

Information technology — Guidelines for the management of IT security —

Part 4: Selection of safeguards

ICS 35.040

National foreword

This British Standard reproduces verbatim ISO/IEC TR 13335-4:2000 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled “International Standards Correspondence Index”, or by using the “Search” facility of the *BSI Electronic Catalogue* or of British Standards Online.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC TR title page, pages ii to vii, a blank page, pages 1 to 61 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 1 March 2004

© BSI 1 March 2004

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)

AVA Documents
Document Sharing Hub

Table of Contents

FOREWORD	vi
INTRODUCTION	vii
1 SCOPE	1
2 REFERENCES	1
3 DEFINITIONS	1
4 AIM	1
5 OVERVIEW	2
6 INTRODUCTION TO SAFEGUARD SELECTION AND THE CONCEPT OF BASELINE SECURITY	4
7 BASIC ASSESSMENTS	8
7.1 IDENTIFICATION OF THE TYPE OF IT SYSTEM	8
7.2 IDENTIFICATION OF PHYSICAL/ENVIRONMENTAL CONDITIONS	8
7.3 ASSESSMENT OF EXISTING/PLANNED SAFEGUARDS	9
8 SAFEGUARDS	9
8.1 ORGANIZATIONAL AND PHYSICAL SAFEGUARDS	10
8.1.1 <i>IT Security Management and Policies</i>	10
8.1.2 <i>Security Compliance Checking</i>	10
8.1.3 <i>Incident Handling</i>	11
8.1.4 <i>Personnel</i>	11
8.1.5 <i>Operational Issues</i>	12
8.1.6 <i>Business Continuity Planning</i>	13
8.1.7 <i>Physical Security</i>	13
8.2 IT SYSTEM SPECIFIC SAFEGUARDS	18
8.2.1 <i>Identification and Authentication (I&A)</i>	18
8.2.2 <i>Logical Access Control and Audit</i>	19
8.2.3 <i>Protection against Malicious Code</i>	19
8.2.4 <i>Network Management</i>	20
8.2.5 <i>Cryptography</i>	21
9 BASELINE APPROACH: SELECTION OF SAFEGUARDS ACCORDING TO THE TYPE OF IT SYSTEM	24
9.1 GENERALLY APPLICABLE SAFEGUARDS	25
9.2 IT SYSTEM SPECIFIC SAFEGUARDS	26
10 SELECTION OF SAFEGUARDS ACCORDING TO SECURITY CONCERNS AND THREATS..	27
10.1 ASSESSMENT OF SECURITY CONCERNS	27
10.1.1 <i>Loss of confidentiality</i>	28
10.1.2 <i>Loss of integrity</i>	28
10.1.3 <i>Loss of availability</i>	28
10.1.4 <i>Loss of accountability</i>	29
10.1.5 <i>Loss of authenticity</i>	29
10.1.6 <i>Loss of reliability</i>	29
10.2 SAFEGUARDS FOR CONFIDENTIALITY	30
10.2.1 <i>Eavesdropping</i>	30

10.2.2	Electromagnetic radiation	30
10.2.3	Malicious code.....	31
10.2.4	Masquerading of user identity	31
10.2.5	Misrouting/re-routing of messages	31
10.2.6	Software failure.....	31
10.2.7	Theft	32
10.2.8	Unauthorized access to computers, data, services and applications	32
10.2.9	Unauthorized access to storage media	32
10.3	SAFEGUARDS FOR INTEGRITY	33
10.3.1	Deterioration of storage media	33
10.3.2	Maintenance error	33
10.3.3	Malicious code.....	33
10.3.4	Masquerading of user identity	33
10.3.5	Misrouting/re-routing of messages	34
10.3.6	Non-Repudiation.....	34
10.3.7	Software failure.....	34
10.3.8	Supply failure (power, air conditioning).....	34
10.3.9	Technical failure.....	35
10.3.10	Transmission errors	35
10.3.11	Unauthorized access to computers, data, services and applications	35
10.3.12	Use of unauthorized programmes and data	36
10.3.13	Unauthorized access to storage media	36
10.3.14	User error	36
10.4	SAFEGUARDS FOR AVAILABILITY	36
10.4.1	Destructive attack	37
10.4.2	Deterioration of storage media.....	37
10.4.3	Failure of communication equipment and services.....	37
10.4.4	Fire, water	38
10.4.5	Maintenance error	38
10.4.6	Malicious code.....	38
10.4.7	Masquerading of user identity	38
10.4.8	Misrouting/re-routing of messages	39
10.4.9	Misuse of resources.....	39
10.4.10	Natural disasters.....	39
10.4.11	Software failures	39
10.4.12	Supply failure (power, air conditioning).....	40
10.4.13	Technical failures.....	40
10.4.14	Theft	40
10.4.15	Traffic overloading	40
10.4.16	Transmission errors.....	41
10.4.17	Unauthorized access to computers, data, services and applications	41
10.4.18	Use of unauthorized programmes and data	41
10.4.19	Unauthorized access to storage media	42
10.4.20	User error	42
10.5	SAFEGUARDS FOR ACCOUNTABILITY, AUTHENTICITY AND RELIABILITY	42
10.5.1	Accountability	42
10.5.2	Authenticity	42
10.5.3	Reliability.....	43
11	SELECTION OF SAFEGUARDS ACCORDING TO DETAILED ASSESSMENTS.....	43
11.1	RELATION BETWEEN PART 3 AND PART 4 OF THIS TECHNICAL REPORT	43
11.2	PRINCIPLES OF SELECTION	43
12	DEVELOPMENT OF AN ORGANIZATION-WIDE BASELINE	45
13	SUMMARY.....	46
	BIBLIOGRAPHY	46

