TECHNICAL REPORT

ISO/IEC TR 13335-3

First edition
1998-06-15

Information technology — Guidelines for the management of IT Security —

Part 3:
Techniques for the management of IT Security

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

Partie 3: Techniques pour la gestion de sécurité IT

Contents

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Committee) 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.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The main task of technical committees is to prepare International Standards, but in exceptional circumstances a technical committee may propose the publication of a Technical Report of one of the following types:

- type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;
- type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;
- type 3, 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).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

ISO/IEC TR 13335-3, which is a Technical Report of type 3, 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 manangement 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 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 ISO/IEC TR 13335 to meet their specific needs. The specific objectives of ISO/IEC TR 13335 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. ISO/IEC TR 13335-1 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 the organization's overall security programme.

ISO/IEC TR 13335-2 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 are responsible 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.

This part of ISO/IEC TR 13335 describes security techniques relevant to those involved with management activities during a project life-cycle, such as planning, designing, implementing, testing, acquisition, or operations.

ISO/IEC TR 13335-4 provides guidance on 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 ISO/IEC TR 13335-3, and how additional assessment methods can be used for the selection of safeguards.

ISO/IEC TR 13335-5 provides guidance to an organization connecting its IT systems to external networks. This guidance includes the selection and use of safeguards to provide security for the external connections and the services supported by those connections, and additional safeguards required for the IT systems because of the connections.

Information technology — Guidelines for the management of IT Security —

Part 3: Techniques for the management of IT Security

1 Scope

This part of ISO/IEC TR 13335 provides techniques for the management of IT security. The techniques are based on the general guidelines laid out in ISO/IEC TR 13335-1 and ISO/IEC TR 13335-2. These guidelines are designed to assist the implementation of IT security. Familiarity with the concepts and models introduced in ISO/IEC TR 13335-1 and the material concerning the management and planning of IT security in ISO/IEC TR 13335-2 is important for a complete understanding of this part of ISO/IEC TR 13335.

2 References

ISO/IEC TR 13335-1: 1996, *Guidelines for the management of IT Security — Part 1: Concepts and models for IT Security*.

ISO/IEC TR 13335-2: 1997, *Guidelines for the management of IT Security — Part 2: Managing and planning IT Security*.

3 Definitions

For the purposes of this part of ISO/IEC TR 13335, the following definitions given 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.

4 Structure

This part of ISO/IEC TR 13335 is divided into 12 clauses. Clause 5 provides information on the aim of this part of ISO/IEC TR 13335. Clause 6 gives an overview of the IT security management process. Clause 7 discusses the importance of a corporate IT security policy and what it should include. Clause 8 provides an overview of four different approaches an organization may use to identify security needs. Clause 9 describes the recommended approach in detail and is followed by a description of safeguard implementation in Clause 10. This clause also includes a detailed discussion of security awareness programmes and the approval process. Clause 11 contains a description on several follow-up activities that are necessary in order to ensure that safeguards are working effectively. Finally, Clause 12 provides a brief summary of this part of ISO/IEC TR 13335.

5 Aim

The aim of this part of ISO/IEC TR 13335 is to describe and recommend techniques for the successful management of IT security. These techniques can be used to assess security requirements and risks, and help to establish and maintain the appropriate security safeguards, i.e. the correct IT security level. The results achieved in this way may need to be enhanced by additional safeguards dictated by the actual organization and environment. This part of ISO/IEC TR 13335 is relevant to everybody within an organization who is responsible for the management and/or the implementation of IT security.

6 Techniques for the Management of IT Security

The process of the management of IT security is based on the principles set out in ISO/IEC TR 13335-1 and ISO/IEC TR 13335-2 . It can be applied to the whole organization as well as to selected parts of it. Figure 1 shows the major stages in this process, and how the results of this process feed back into the various parts of it. Feedback loops should be established whenever required, be it within a stage, or after one or more of the stages are completed. Figure 1 (below) is a revision of Figure 1 in ISO/IEC TR 13335-2 emphasizing the topics this part of ISO/IEC TR 13335 is concentrating on.

