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)

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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.

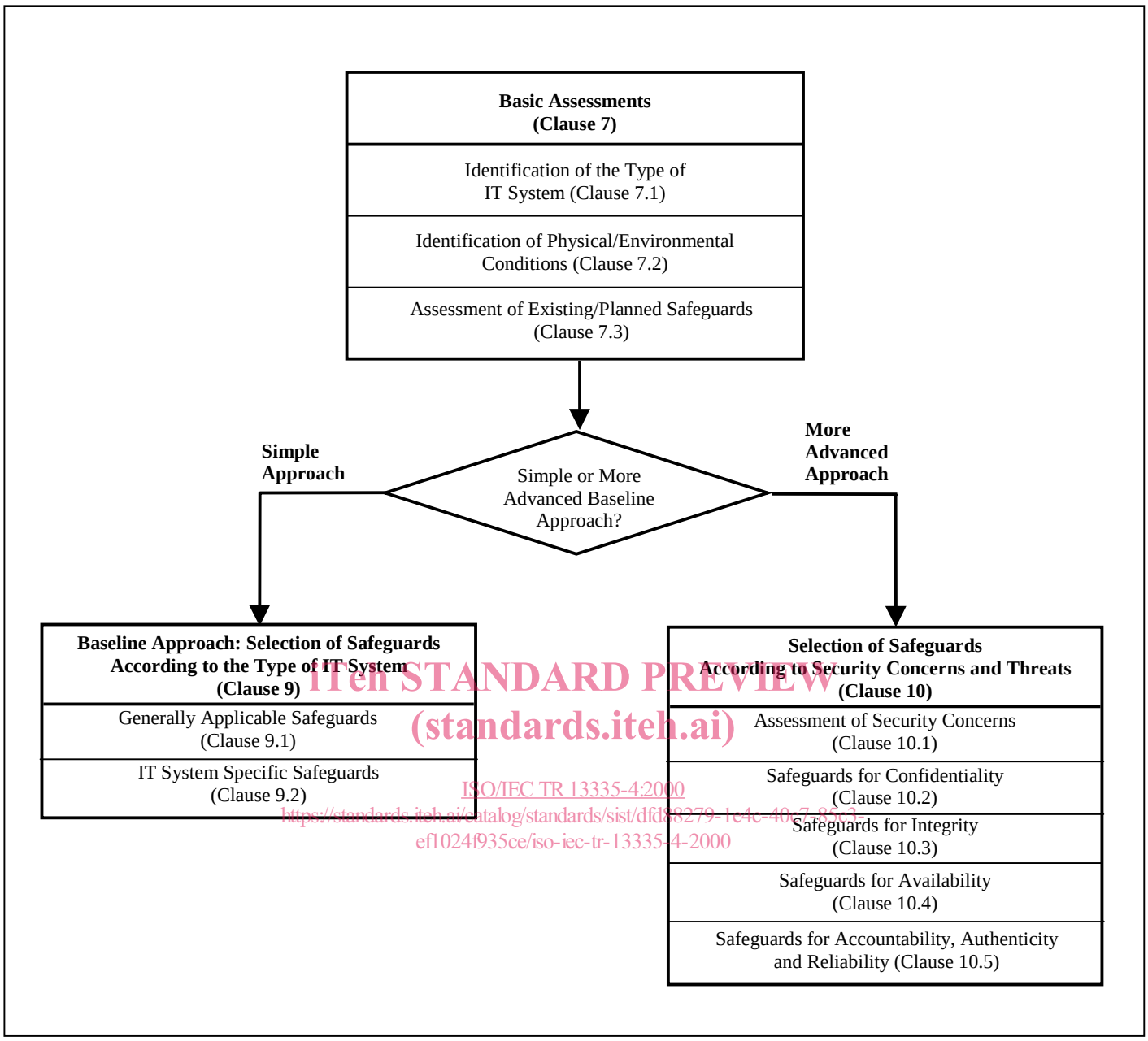

Figure 1 — Selection of Safeguards According to the Type of IT System or According to Security Concerns and Threats

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.

