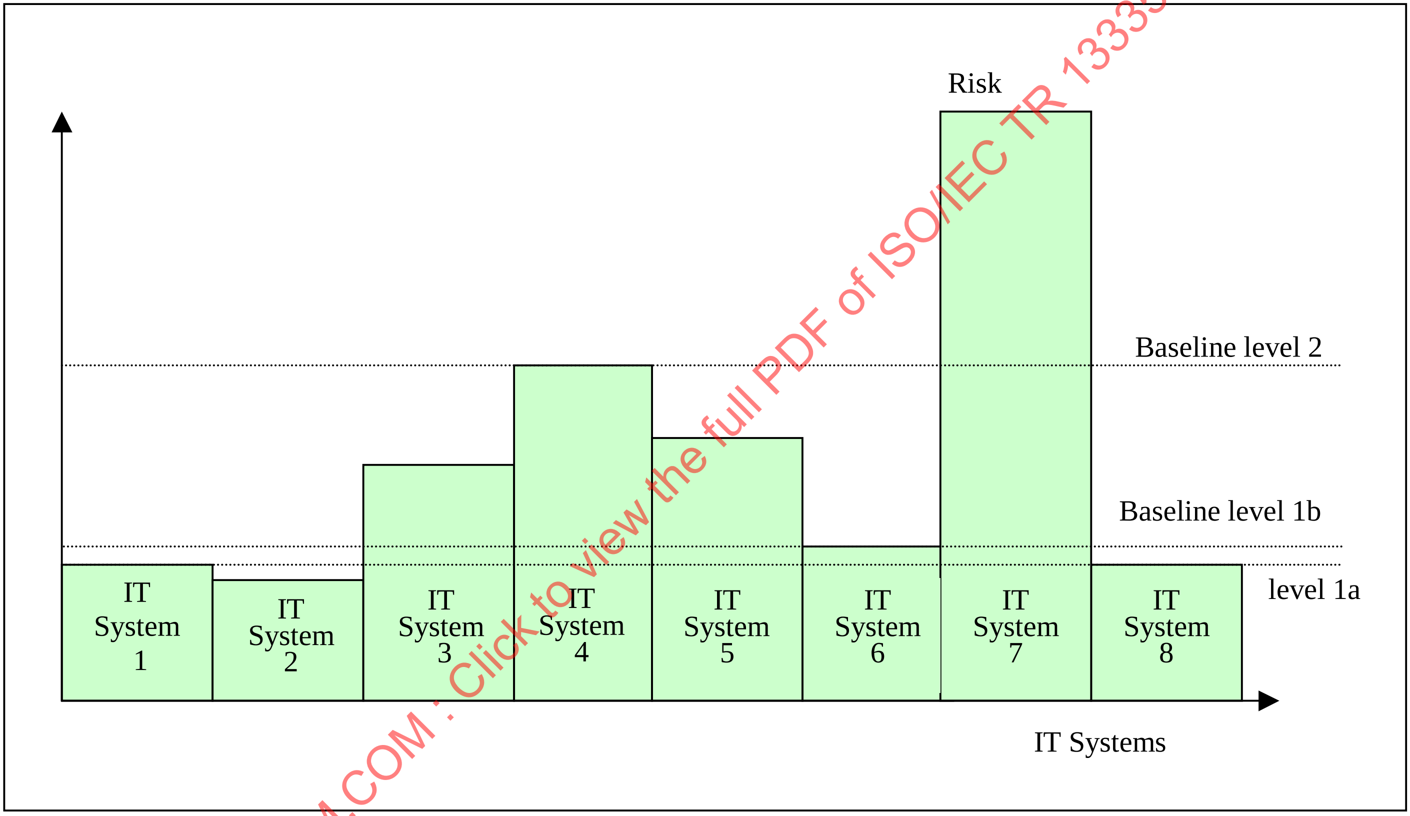

Figure 4 — Different Baseline Levels

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 IT systems 1, 2, 6, and 8 with baseline level 1 and IT systems 3, 4, and 5 with baseline level 2 in Figure 4). If IT systems with different security requirements are ‘really different’ (in the sense that most of the safeguards required to protect each of the IT 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 IT systems they are supposed to protect. Generally, any baseline level should not aim at security below the lowest security requirements of the IT systems to be protected (like below the requirements of IT system 2 in Figure 4). It is sensible to aim at a level which is sufficient for most (Baseline level 1a in Figure 4) or all (Baseline level 1b) of the IT systems which are supposed to be protected. It is often advisable to aim at the highest security level of the IT systems to be protected by the baseline safeguards since this is normally not very expensive but provides sufficient security for all IT systems involved. A careful consideration of the involved IT systems is necessary to make the final decision on which IT systems should be protected by the same baseline. Some IT 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 IT 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 IT systems with higher requirements,
- a medium level, adding specific safeguards to protect all IT systems with higher requirements, or
- a high level which is sufficient to protect all IT systems which are supposed to be 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 IT systems considered.

13 Summary

This part of ISO/IEC TR 13335 discusses different ways of safeguard selection that can be used to achieve baseline protection, or to support the techniques described in ISO/IEC TR 13335-3. This part of ISO/IEC TR 13335 also contains an overview of common safeguards which can be selected following any of the approaches mentioned above, and a reference to various baseline safeguard manuals which contain more detailed descriptions of these safeguards. Finally, the different ways of developing an organization-wide baseline and the advantages and disadvantages of the alternatives are described. This part of ISO/IEC TR 13335 can be used by any organization, large or small, that wants to select safeguards to protect its IT systems.

Bibliography

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

Annex A
Code of Practice for Information Security Management

(Type: generic)

Scope

BS 77999 is issued as a two-part standard

BS 7799-1: 1999 Code of Practice for Information Security Management;
BS 7799-2: 1999 Specification for Information Security Management Systems.

These standards are published under the authority of the Standards Board of the British Standards Institution (BSI). BS 7799-1:1999 supersedes the 1995 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 1999 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 are 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 7799-1:1999

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