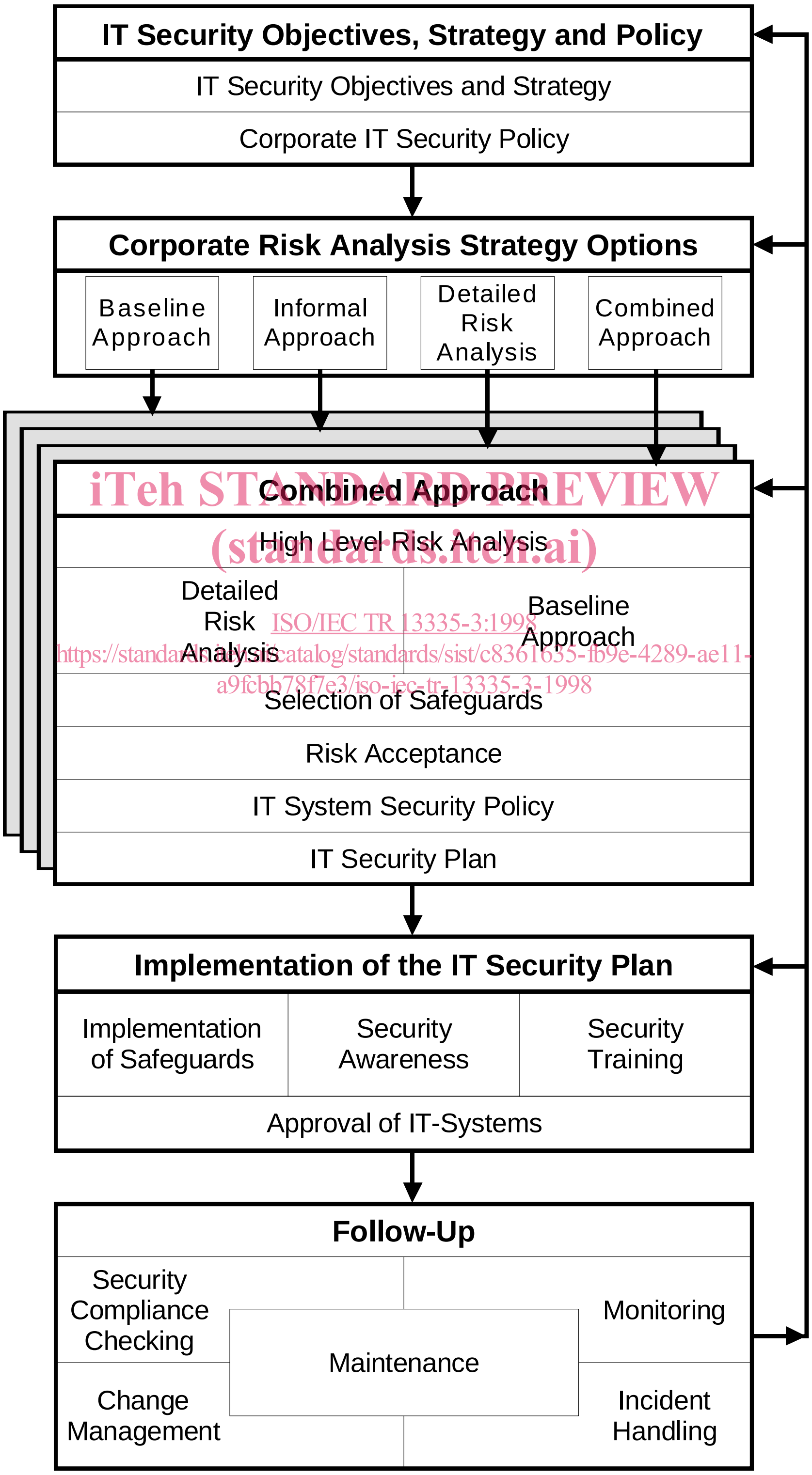

Figure 1: Management of IT Security

The management of IT security includes the analysis of the requirements for security, the establishment of a plan for satisfying these requirements, the implementation of this plan, as well as maintenance and administration of the implemented security. This process starts with establishing the organization’s IT security objectives and strategy, and the development of a corporate IT security policy.