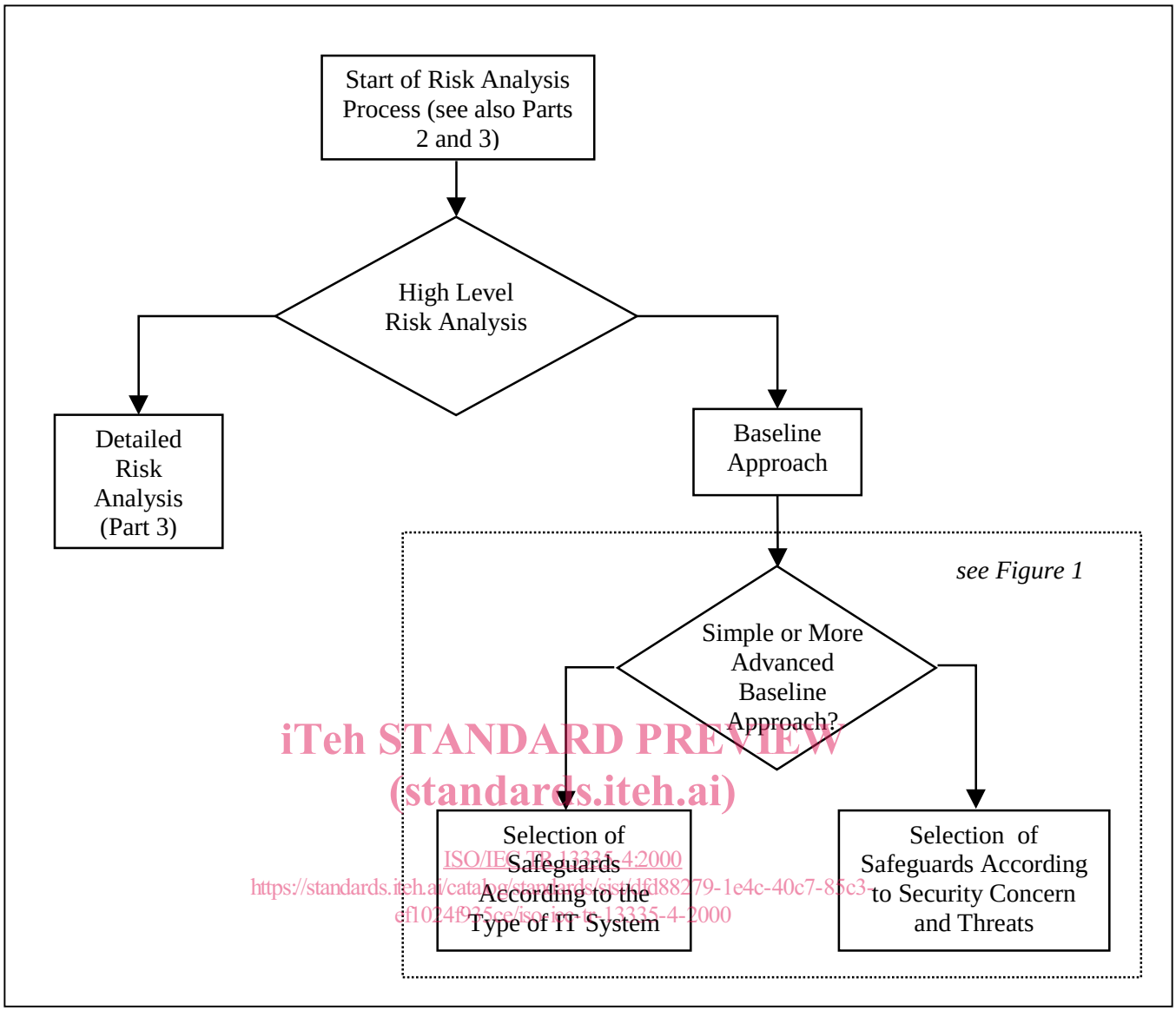

Figure 2 — Ways of Safeguard Selection

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.