ANNEX A	CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT.....	47
ANNEX B	ETSI BASELINE SECURITY STANDARD FEATURES AND MECHANISMS	49
ANNEX C	IT BASELINE PROTECTION MANUAL	51
ANNEX D	NIST COMPUTER SECURITY HANDBOOK	53
ANNEX E	MEDICAL INFORMATICS: SECURITY CATEGORISATION AND PROTECTION FOR HEALTHCARE INFORMATION SYSTEMS	55
ANNEX F	TC68 BANKING AND RELATED FINANCIAL SERVICES - INFORMATION SECURITY GUIDELINES	56
ANNEX G	PROTECTION OF SENSITIVE INFORMATION NOT COVERED BY THE OFFICIAL SECRETS ACT - RECOMMENDATIONS FOR COMPUTER WORKSTATIONS.....	58
ANNEX H	CANADIAN HANDBOOK ON INFORMATION TECHNOLOGY SECURITY.....	60

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.

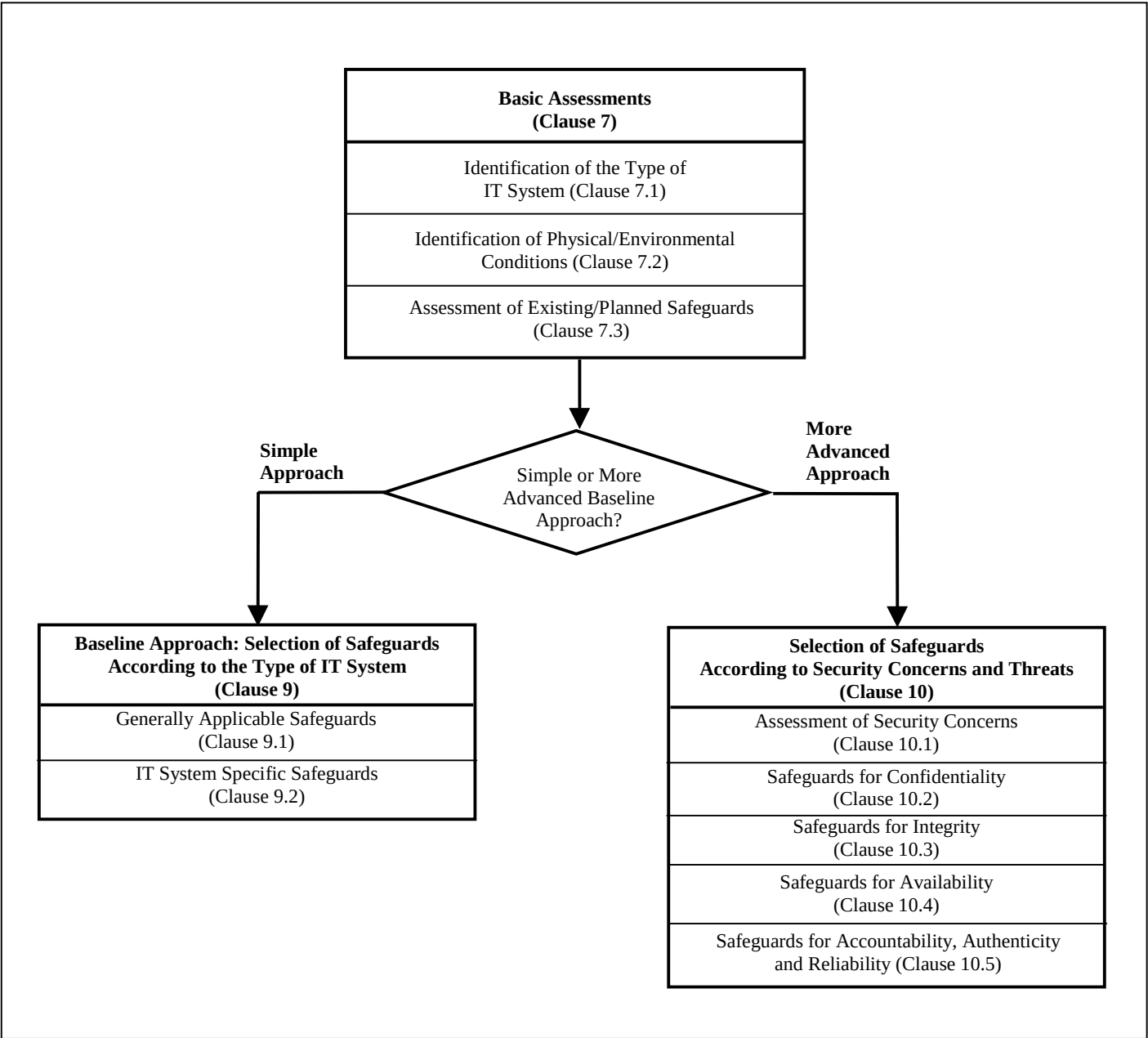


Figure 1 — Selection of Safeguards According to the Type of IT System or According to Security Concerns and Threats

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.

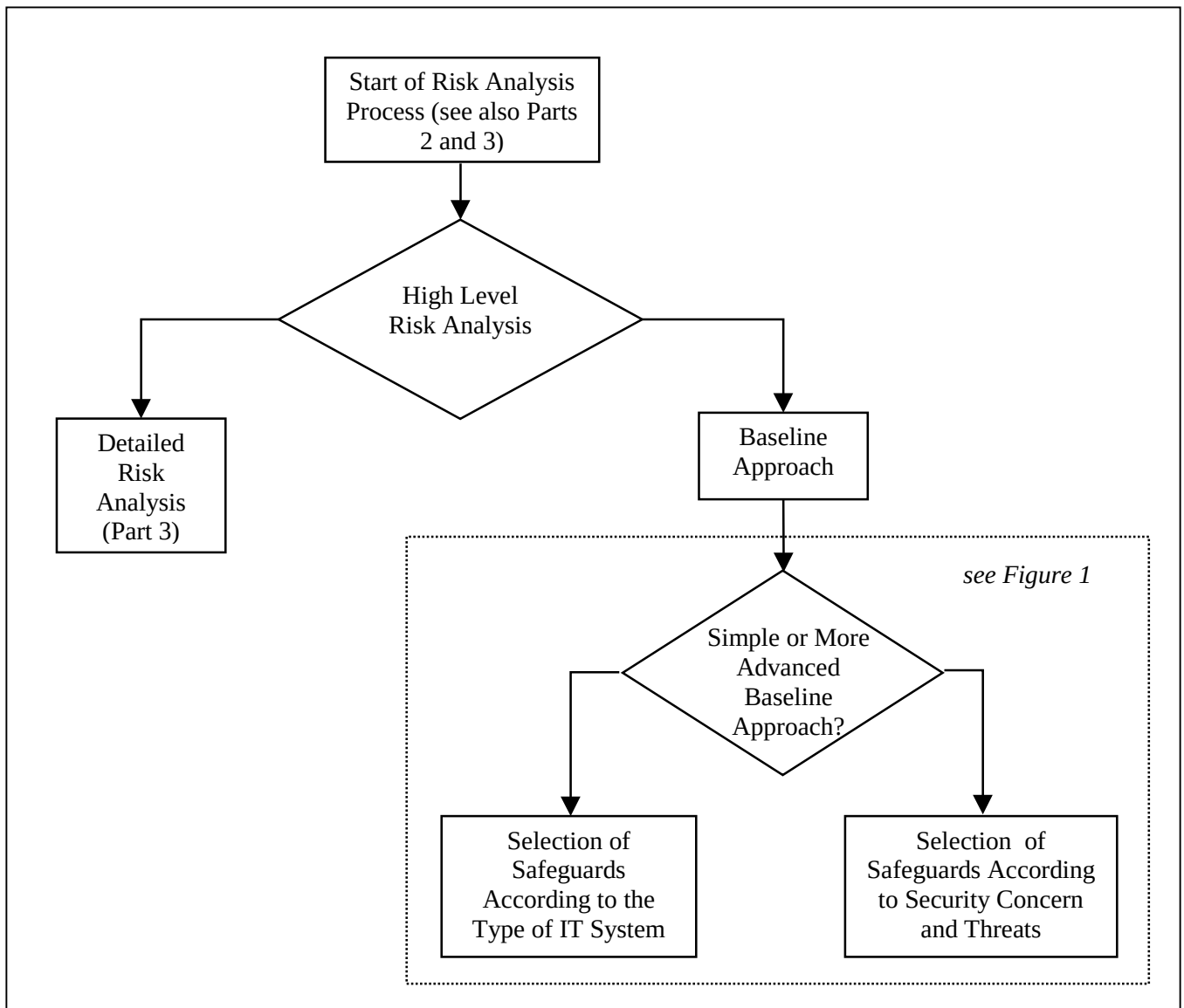


Figure 2 — Ways of Safeguard Selection

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.