An important part of the IT security management process is the assessment of risks, and how they can be reduced to an acceptable level. It is necessary to take into account the business objectives, as well as organizational and environmental aspects, and each IT system's specific needs and risks.

After assessing the security requirements of the IT systems and services, it is advisable to select a corporate risk analysis strategy. The major strategy options are discussed in detail in Clause 8 below. The recommended option involves conducting a high level risk analysis for all IT systems to identify those systems at high risk. These systems are then examined through detailed risk analysis, while a baseline approach is applied for the remaining systems. For the high risk systems, the detailed consideration of assets, threats and vulnerabilities will lead to a detailed risk analysis which facilitates the selection of effective safeguards commensurate with the assessed risks. By using this option, the risk management process can be focused on where the significant risks or greatest needs are, and the overall programme can be made more cost and time effective.

Following the risk assessment, appropriate safeguards are identified for each IT system to reduce the risks to an acceptable level. These safeguards are implemented as outlined in the IT security plan. The implementation should be supported by an awareness and training programme, which is important for the effectiveness of the safeguards.

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

7 IT Security Objectives, Strategy and Policies

After establishing the organization's IT security objectives, an IT security strategy should be developed to form a basis for the development of a corporate IT security policy. The development of a corporate IT security policy is essential to ensure that the results of the risk management process are appropriate and effective. Management support across the organization is required for the development and effective implementation of the policy. It is essential that a corporate IT security policy takes into account the corporate objectives and particular aspects of the organization. It must be in alignment with the corporate security policy and the corporate business policy. With this alignment, the corporate IT security policy will help to achieve the most effective use of resources, and will ensure a consistent approach to security across a range of different system environments.

It may be necessary to develop a separate and specific security policy for each or some of the IT systems. This policy should be based on risk analysis or baseline results and be consistent with the corporate IT security policy, thus taking into account the security recommendations for the system to which it relates.

7.1 IT Security Objectives and Strategy

As a first step in the process of managing IT security, one should consider the question 'what broad level of risk is acceptable to the organization?'. The correct level of acceptable risks, and thence the appropriate level of security, is the key to successful security management. The necessary broad level of security is determined by the IT security objectives an organization needs to meet. In order to assess these security objectives, the assets and how valuable they are for the organization should be considered. This is mainly determined by the importance that IT has for supporting the conduct of the organization's business; the costs of IT itself is only a small part of its value. Possible questions for assessing how much an organization's business depends on IT are:

- What are the important/very important parts of the business which cannot be carried out without IT support?
- What are the tasks which can only be done with the help of IT?
- What essential decisions depend on the accuracy, integrity, or availability of information processed by IT, or on how up-to-date this information is?
- What confidential information processed needs to be protected?
- What are the implications of an unwanted security incident for the organization?

Answering these questions can help to assess the security objectives of an organization. If, for example, some important or very important parts of the business are dependent on accurate or up to date information, then one of the security objectives of this organization may be to ensure the integrity and timeliness of the information as it is processed in the IT systems. Also, important business objectives and their relation to security should be considered when assessing security objectives.

Dependent on the security objectives, a strategy for achieving these objectives should be agreed upon. The strategy chosen should be appropriate to the value of the assets to be protected. If, for example, the answers to one or more of the questions above is 'Yes', then it is likely that the organization has high security requirements, and it is advisable to choose a strategy which includes sufficient effort to fulfil these requirements.

An IT security strategy outlines in general terms how an organisation will achieve its IT security objectives. The topics such a strategy should address will depend on the number, type and importance of those objectives, and normally be those which the organisation considers important to be uniformly addressed throughout the organisation. The topics could be quite specific, or very broad, in nature.