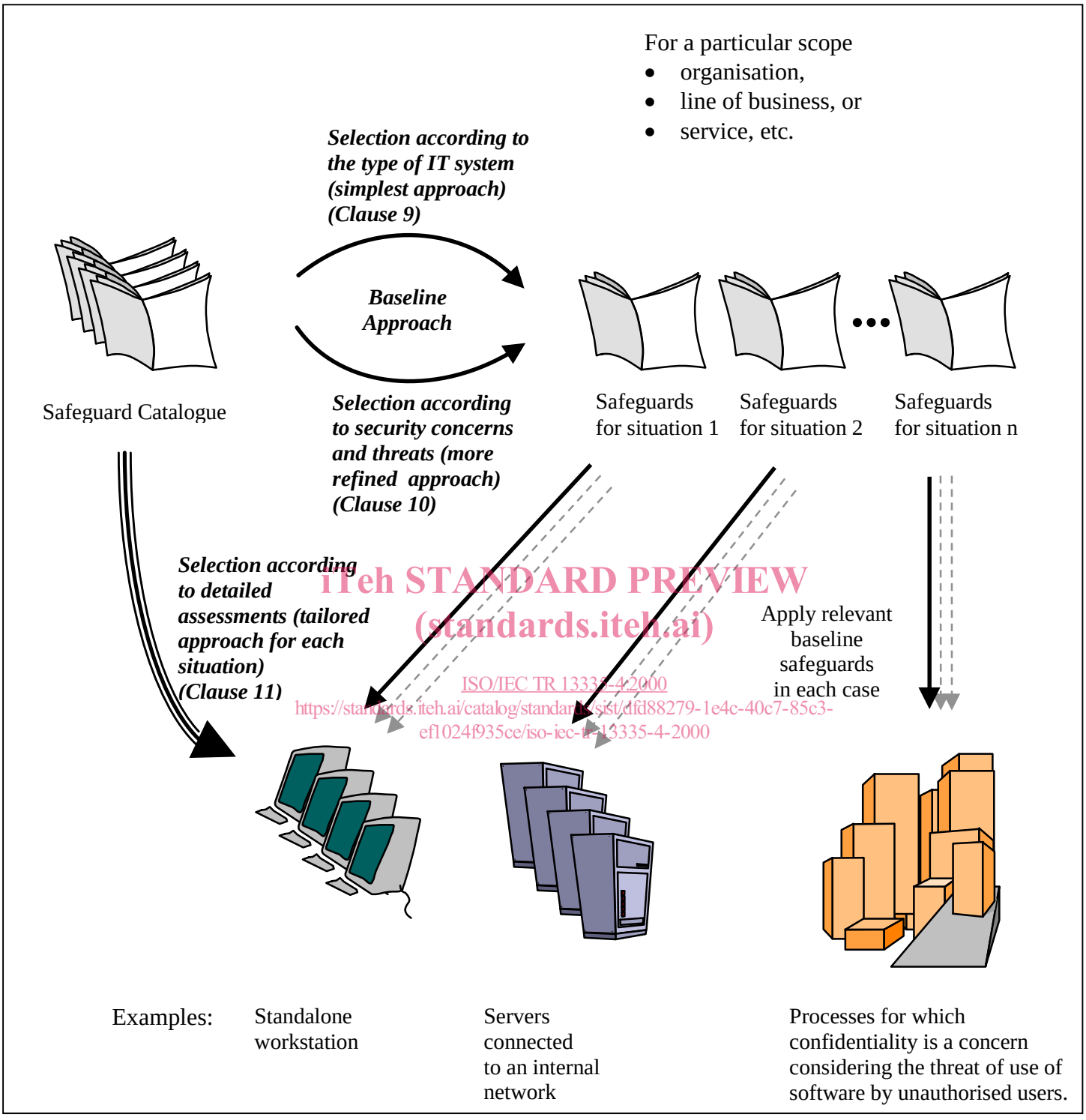

Figure 3 — Approaches to Safeguard Selection

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.