BS 7799-3:2006

BRITISH STANDARD

Information security management systems –

Part 3: Guidelines for information security risk management

ICS 35.020; 35.040

British Standards

Publishing and copyright information

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

ISBN 0 580 47247 7

The following BSI references relate to the work on this standard:
Committee reference BDD/2
Draft for comment 05/30125021 DC

Publication history

First published March 2006

Amendments issued since publication

Amd. no.	Date	Text affected

Contents

Annexes

List of figures

List of tables

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, pages 1 to 50, an inside back cover and a back cover.

Foreword

Publishing information

This British Standard was published by BSI and came into effect on 17 March 2006. It was prepared by Technical Committee BDD/2, *Information security management.*

Relationship with other publications

This British Standard includes and replaces the existing BS 7799 guidance material provided in the BSI publications PD 3002 and PD 3005.

It is harmonized with other ISO/IEC work, in particular BS ISO/IEC 17799:2005 and BS ISO/IEC 27001:2005 (the revised version of BS 7799-2:2002) to ensure consistency of terminology and methods.

Information about this document

This British Standard provides guidance and support for the implementation of BS 7799-2 and is generic enough to be of use to small, medium and large organizations. The guidance and advice given in this British Standard is not exhaustive and an organization might need to augment it with further guidance before it can be used as the basis for a risk management framework for BS ISO/IEC 27001:2005 (the revised version of BS 7799-2:2002).

As a guide, this British Standard takes the form of guidance and recommendations. It should not be quoted as if it was a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Contractual and legal considerations

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

Compliance with a British Standard cannot confer immunity from legal obligations.

0 Introduction

0.1 General

This British Standard has been prepared for those business managers and their staff involved in ISMS (Information Security Management System) risk management activities. It provides guidance and advice to specifically support the implementation of those requirements defined in BS ISO/IEC 27001:2005 that relate to risk management processes and associated activities. Table E.1 illustrates the relationship between the two documents.

0.2 Process approach

This British Standard promotes the adoption of a process approach for assessing risks, treating risks, and ongoing risk monitoring, risk reviews and re-assessments. A process approach encourages its users to emphasize the importance of:

a) understanding business information security requirements and the need to establish policy and objectives for information security;

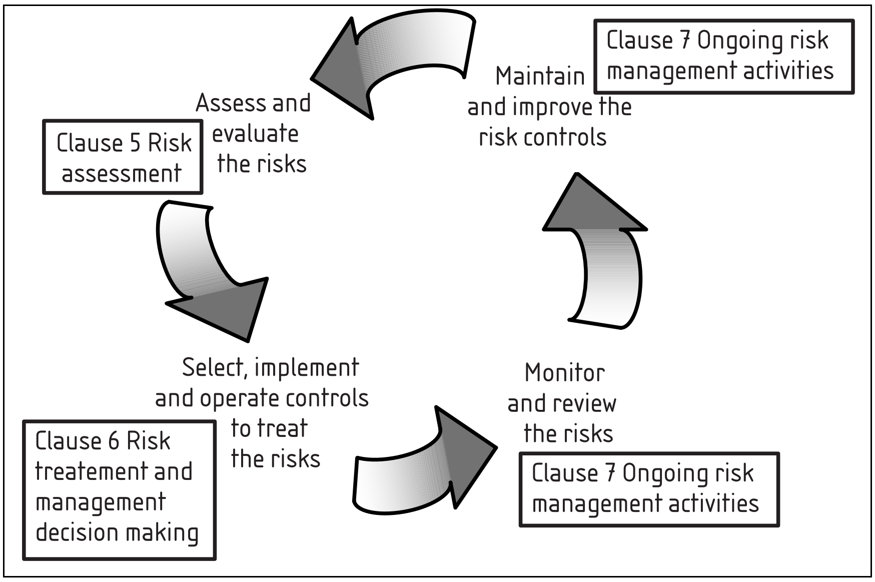
b) selecting, implementing and operating controls in the context of managing an organization's overall business risks;

c) monitoring and reviewing the performance and effectiveness of the Information Security Management System (ISMS) to manage the business risks;

d) continual improvement based on objective risk measurement.

See Figure 1.

Figure 1 **Risk management process model**


Clause 7 Ongoing risk management activities
Maintain and improve the risk controls
Assess and evaluate the risks
Clause 5 Risk assessment
Select, implement and operate controls to treat the risks
Clause 6 Risk treatement and management decision making
Monitor and review the risks
Clause 7 Ongoing risk management activities

This risk management process focuses on providing the business with an understanding of risks to allow effective decision-making to control risks. The risk management process is an ongoing activity that aims to continuously improve its efficiency and effectiveness.