As an example of the former, an organisation could have a primary IT security objective that, because of the nature of its business, all of its systems should maintain a high level of availability. In this case, one strategy topic could be directed at minimising virus infestation through organisation-wide installation of anti-virus software (or nominating selected sites for virus checking through which all software received must be passed).

To illustrate the latter, at a broad level, an organisation could have an IT security objective, because its business is selling its IT services, that the security of its systems have to be proven to its potential customers. In this case, a strategy topic could be that all systems have to be validated as being secure by a recognised third party.

Other possible topics for an IT security strategy, because of specific objectives or combinations thereof, could include:

- the risk analysis strategy and methods to be adopted organisation-wide,
- the need for an IT system security policy for each system,
- the need for security operating procedures for each system,
- an organisation-wide information sensitivity categorisation scheme,

- the need for security conditions of connections to be met, and checked, before other organizations are connected, and
- the incident handling scheme to be universally used.

Once determined, the security strategy and its constituent topics should be encompassed in the corporate IT security policy.

7.2 Corporate IT Security Policy

A corporate IT security policy should be produced based on the agreed corporate IT security objectives and strategy. It is necessary to establish and maintain a corporate IT security policy, consistent with the corporate business, security, and IT policies, and security related legislation and regulation.

As reflected in 7.1, an important fact influencing the corporate IT security policy is how dependent an organization is on the IT it is using. The more important the use of IT is, and the more an organization has to rely on its IT, the more security is needed to guarantee that the business objectives are met. When writing the corporate IT security policy, the cultural, environmental and organizational characteristics should be borne in mind, since they can influence the approach towards security, e.g. some safeguards, which might be easily accepted in one environment, may be totally unacceptable in another.

The security relevant activities described in the corporate IT security policy can be based on the organizational objectives and strategy, the results of previous security risk analysis and management reviews, the results of follow-up actions such as security compliance checking of implemented safeguards, of monitoring and reviewing IT security in day-to-day use, and of reports of security relevant incidents. Any serious threat or vulnerability detected during these activities needs to be addressed, with the corporate IT security policy describing the organization's overall approach to deal with these security problems. The detailed actions are described in the various IT system security policies, or in other supporting documents, for example, security operating procedures.

When developing the corporate IT security policy, representatives from the following functions should participate:

- audit,
- finance,
- information systems (technicians and users),
- utilities/infrastructure (i.e. persons responsible for building structure and accommodation, power, air-conditioning),
- personnel,
- security, and
- senior business management.

According to the security objectives, and the strategy an organization has adopted to achieve these objectives, the appropriate level of detail of the corporate IT security policy is selected. As a minimum, the corporate IT security policy should describe:

- its scope and purpose,
- the security objectives with respect to legal and regulatory obligations, and business objectives,
- IT security requirements, in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability of information,
- the administration of information security, covering organization and individual responsibilities and authorities,
- the risk management approach which is adopted by the organization,

- the means by which priorities for the implementation of safeguards can be determined,
- the broad level of security and residual risk sought by management,
- any general rules for access control (logical access control as well as the control of physical access to buildings, rooms, systems, and information),
- the approach to security awareness and training within the organization,
- broad procedures to check and maintain security,
- general personnel security issues,
- the means by which the policy will be communicated to all persons involved,
- the circumstances under which the policy should be reviewed, and
- the method of controlling changes to the policy.

Where a more detailed corporate IT security policy is needed, the following issues should also be considered:

- organization-wide security models and procedures,
- the use of standards,
- the procedures for the implementation of safeguards,
- the approach towards follow-up activities like
    - security compliance checking,
    - monitoring of safeguards,
    - handling of security related incidents,
    - monitoring of IT system usage, and
- the circumstances under which external security consultants will be engaged.

An example contents list for a corporate IT security policy is given in Annex A.

