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

Reference number
ISO/IEC TR 13335-3:1998(E)

Contents

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 Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.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 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 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.

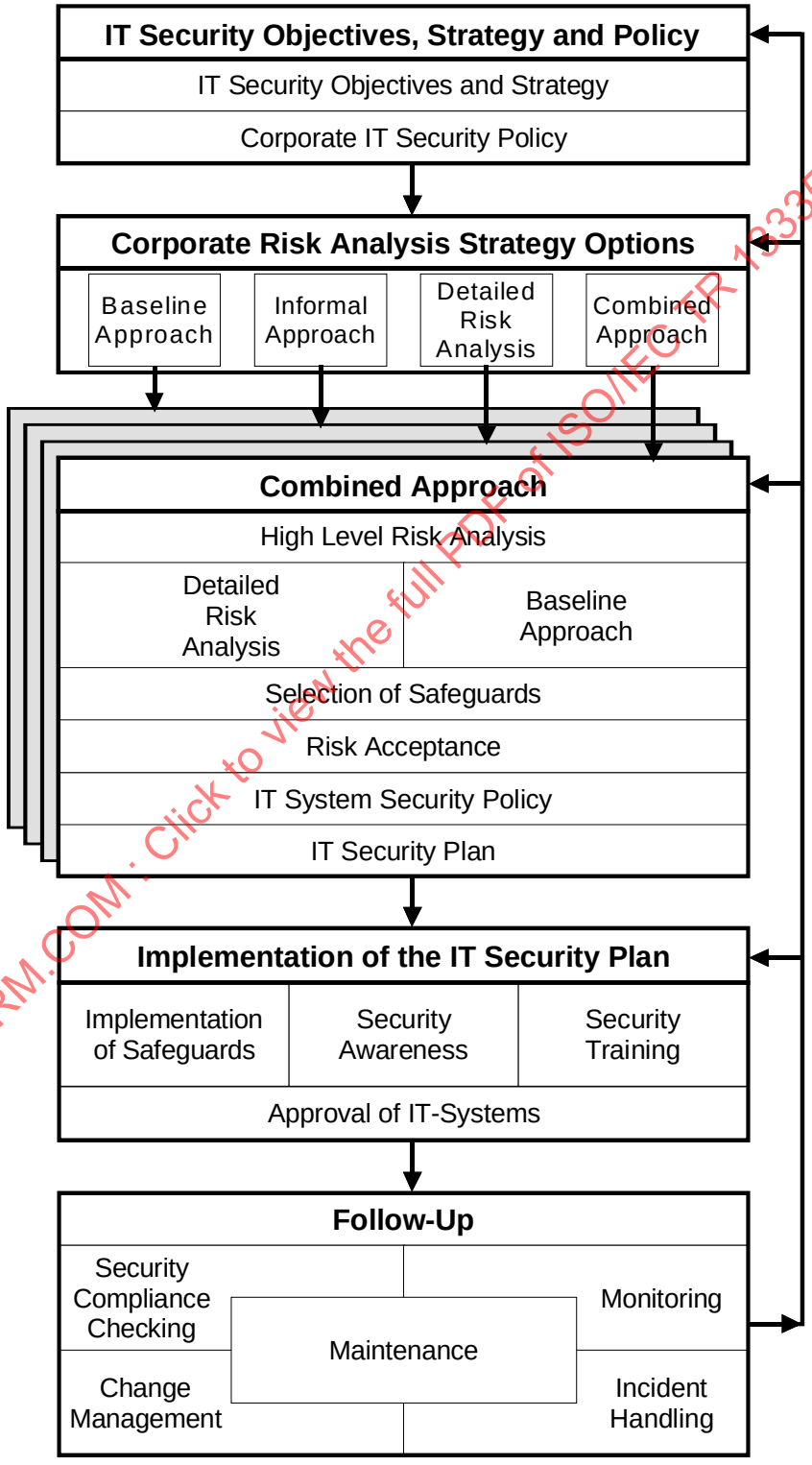

Figure 1: Management of IT Security

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.

9 Combined Approach

This section provides guidance for implementing the combined risk analysis strategy recommended above.

9.1 High Level Risk Analysis

First it is necessary to conduct an initial high level risk analysis to identify which approach (baseline or detailed risk analysis) is appropriate for each IT system. This high level risk analysis considers the business values of the IT systems and the information handled, and the risks from the organization's business point of view. Input for the decision as to which approach is suitable for which IT system can be obtained from consideration of the following:

- the business objectives to be achieved by using the IT system,
- the degree to which the organization's business depends on the IT system, i.e. whether functions that the organization considers critical to its survival or the effective conduct of business are dependent on this system, or on the confidentiality, integrity, availability, accountability, authenticity, and reliability of the information processed on this system,
- the level of investment in this IT system, in terms of developing, maintaining, or replacing the system, and
- the assets of the IT system, for which the organization directly assigns value.

When these items are assessed, the decision is generally easy. If the objectives of a system are important to an organization's conduct of business, if system replacement costs are high, or if the values of the assets are at high risk, then a detailed risk analysis is necessary for the system. Any one of these conditions may be enough to justify conducting a detailed risk analysis.

A general rule to apply is: if the lack of IT system security can result in significant harm or damage to an organization, its business processes or its assets, then a detailed risk analysis (9.3) is necessary to identify potential risks. In all other cases, the application of a baseline approach (9.2) provides appropriate protection.

9.2 Baseline Approach

The objective of baseline protection is to establish a minimum set of safeguards to protect all or some IT systems of an organization. Using this approach, it is possible to apply baseline protection organization-wide, and, as reflected above, additionally use detailed risk analysis reviews to protect IT systems at high risk or systems critical to the business. The use of the baseline approach reduces the investment that the organization has to make in the performance of risk analysis reviews (8.1).

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

Baseline catalogues may specify safeguards to be used in detail, or they may suggest a set of security requirements to be addressed with whatever safeguards appropriate to the system under consideration. Both approaches have advantages. Catalogues of both types can be found in the Annexes of ISO/IEC TR 13335-4. One of the objectives of the baseline approach is consistency of security safeguards throughout the organization, which can be achieved by both approaches.