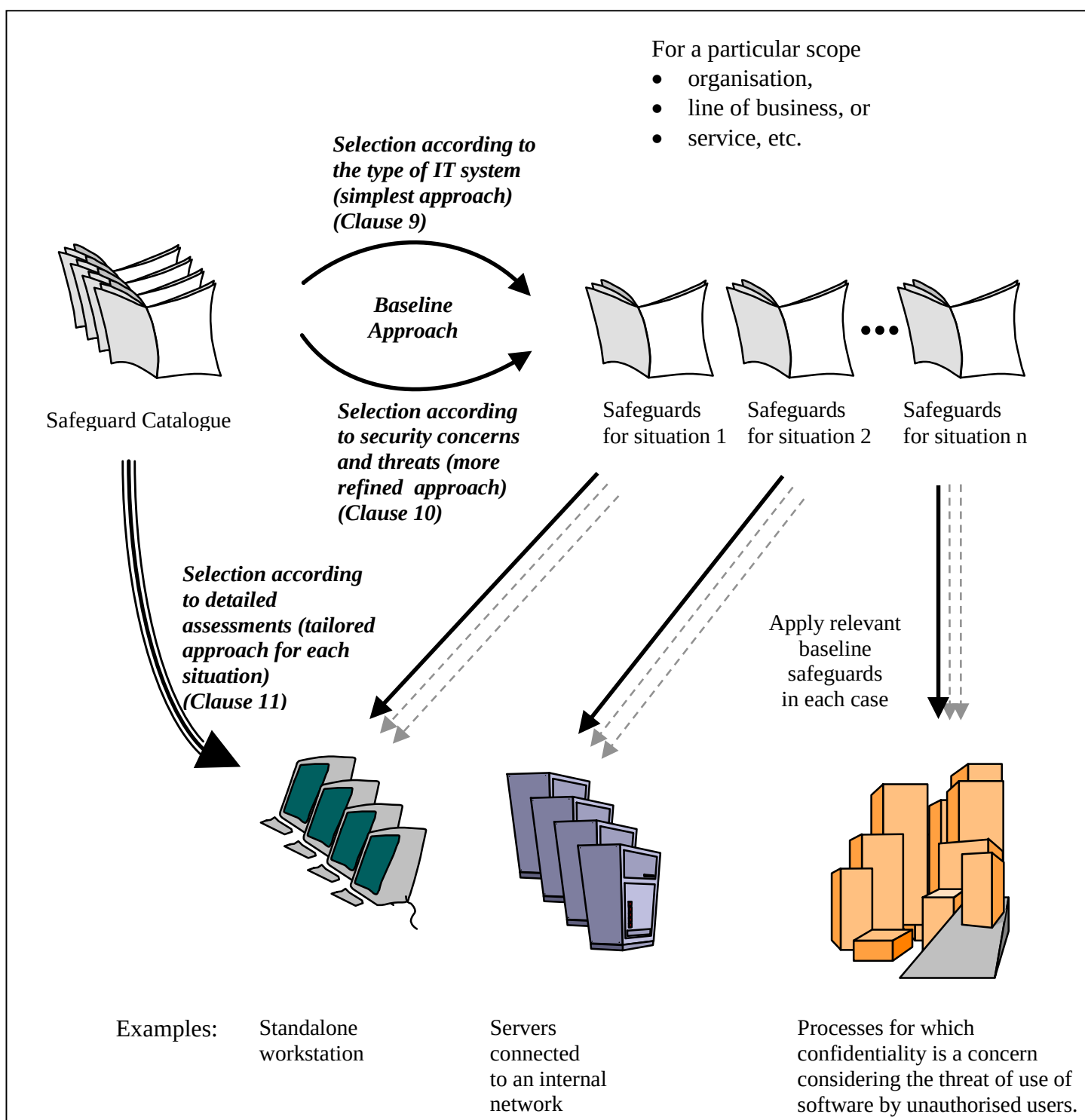


Figure 3 — Approaches to Safeguard Selection

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 than 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.