As discussed earlier in this clause, the results of previous risk analysis and management reviews, security compliance checking and security incidents may have an effect on the corporate IT security policy. This, in turn, may require that a previously defined strategy or policy is reviewed or refined.

To ensure adequate support for all security related measures, the corporate IT security policy should be approved by top management.

Based on the corporate IT security policy, a directive should be written, which is binding for all managers and employees. This may require the signature of each employee on a document which acknowledges his/her responsibility for security within the organization. Furthermore, a programme for security awareness and training should be developed and implemented to communicate these aspects.

An individual should be designated to be responsible for the corporate IT security policy, and for ensuring that this policy reflects the requirements and the actual status of the organization. This person would typically be the corporate IT security officer, who among other things should be responsible for the follow-up activities. This includes security compliance check reviews, the handling of incidents and security weaknesses, and any changes to the corporate IT security policy which might be necessary according to the results of those actions.

8 Corporate Risk Analysis Strategy Options

NOTE — To ensure that this part of ISO/IEC TR 13335 is complete, consistent, and can be read independently of ISO/IEC TR 13335-2, Clause 8 deals with the same topics as Clause 10 of ISO/IEC TR 13335-2.

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

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

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

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

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

8.1 Baseline Approach

For the first option, an organization could apply baseline security to all IT systems by selecting standard safeguards. A variety of standard safeguards are suggested in baseline documents and codes of practice; a more detailed explanation of this approach can also be found in 9.2.

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

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

The disadvantages of this option are:

- if the baseline level is set too high, there might be an excessive level of security on some IT systems,
- if the level is set too low there may be a lack of security on some IT systems, resulting in a higher level of exposure, and
- there might be difficulties in managing security relevant changes. For instance, if a system is upgraded, it might be difficult to assess whether the original baseline safeguards are still sufficient.

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

8.2 Informal Approach

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

The advantage of this option is:

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

However, there are a number of disadvantages:

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

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

8.3 Detailed Risk Analysis

The third option is to conduct detailed risk analysis reviews for all IT systems in the organization. Detailed risk analysis involves in-depth identification and valuation of assets, the assessment of threats to those assets, and assessment of vulnerabilities. The results from these activities are then used to assess the risks and thence identify justified security safeguards. This approach is described in detail in 9.3.

The advantages with this approach are:

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

The disadvantages of this option are:

it requires a considerable amount of time and effort, and expertise, to obtain results.

there is the possibility that the security needs of a critical system are addressed too late, since all IT systems would be considered in the same detail and a considerable amount of time is required to complete the analyses.

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

- use of a standard approach, that meets the criteria reflected in this TR (for example, the approach described in 9.3),
- use a standard approach in different ways appropriate to the organization; the use of 'risk modelling techniques' (described in 9.3) could be of advantage to some organizations.

8.4 Combined Approach

The fourth option is to first conduct an initial high level risk analysis for all IT systems, in each case concentrating on the business values of the IT system and the serious risks to which it is exposed. For the IT systems identified as being important for the organization's business and/or exposed to high risks, a detailed risk analysis should be conducted in a priority order. For all other IT systems, a baseline approach should be chosen. This option, which is in a sense the combination of the best points of the options described in 8.1 and 8.3, provides a good balance between minimizing the time and effort spent in identifying safeguards, while still ensuring that the high risk systems are appropriately protected.

Additional advantages of this option are:

- the incorporation of an initial quick and simple approach is likely to gain acceptance of the risk analysis programme,
- it should be possible to quickly build a strategic picture of an organizational security programme, i.e. it will act as a good planning aid,
- resources and money can be applied where they are most beneficial, and systems likely to be in the greatest need of protection will be addressed first, and
  the follow up actions will be more successful.

The only potential disadvantage is:

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

The adoption of a high level risk analysis approach, combined with the baseline approach, and detailed risk analysis where appropriate, offers the majority of organizations the most effective way forward. This approach is recommended and will be examined in more detail in Clause 9.