Several documents are already available which provide sets of baseline safeguards. Also, sometimes a similarity of environments can be observed among companies within the same industrial sector. After the examination of the basic needs, it may be possible for baseline safeguard catalogues to be used by a number of different organizations. For example, catalogues of baseline safeguards could be obtained from:

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

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

9.3 Detailed Risk Analysis

As indicated in 8.3, a detailed risk analysis for an IT system involves the identification of the related risks, and an assessment of their magnitude. The need for a detailed risk analysis can be determined without unnecessary investment in time and money when high level reviews are conducted for all systems, followed by detailed risk analysis reviews only on high risk or critical systems as recommended in 8.4.

The risk analysis is done by an identification of potential adverse business impacts of unwanted events and the likelihood of their occurrence. Unwanted events can adversely impact the business, persons or any other valuable entity of the organization. The adverse impact of an unwanted event is a composite of possible damages related to the value of the assets at risk. The likelihood of occurrence is dependent on how attractive the asset is for a potential attacker, the likelihood of threats occurring, and the ease with which the vulnerabilities can be exploited. The results of the risk analysis lead to the identification and selection of safeguards which can be used to reduce the identified risks to an acceptable level.

Detailed risk analysis involves in-depth reviews at each of the steps shown in Figure 2. It leads to the selection of justified safeguards as part of the risk management process. The requirements for these safeguards are documented in the IT system security policy and the related IT security plan. A number of incidents and external influences which may affect the security requirements of the system can make it necessary to reconsider parts of or the whole risk analysis. Those influences could be: recent significant changes to the system, planned changes, or the consequences of incidents which need to be dealt with.

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

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

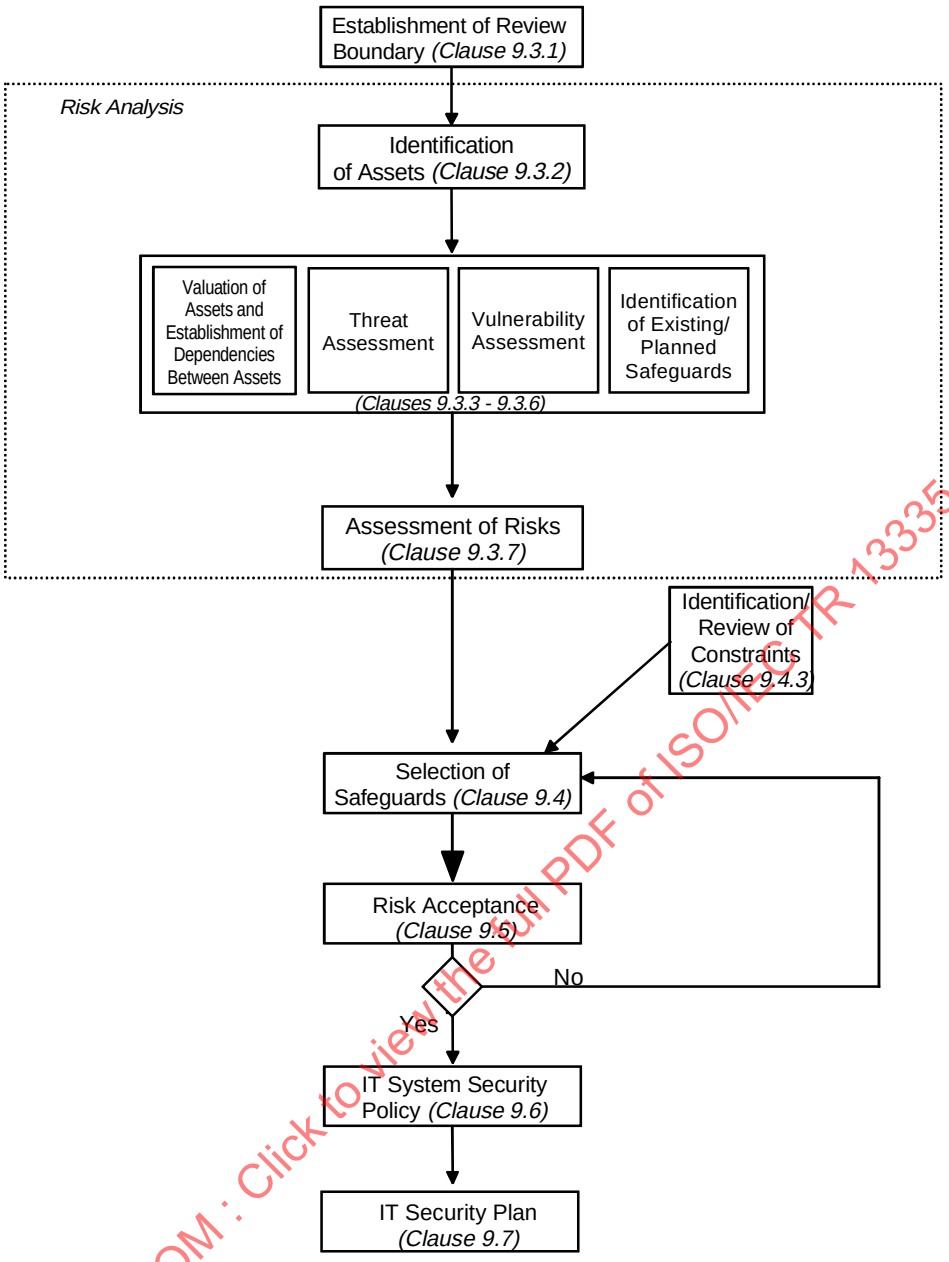

Figure 2: Risk Management Involving Detailed Risk Analysis

9.3.1 Establishment of Review Boundary

As shown in Figure 2, prior to gathering input for the asset identification and valuation, the boundaries of the review should be defined. A careful definition of boundaries at this stage avoids unnecessary work and improves the quality of the risk analysis. The boundary description should clearly define which of the following have to be considered when carrying out the risk analysis review for the considered IT system:

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

9.3.2 Identification of Assets

An asset is a component or part of a total system to which an organization directly assigns value and hence for which the organization requires protection. For the identification of assets it should be borne in mind that an IT system consists of more than hardware and software. For example, asset types can be any of the following:

- information/data (e.g. files containing payment details, product information),
- hardware (e.g. computer, printer),
- software, including applications (e.g. text processing programs, programs developed for special purposes),
- communications equipment (e.g. telephones, copper cable, fibre),
- firmware (e.g. floppy discs, CD Read Only Memories, Programmable ROMs),
- documents (e.g. contracts),
- funds (e.g. in Automatic Teller Machines),
- manufactured goods,
- services (e.g. information services, computing resources),
- confidence and trust in services (e.g. payment services),
- environmental equipment,
- personnel,
- image of the organization.

All assets within the review boundary established (see 9.3.1) must be identified. Conversely, any assets to be excluded from a review boundary, for whatever reason, need to be assigned to another review to ensure that they do not get forgotten or overlooked.

9.3.3 Valuation of Assets and Establishment of Dependencies Between Assets

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

The input for the valuation of assets should be provided by owners and users of the assets. The person(s) carrying out the risk analysis will list the assets. They should seek assistance from those involved in business planning, finance, information systems and other relevant activities in order to identify values for each of these assets. The values assigned should be related to the cost of obtaining and maintaining the asset, and the potential adverse business impacts from loss of confidentiality, integrity, availability, accountability, authenticity and reliability. Each of the assets identified should be of value to the organization. However, there will not be a direct or easy way to establish financial value for all. It is also necessary to establish the value or extent of importance in non-financial, i.e. qualitative, terms to the organization. Otherwise it will be difficult to identify the level of protection and the amount of resource the organization should devote to protect the assets. An example for such a valuation scale could be a distinction between low, medium and high, or, in more detail:

negligible - low - medium - high - very high.

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

- violation of legislation and/or regulation,
- impairment of business performance,
- loss of goodwill/negative effect on reputation,

- breach of confidentiality associated with personal information,
- endangerment of personal safety,
- adverse effects on law enforcement,
- breach of commercial confidentiality,
- breach of public order,
- financial loss,
- disruption to business activities, and
- endangerment of environmental safety.

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

It should be emphasized at this stage that the method for assessment must allow not only quantitative valuation, but also qualitative valuation where quantitative valuation is impossible or illogical (for example, the potential for loss of life, or loss of business goodwill). Explanation should be given of the valuation scale used.

Dependencies of assets on other assets should also be identified, since this might influence the values of the assets. For example, the confidentiality of data should be kept throughout its processing, i.e. the security needs of a data processing program should be directly related to the value representing the confidentiality of the data processed. Also, if a business process is relying on the integrity of certain data being produced by a program, the input data of this program should be of appropriate reliability. Moreover, the integrity of information will be dependent on the hardware and software used for its storage and processing. Also, the hardware will be dependent on the power supply and possibly the air conditioning. Thus information about dependencies will assist in the identification of relevant threats and particularly vulnerabilities. It will also help to assure that the true value of the assets (through the dependency relationships) is given to the assets and thereby ensuring an appropriate level of protection.

The values of assets on which other assets are dependent may be modified in the following way:

- if the values of the dependent assets (e.g. data) are lower or equal to the value of the asset considered (e.g. software), its value remains the same, and
- if the values of the dependent asset (e.g. data) is greater, then the value of the asset considered (e.g. software) should be increased according to:
  - the degree of dependency, and
  - the values of the other assets.

An organization may have some assets which are available more than once, like copies of software programs or the same type of PC used in most of the offices. It is important to consider this fact when doing the asset valuation. On one hand, these copies etc. are overlooked easily, so care must be taken to identify all of them; on the other hand, they could be used to reduce availability problems.

The final output of this step is a list of assets and their values relative to disclosure (preservation of confidentiality), modification (preservation of integrity), non-availability and destruction (preservation of availability), and replacement cost.

9.3.4 Threat Assessment

A threat has the potential to harm the IT system and its assets under review. If a threat occurred, it could impinge on the IT system in some way to cause unwanted incidents and thus adverse impacts. Threats may be of natural or human origin, and could be accidental or deliberate. Both accidental or deliberate threat sources should be identified and the likelihood

of their occurrence should be assessed. It is essential that no relevant threat is overlooked, since this could result in failure or weaknesses in the IT system security.

Input to the threat assessment should be obtained from the asset owners or users, from personnel department staff, from facility planning and IT specialists, as well as from people responsible for the protection of the organization. Other organizations like legal bodies and national government authorities may be able to assist, for example by providing threat statistics. A list of generally possible threats is helpful to perform the threat assessment. An example is given in Annex C. Nevertheless it might be worthwhile to consult other threat catalogues (maybe specific to your organization or business) since no list can be exhaustive. Some of the most common manifestations of threats are:

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

When using threat catalogues or the results of earlier threat assessments, one should be aware that threats are continually changing, especially if the business environment or the IT changes. For example, the viruses of the 90's are significantly more complex than those of the 80's. It is also interesting to note that the implementation of safeguards such as virus checking software always seem to lead to the development of new viruses which are resistant to current safeguards.

After identifying the threat source (who and what causes the threat) and the threat target (i.e. what elements of the system may be affected by the threat), it is necessary to assess the likelihood of the threats. This should take account of:

- the threat frequency (how often it might occur, according to experience, statistics, etc.), if statistics etc. can be applied,
- the motivation, the capabilities perceived and necessary, resources available to possible attackers, and the perception of attractiveness and vulnerability of IT system assets for the possible attacker, for deliberate threat sources, and
- geographical factors such as proximity to chemical or petroleum factories, the possibility of extreme weather conditions, and factors that could influence human errors and equipment malfunction, for accidental threat sources.

Depending on the need for accuracy, it might be necessary to split assets into their components and relate the threats to the components. For instance, a physical asset might initially be considered to be 'central data servers', but when it is identified that these servers are in different geographic locations, it would be split into 'central data server 1' and 'central data server 2' because some threats may be different, and others at different levels. Similarly, a software asset might first be regarded as 'application software' but later broken down into two or more instances of 'application software'. An example with regard to a data asset could be where it is first determined as 'criminal record' but later split into 'criminal record text' and 'criminal record image'.

At the completion of the threat assessment, there will be a list of threats identified, the assets or groups of assets they would affect, and measures of the likelihood of threats occurring on a scale such as high, medium, or low.

9.3.5 Vulnerability Assessment

This assessment includes identifying weaknesses in the physical environment, organization,

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

Vulnerabilities can be related to properties or attributes of the asset that can be used in a way, or for a purpose, other than that intended when the asset was purchased or made. For example, one of the properties of an EEPROM (Electronically Erasable Programmable Read Only Memory) is that the information stored on it can be erased and replaced. This is one of the design criteria of an EEPROM. However, this property also means that the unauthorized destruction of information stored on the EEPROM is possible. This can be a vulnerability.

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

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

More examples of vulnerabilities can be found in Annex D.

It is important to assess how severe the vulnerabilities are, in other words how easily they may be exploited. A vulnerability should be assessed in relation to each threat that might exploit it in a particular situation. For instance, a system may have a vulnerability to the threats of masquerading of user identity and misuse of resources. The vulnerability to masquerading of user identity may be high because of lack of user authentication. On the other hand, the vulnerability to misuse resources may be low because even with lack of user authentication the means by which resources might be misused are limited.

The result of this step should be a list of vulnerabilities and assessments of the ease of exploitation, e.g. on a scale high, medium, and low.

9.3.6 Identification of Existing/Planned Safeguards

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

In addition, a check needs to be made to determine whether the safeguards selected following the risk analysis review (see 9.4) are compatible with existing and planned safeguards, i.e. that the safeguards being selected and existing safeguards should not hinder each other.

While identifying the existing safeguards, a check should be made to ensure that the safeguards are working correctly. A safeguard which is relied on to work correctly, but does not function in the business process, is a source of possible vulnerability.

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

9.3.7 Assessment of Risks

The objective of this step is to identify and assess the risks to which the IT system and its assets are exposed, in order to identify and select appropriate and justified security safeguards. Risks are a function of the values of the assets at risk, the likelihood of threats occurring to cause the potential adverse business impacts, the ease of exploitation of the vulnerabilities by the identified threats, and any existing or planned safeguards which might reduce the risk.

There are different ways of relating these factors; for example, the values assigned to the assets, vulnerabilities and threats are combined to obtain values measuring the risk. A detailed consideration of the different types of risk analysis method based on values assessed for assets, vulnerabilities, and threats can be found in Annex E.

Whatever way is taken to assess the measures of risk, the result of this step should be a list of measured risks for each of the impacts of disclosure, modification, non-availability, and destruction for the considered IT system. Further, the measures of risk help identify which risks should be dealt with first when selecting safeguards. The method used should be repeatable and traceable.

As reflected earlier, various automated software tools may be used to support all or parts of the risk analysis process. If an organization decides to use a tool, care should be taken that the approach used is in line with the organization's IT security strategy and policy. Also, effort should be made to obtain accurate input, since a tool can only work as precisely as its input allows.

9.4 Selection of Safeguards

Appropriate and justified safeguards should be identified and selected to reduce the assessed risks to an acceptable level. Existing and planned safeguards, the IT security architecture, and constraints of various types have to be taken into account to allow a proper selection (see 9.3.6, 9.4.2 and 9.4.3). Additional advice on the selection of safeguards can be found in ISO/IEC TR 13335-4.

9.4.1 Identification of Safeguards

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

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

There might be alternatives, which are decided on according to the costs of the considered safeguards. Areas where safeguards are applicable include:

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

The existing and planned safeguards should be re-examined in terms of cost comparisons, including maintenance, with a view to removing (or not implementing) or improving them if they are not effective enough. Here it should be noted that sometimes it is more expensive to remove an inappropriate safeguard than to leave it in place, and maybe add another safeguard. It is possible as well that a safeguard may provide protection to assets outside of the current review boundary.

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

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

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

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

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

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

Physical security safeguards include strength of internal building walls, key coded door locks, fire suppression systems, and guards. Personnel security covers personnel recruitment checks, (especially people in 'positions of trust'), staff monitoring, and security awareness programmes.

Procedural security includes secure operating procedures documentation, application development and acceptance procedures as well as procedures for incident handling. Related to this category, it is very important that an appropriate business continuity, including contingency planning/disaster recovery, strategy and plan(s) are developed for each system. The plan should include details of the key functions and priorities for recovery, processing needs, and the organizational procedures to follow if a disaster or service interruption occurs. Such plans must include the steps required to safeguard sensitive information being processed, while still permitting the organization to conduct business.

Technical security encompasses hardware and software security as well as communications safeguards. These safeguards are selected according to the risks to provide security

functionality and assurance. The functionality will cover, for example, identification and authentication, logical access control requirements, audit trail/security logging needs, dial-back security, message authentication, encryption, and so on. Assurance requirements document the level of trust needed in security functions and thus the amount and type of checking, security testing, etc., necessary to confirm that level. In deciding on the complimentary blend of operational and technical safeguards, there will be different options for implementing the technical security requirements. A technical security architecture should be defined for each option to help identifying that security can be provided as required, and also that it is feasible with available technology.

An organization may chose to make use of evaluated products and systems as part of the final system solution. Evaluated products are those which have been examined by a third party. The third party may be another part of the same organization or an independent organization specializing in product and system evaluation. The evaluation may be performed against a set of predetermined criteria that are created specifically for the system being built or it may be a generalized set of criteria that can be used in a variety of situations. The evaluation criteria may specify functional requirements and/or assurance requirements. A number of evaluation schemes are in existence, many of them sponsored by government and international standards organizations. An organization could decide to make use of evaluated products and systems when it requires confidence that the set of functionality implemented is what is required, and when it needs to trust in the correctness and completeness of the implementation of that functionality. Alternatively, focused pragmatic security testing could provide assurance of confidence in the security provided.

When selecting safeguards for implementation, a number of factors should be considered including:

- ease of use of the safeguard,
- transparency to the user,
- the help provided to the users to perform their function,
- the relative strength of the safeguards, and
- the types of functions performed - prevention, deterrence, detection, recovery, correction, monitoring, and awareness.

Generally, a safeguard will fulfil more than one of these functions - the more it can fulfil the better. When examining the overall security, or set of safeguards to be used, a balance should be maintained between the types of functions if at all possible. This helps the overall security to be more effective and efficient. A cost / benefit analysis may be required as well as a trade-off analysis (a method of comparing competing alternatives using a set of criteria which are weighted for relative importance in regard to the particular situation).

9.4.2 IT Security Architecture

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

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

An IT security architecture focuses on technical security services and how they will fulfil the security objectives. In doing this, related non-technical security safeguards are taken into account. Even though the architecture can be built from a number of different perspectives and approaches, one fundamental principle should be taken into account. A security problem in a

unique security domain (an area of the same or similar security requirements and safeguards) must not be permitted to adversely impact the security of another unique security domain. An IT security architecture will normally consist of one or more security domains. The security domains should follow the business domains that the organization is using and has established, as closely as practical. These business domains may follow particular business functional divisions such as payroll, manufacturing, or customer service, or they may follow business services divisions such as e-mail services or office services.

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

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

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

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

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

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

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

9.4.3 Identification/Review of Constraints

There are many constraints which can affect the selection of safeguards. These constraints must be taken into account when making recommendations and during the implementation. Typical constraints are:

Time constraints:
Many types of time constraints can exist. For example, safeguards should be implemented within a time period acceptable for management. Another type of time constraints is whether a safeguard can be implemented within the lifetime of the system. A third type of time constraint may be the period of time management decides is an acceptable period to leave the system exposed to a particular risk.

Financial constraints:
Safeguards should not be more expensive to implement than the value of assets they are designed to protect. Every effort should be made not to exceed assigned budgets. However, in some cases it may not be possible to achieve the desired security and level of risk acceptance within those budget constraints. This therefore becomes a management decision as to the resolution of this situation.

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

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

Environmental constraints:
Environmental factors may influence the selection of safeguards, like space availability, extreme climate conditions, surrounding natural and urban geography, etc.

Legal constraints:
Legal factors like personal data protection or criminal code provisions for information processing could affect the selection of safeguards. Non IT specific laws and regulations like fire department regulations, labour relations laws etc. could also affect safeguard selection.

9.5 Risk Acceptance

After choosing the safeguards and identifying the reduction of risks these safeguards will achieve, there will always be residual risks - no system can be made absolutely secure. These residual risks should be categorized as 'acceptable' or 'unacceptable' for the organization. This categorization can be accomplished by reviewing the potential adverse business impacts associated with those risks. Obviously, the unacceptable risks cannot be tolerated without further considerations. It is a management decision whether these risks will be accepted because of other constraints (like costs, or simply impossibility of prevention - as in the case of planes crashing on a building or earthquakes; however, plans to recover from such events can still be made), or whether additional and maybe expensive safeguards are selected to reduce the unacceptable risks.

9.6 IT System Security Policy

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

Many systems require their own security policies, which should be based on risk analysis reviews. This is normally the case with large and complex systems, or with systems that introduce unique and special considerations not found in other systems of the organization. The IT system security policy should be compatible with the corporate IT security policy, and any conflict should be avoided. It should address issues at a level lower than that of the corporate IT security policy. The IT system security policy is based on the results of the risk analysis review and identification of safeguards for this system and is supported by the set of safeguards selected according to the assessed risks. These safeguards ensure that an adequate level of protection is achieved for the system.

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

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

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

9.7 IT Security Plan

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

- the security objectives in terms of confidentiality, integrity, availability, accountability, authenticity and reliability,
- the risk analysis option decided on for this IT system (see Clause 8),
- an assessment of the residual risks expected and accepted after implementing the safeguards identified (see 9.5),
- a list of the selected safeguards to be implemented (see 9.4), and a list of existing and planned safeguards, including a determination of their effectiveness and the safeguard upgrades needed (see 9.3.6 and 9.4); this list should include:
    - priorities for the implementation of the selected safeguards and the upgrading of existing safeguards, and
    - how these safeguards should work in practice,
- the estimation of the installation and running costs for these safeguards,
- the estimation of man-power resources for the implementation of these safeguards, and for follow-up actions, and

- a detailed workplan for the implementation, containing:
  - priorities,
  - an implementation schedule in relation to priorities,
  - the budget needed,
  - responsibilities,
  - the security awareness and training procedures for IT staff and end users which is needed to ensure the effectiveness of the safeguards,
  - a schedule for approval processes to take place where needed, and
  - a schedule for follow-up procedures.

Moreover, the IT security plan should describe the facilities to control the process of correct implementation of safeguards, like

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

The result of this step should be a detailed IT security plan for each system, based on the IT system security policy, which takes into account the results of the review described in Clause 9. It should ensure that the safeguards are implemented in time, according to the priorities derived from the risks to the IT system, and in line with a description of how to implement the safeguards and how to reach the security level which is appropriate. It also should contain a schedule for follow-up procedures to maintain this security level. These follow-up procedures are described in detail in Clause 11.

10 Implementation of the IT Security Plan

The correct implementation of security safeguards relies heavily upon a well structured and documented IT security plan. Security awareness and training associated with each IT system should take place in parallel. When the implementation of the IT security plan is completed, approval of all safeguards may be required before the system or service can be put into operational use.

10.1 Implementation of Safeguards

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

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

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

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

Once the IT security plan is completed and signed-off by the responsible functions, safeguards must be implemented, security compliance checked, and tested. A security compliance check review should be conducted to ascertain that the security safeguards have been implemented correctly, that they are being used effectively and tested properly. Security testing can be conducted as part of this review. Testing is an important technique to ensure that the implementation has been carried out and completed correctly. Security testing should be guided by a security test plan that describes the testing approach, schedule and environment. Penetration testing can be used if justified by the risks assessed. Detailed security testing procedures should be written and a standard test report used. The objective is to perform implementation and testing in a manner which ensures that the requirements from the IT security plan are met and the risk is reduced as specified.

10.2 Security Awareness

The objective of the security awareness programme is to increase the level of awareness within the organization to the point where security becomes second nature and the process becomes a routine that all employees can easily follow. The programme should ensure that the IT staff and the end users have enough knowledge of the IT systems (hardware and software), and that they understand why safeguards are necessary and how to use them correctly. Only safeguards accepted by the IT staff and end users can work effectively.

The input to the security awareness programme should come from all levels of the organization. It should include the corporate IT security policy and it should cover all objectives of the organizational IT security plan. Management support from all departments is necessary for the awareness team. In detail, the following topics should be covered by courses, talks, or any other activities described in the security awareness programme:

- the explanation of the importance of security to both the organization and the individual,
- the security needs and objectives for the IT systems in terms of confidentiality, integrity, availability, accountability, authenticity, and reliability,
- the implication of security incidents to both the organization and the individual,
- the correct use of the IT systems, including hardware and software,
- the objectives behind, and an explanation of, the corporate IT security policy, any security guidelines and directives, and the risk management strategy, leading into an understanding of risks and safeguards,
- the necessary protection for and the risks to the IT systems,
- restricted access to IT areas (authorized personnel, door locks, badges, entrance log) and to information (logical access control, read/update rights), and why these restrictions are necessary,
- the need to report breaches of security or attempts,
- procedures, responsibilities and job descriptions,
- anything the IT staff and end users must not do because of security factors,
- the consequences if staff are responsible for security breaches,
- the IT system security plans to implement and check safeguards,
- why these safeguards are necessary, and how to use them correctly,
- procedures related to security compliance checking, and
- change and configuration management.

The development of the security awareness programme starts with a review of the security strategies, objectives and policies. This process should be conducted by a team of individuals who are in the position to identify the critical functions of the organization and who have the full support of senior management.

The review team must determine the breakdown of requirements in accordance with the corporate IT security policy. This should be combined with overall security (i.e. not just IT) initiatives and published in various formats such as awareness posters, periodicals, company bulletins, and internal mail.

The team should then conduct specific briefings on security concerns. A thorough review of the requirements should be conducted to build the required information base for the briefings. Each briefing should be conducted at regular time intervals (e.g. every six months) to ensure that all staff are familiar with the risks inherent in modern information technology.

The responsibility for determining the objectives and content of the awareness programme should be allocated at the senior management level to the IT security forum (see ISO/IEC TR 13335-2. The responsibility for its development and implementation should be allocated to the corporate IT security officer and to a security awareness development team. This should be done in conjunction with other corporate training and education activities. However, it is within the responsibility of every individual to review and be intimately familiar with the security policies and procedures of their work environment, hence the security awareness programme should be implemented at all levels of the organization.

To successfully develop a security awareness programme, the following components should be incorporated:

10.2.1 Needs Analysis

To determine the level of awareness already existing within the target groups (executives, management and employees) and the most acceptable methods of conveying new information to them, it is necessary to perform a security knowledge needs analysis. A needs analysis examines policy, procedures, attitudes, security knowledge and desired performance in relation to current actual performance.

10.2.2 Programme Delivery

A comprehensive security awareness programme should include both interactive and promotional techniques. The focus of this part of an awareness programme should be the deficiencies that were identified through the needs analysis. Employees need to gain an appreciation and understanding that IT assets are valuable and that the threats to those are real.

One benefit derived from such an organizational security awareness programme is that it provides employees an opportunity to participate in the security programme. Interactive techniques (staff meetings, training courses, etc.) provide two way communications that allow participants and security personnel to validate the concepts and requirements that resulted from the needs analysis. Promotional techniques (video, E-mail security banners, posters, publications, etc.) are single directional communications methods which allow management to broadcast concepts, information, and attitude in an inexpensive manner.

10.2.3 Monitoring of Security Awareness Programmes

There are two distinct components which comprise effective monitoring of security awareness programmes:

- periodic performance evaluations - which will determine the effectiveness of an awareness programme by monitoring security related behaviour and identify where changes affecting the programme delivery might be required, and

- awareness change management - whenever there are changes to the overall security programme (i.e. policy or strategy changes, new assets or technology are introduced, variations in threats occur, etc.), there will be a need to alter the security awareness programme to update the existing knowledge and skill levels to reflect those changes.

10.3 Security Training

Besides the general security awareness programme, which should apply to everybody within an organization, specific security training is required for personnel with tasks and responsibilities related to IT security. The degree of depth of security training should be dependent on the overall importance IT security has for the organization, and should vary according to the security requirements of the performed roles. If necessary, more extensive education, like participation in university lectures, courses etc., should also be provided. An IT security training programme should be developed to cover all security needs relevant for the organization.

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

- personnel with key responsibilities for the IT system design and development,
- personnel with key responsibilities for IT system operations,
- corporate, IT project, and IT system security officers, and
- personnel with security administration responsibilities, e.g., for access control or directory management.

In addition, a check should be made to see if special security training is required for current and planned tasks, projects, etc. Whenever tasks or projects with special security requirements are started, it should be ensured that the corresponding security training programme is developed before the project starts, and that the activities are carried out in time.

The topics covered by the security training courses should be dependent on the role and function of the person participating. General issues could be:

- what is security,
  - prevention of breaches of confidentiality, integrity, and availability,
  - potential adverse business impacts, for the organization or the individual, and
  - information sensitivity categorization scheme,
- the overall security process,
  - a description of the overall process, and
  - risk analysis components,
- safeguards, and the training necessary to comply with the safeguards,
- roles and responsibilities, and
- IT system security policy.

The correct implementation and use of safeguards is one of the most important issues which should be covered by the security training programme. Each organization should develop its own security training programme according to its needs, and existing or planned safeguards. The following are examples of safeguard related topics which should be covered, with an emphasis on the need for balance between non-technical and technical safeguards:

- security infrastructure,
  - roles and responsibilities,
  - security policy,
  - regular security compliance checking, and
  - security incident handling,
- physical security,
  - buildings,

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

10.4 Approval of IT Systems

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

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

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

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

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

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

- wishes to establish its own tailored version of baseline security or a code of practice and issue it to its suppliers/trading partners for compliance and approval purposes prior to allowing connection to its IT facilities,
- trades with a number of other companies and wishes to be IT connected, but to do so needs to demonstrate an acceptable security profile against baseline security or code of practice as a whole, or
- wishes to establish the levels of security risks associated with other companies connecting to its IT facilities, and the security profile it will expect other companies to meet. This will enable the company to enforce approval on the basis of a security compliance check review indicating compliance with those parts of the baseline security or code of practice consistent with its security profile.

11 Follow-up

Follow-up, even though often neglected, is one of the most important aspects of IT security. The implemented safeguards can only work effectively if they are checked in real business life. It must be assured that they are used correctly, and that any security incidents and changes are detected and dealt with. The prime intent of the follow-up activity is to ensure that security safeguards continue to function as implemented. Over time there is a tendency for the performance of any service or mechanism to deteriorate. Follow-up is intended to detect this deterioration and initiate corrective action. This is the only way to maintain the security levels necessary to protect IT systems. The procedures described in this clause form the basis of an effective follow-up programme. The management of IT security is an ongoing process which does not stop after the implementation of the IT security plan.

11.1 Maintenance

The majority of safeguards will require maintenance and administrative support to ensure their correct and appropriate functioning during their life. These activities (maintenance and administration) should be planned and performed on a regular scheduled basis. In this manner their overhead can be minimized, and the value of the safeguards preserved.

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

Maintenance activities include:

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

The cost of maintenance and administration should always be factored in when assessing and selecting between different safeguards. This is because maintenance and administrative costs can differ widely between one safeguard and the next. Hence, this can often become a significant determinant in the selection of safeguards. Generally speaking, it is desirable to minimize the ongoing maintenance and administrative costs wherever possible as they represent recurring costs rather than one time costs.

11.2 Security Compliance Checking

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

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

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

The safeguards protecting the IT system may be checked by:

- conducting periodic checks, and tests,
- monitoring operational performance against actual incidents occurring, and
- conducting spot checks to check the status of security levels and objectives in particular areas of sensitivity or concern.

To assist the conduct of any security compliance check, valuable information about the activities on an IT system can be obtained from :

- the use of software packages used to record events, and
- the use of audit trails to trace the entire history of events.

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

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

It helps to have a comprehensive checklist and agreed report formats - these are not to be underestimated. These checklists should cover general identification information, e.g. configuration detail, security responsibilities, policy documents, surrounding locale. Physical security should address external aspects, like outside buildings, including accessibility through manhole covers, and internal aspects, like soundness of construction, locks, fire detection and prevention (including alarm aspects), similarly for water/liquid detection, failure of power, etc.

There are many things to detect, such as

- areas open to physical penetration or circumvented controls; for example, wedges under doors which should operate under a keypad and card system, and
- incorrect mechanisms, or incorrect installation of mechanisms, e.g. lack or poor distribution or wrong type of detection facilities. Are smoke/heat detectors plentiful enough for an area, and at the correct height? Is there adequate response to alarms? Are alarms properly linked to a control point? Are there any new sources of danger - someone suddenly using a room to store flammables? Is there adequate power back-up and failure procedures? Are the correct types of cable used and not located near sharp tray edges?

To detect security gaps for other aspects of security, the following questions might be helpful:

- For *personnel security*, watch for the procedures for employment. Are references actually taken? Are employment gaps checked? Are personnel really aware and knowledgeable of security? Is there dependence on one person for a key function?

- For *administrative security*, how are documents really disposed of? Is the documentation in general use actually up-to-date? Are the risk analysis, status check and incident reporting activities actually used as they should? Is the business continuity plan coverage correct, and is it current?

- For *hardware/software security*, is there redundancy at the required level? How good are user id/password selection and procedures? Does the audit trail cover error logging and traceability issues to the right granularity and selection? Does an evaluated product meet the agreed requirement?

- For *communications security*, is the required redundancy there? If there is a dial-up facility, is the requisite equipment and software in place and used properly? If encryption and/or message authentication is required, how effective is the key management system and related operation?

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

11.3 Change Management

IT systems and the environment in which they operate are constantly changing. These changes are a result of the availability of new features and services, or the discovery of new threats and vulnerabilities. These changes can also result in new threats and vulnerabilities. Changes of the IT system include:

- new procedures,
- new features,
- software updates,
- hardware revisions,
- new users to include external groups or anonymous groups, and
- additional networking and interconnection.

When a change to an IT system occurs or is planned, it is important to determine what, if any, impact the change will have on the security of the system. If the system has a Configuration Control Board or other organizational structure to manage technical system changes, the IT system security officer, or his/her representative, should be assigned to the board and be given responsibility to make determinations about whether any change will impact security, and if so how. For major changes that involve the purchase of new hardware, software or service, an analysis will be necessary to determine the new security requirements. On the other hand, many changes made to systems are minor in nature and do not require the extensive analysis that is needed for major changes, but do require some analysis. For both types of change, an analysis that considers the benefits and costs should be made. For minor changes, this can be performed informally at meetings, but the result and management decisions should be documented.

11.4 Monitoring

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

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

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

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

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

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

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

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

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

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

Many safeguards produce output in the form of logs of the occurrence of events. These logs should be analyzed using statistical techniques to permit the early detection of trend changes, and the detection of incidents occurring repeatedly. The responsibilities for the analysis of those logs should be allocated.

In distributed environments, logs may only record information related to a single environment. To truly understand the nature of a complex event, it is necessary to bring together the information from different logs, and fuse them into a single event record. These fused event records should then be subjected to analysis. Event record fusion is a complex task and its most important aspect is the identification of parameter(s) which permit the different log records to be combined with confidence.

The management technique for controlling day to day monitoring is to prepare a security operating procedures document for the necessary activities. This document describes all the actions required to ensure that the level of security for all systems and services is maintained and not compromised as systems and services evolve over time.

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

The procedure for monitoring security safeguards needs to be described. The approach and frequency of security log reviews should be stated. The use of statistical analysis methods and tools should be described. Guidance should be given for how to adjust audit thresholds based on various operational conditions.

11.5 Incident Handling

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

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

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

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

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

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

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

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

- preparation - pre-documented preventive measures, incident handling guidelines and procedures (including for the protection of evidence, maintenance of event logs, and handling public relations), documentation required, and business continuity plans,
- notification - the procedures, means and responsibilities for reporting incidents, and to whom,
- assessment - the procedures and responsibilities for investigating incidents and determining their seriousness,

- management - the procedures and responsibilities for dealing with, limiting the damage from, and eradicating incidents, and notifying higher management,
- recovery - the procedures and responsibilities for re-establishment of normal service,
- review - the procedures and responsibilities for post-incident actions, including investigation of legal implications and trend analysis.

It is emphasised that whilst there is benefit to individual organizations from the use of IAS, some organizations may consider that even more benefit could be accrued from sharing some incident information with others to provide a wider base from which to gain 'alerts', quickly identify trends and enable prevention. To facilitate this an IAS database structure should be used which is flexible enough to cover the range of requirements for total (all sectors, threat types and impacts) and sectorial / threat / impact specific needs. Whether intra or inter organization, each connecting IAS would use similar typology, metrics and structure to record information on incidents. This would allow for comparison and analysis. The use of a common structure is key to the enablement of more comprehensive results, and particularly a more solid base for the rapid identification of 'alerts', in some cases which may not have been identified through individual IAS.

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

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

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

12 Summary

This part of ISO/IEC TR 13335 examined several techniques that are important to the management of IT security. These techniques are based on the concepts and models provided in ISO/IEC TR 13335-1 and the management process and responsibilities discussed in ISO/IEC TR 13335-2. The discussion in this part of ISO/IEC TR 13335 shows the advantages and disadvantages of four possible strategies for risk analysis. The combined approach, and several techniques that are useful for its implementation, are described in detail. Some organizations, particularly small ones, may not be able to implement all the techniques provided in this part of ISO/IEC TR 13335 in exactly the way they are described. It is, however, important that each of these techniques are addressed in a way suitable for the organization.

Annex A

An Example Contents List for a Corporate IT Security Policy

Contents

Annex B

Valuation of Assets

The valuation of an organization's assets is an essential step in the overall risk analysis process. The value assigned to each asset should be expressed in terms which are relevant to the asset and to the business entity involved. To perform the asset valuation, an organization first needs to identify all of its assets. To assure that all assets are accounted for, it is often helpful to group them by type such as information assets, software assets, physical assets, and services. This is also valuable to assign an asset owner who will be responsible for determining the asset's value.

The next step is to agree upon the scale to be used and the criteria for assigning a particular valuation to an asset. Because of the diversity of assets found within most organizations, it is likely that some assets which have a known monetary value will be valued in the local unit of currency while others which have a more qualitative value may be assigned a value ranging for example from "very low" to "very high". The decision to use a quantitative based scale versus a qualitative scale is really a matter of organizational preference, but should be relevant to the assets being valued. Both valuation types could be used for the same asset.

Typical terms used for the qualitative valuation of assets include words such as: negligible, very low, low, medium, high, very high, and critical. The choice and range of terms which are suitable to an organization is strongly dependent on an organization's needs for security, organizational size, and other organization specific factors.

The criteria used as the basis for assigning a value to each asset should be written out in unambiguous terms. This is often one of the most difficult aspects of asset valuation since the values of some assets may have to be subjectively determined and since many different individuals are likely to be making the determinations. Possible criteria used to determine an asset's value include its original cost, its replacement or re-creation cost, or its value may be abstract, e.g., the value of a company's good name or reputation.

Another basis for the valuation of assets is the costs incurred due to the loss of confidentiality, integrity, or availability as the result of an incident. Such a valuation would provide three important dimensions to asset value, in addition to replacement cost, based on estimates of the potential damage or adverse business impact which would result from security incidents with an assumed set of circumstances. It is emphasised that this approach accounts for damage and other impact costs which are necessary to factor into the risk assessment equation.

Many assets may during the course of valuation have several values assigned. For example: a business plan may be valued based on the labour expended to develop the plan, it might be valued on the labour to input the data, and it could be valued based on its value to a competitor. Each of the assigned values will most likely differ considerably. The assigned value may be the maximum of all possible values or may be the sum of some or all of the possible values. In the final analysis, which value or values are assigned to an asset must be carefully determined since the final value assigned enters into the determination of the resources to be expended for the protection of the asset.

Ultimately, all asset valuations need to be reduced to a common basis. This may be done with the aid of criteria such as those that follow. Criteria which may be used to assess the possible damages resulting from a loss of confidentiality, integrity or availability of assets are:

- violation of legislation and/or regulation,
- impairment of business performance,
- loss of goodwill/negative effect on reputation,
- breach associated with personal information,
- endangerment of personal safety,

- adverse effects on law enforcement,
- breach of commercial confidentiality,
- breach of public order,
- financial loss,
- disruption to business activities, and
- endangerment of environmental safety.

These criteria are examples of issues to be considered for asset valuation. For carrying out valuations, an organization needs to select criteria relevant to its type of business and security requirements. This might mean that some of the criteria listed above are nor applicable, and that others might need to be added to the list.

After establishing the criteria to be considered, the organization should agree on a scale to be used organization-wide. The first step is to decide on the number of levels to be used. There are no rules with regard to the number of levels that are most appropriate. More levels provide a greater level of granularity, but sometimes a too fine differentiation makes consistent assignments throughout the organization difficult. Normally, any number of levels between 3 (e.g. low, medium, and high) and 10 can be used as long as it is consistent with the approach the organization is using for the whole risk assessment process.

Also, an organization may define its own limits for asset values, like 'low', 'medium', or 'high'. These limits should be assessed according to the criteria selected, e.g. for possible financial loss, they should be given in monetary values, but when considering endangerment of personal safety, monetary valuation will not be appropriate. Finally, it is entirely up to the organization to decide what is considered as being a 'low' or a 'high' damage - a damage that might be disastrous for a small organization could be low or even negligible for a very large organization.