The risk management process should be applied to the whole ISMS (as specified in BS ISO/IEC 27001:2005), and new information systems should be integrated into the ISMS in the planning and design stage to ensure that any information security risks are appropriately managed. This document describes the elements and important aspects of this risk management process.

The information security risks need to be considered in their business context, and the interrelationships with other business functions, such as human resources, research and development, production and operations, administration, IT, finance, and customers need to be identified, to achieve a holistic and complete picture of these risks. This consideration includes taking account of the organizational risks, and applying the concepts and ideas of corporate governance. This, together with the organization's business, effectiveness, and the legal and regulatory environment all serve as drivers and motivators for a successful risk management process. These ideas are described in more detail in Clause **4**.

An important part of the risk management process is the assessment of information security risks, which is necessary to understand the business information security requirements, and the risks to the organization's business assets. As also described in BS ISO/IEC 27001:2005, the risk assessment includes the following actions and activities, which are described in more detail in Clause **5**.

- Identification of assets.
- Identification of legal and business requirements that are relevant for the identified assets.
- Valuation of the identified assets, taking account of the identified legal and business requirements and the impacts of a loss of confidentiality, integrity and availability.
- Identification of significant threats and vulnerabilities for the identified assets.
- Assessment of the likelihood of the threats and vulnerabilities to occur.
- Calculation of risk.
- Evaluation of the risks against a predefined risk scale.

The next step in the risk management process is to identify the appropriate risk treatment action for each of the risks that have been identified in the risk assessment. Risks can be managed through a combination of prevention and detection controls, avoidance tactics, insurance and/or simple acceptance. Once a risk has been assessed a business decision needs to be made on what, if any, action to take. In all cases, the decision should be based on a business case which justifies the decision and which can be accepted or challenged by key stakeholders. The different risk treatment options and factors that influence this decision are described in Clause **6**.

Once the risk treatment decisions have been made and the controls selected following these decisions have been implemented, the ongoing risk management activities should start. These activities include the process of monitoring the risks and the performance of the ISMS to ensure that the implemented controls work as intended. Another activity is the risk review and re-assessment, which is necessary to adapt the risk assessment to the changes that might occur over time in the business environment. Risk reporting and communication is necessary to ensure that business decisions are taken in the context of an organization-wide understanding of risks. The co-ordination of the different risk related processes should ensure that the organization can operate in an efficient and effective way. Continual improvement is an essential part of the ongoing risk management activities to increase the effectiveness of the implemented controls towards achieving the goals that have been set for the ISMS. The ongoing risk management activities are described in Clause **7**.

The successful implementation of the risk management process requires that roles and responsibilities are clearly defined and discharged within the organization. Roles and responsibilities that are involved in the risk management process are included in the document, as relevant.

1 Scope

This British Standard gives guidance to support the requirements given in BS ISO/IEC 27001:2005 regarding all aspects of an ISMS risk management cycle. This cycle includes assessing and evaluating the risks, implementing controls to treat the risks, monitoring and reviewing the risks, and maintaining and improving the system of risk controls.

The focus of this standard is effective information security through an ongoing programme of risk management activities. This focus is targeted at information security in the context of an organization's business risks.

The guidance set out in this British Standard is intended to be applicable to all organizations, regardless of their type, size and nature of business. It is intended for those business managers and their staff involved in ISMS (Information Security Management System) risk management activities.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO/IEC 27001:2005 (BS 7799-2:2005), *Information technology – Security techniques – Information security management systems – Requirements*

3 Terms and definitions

For the purposes of this British Standard, the following terms and definitions apply.

3.1 information security event
an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant [BS ISO/IEC TR 18044:2004]

3.2 information security incident
an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [BS ISO/IEC TR 18044:2004]

3.3 residual risk
risk remaining after risk treatment [ISO Guide 73:2002]

3.4 risk
combination of the probability of an event and its consequence [ISO Guide 73:2002]

3.5 risk acceptance

decision to accept a risk [ISO Guide 73:2002]

NOTE 1 The verb "to accept" is chosen to convey the idea that acceptance has its basic dictionary meaning.

NOTE 2 Risk acceptance depends on risk criteria.

3.6 risk analysis

systematic use of information to identify sources and to estimate the risk [ISO Guide 73:2002]

NOTE 1 Risk analysis provides a basis for risk evaluation, risk treatment, and risk acceptance.

NOTE 2 Information can include historical data, theoretical analysis, informed opinions, and the concerns of stakeholders.

3.7 risk assessment

overall process of risk analysis and risk evaluation [ISO Guide 73:2002]

3.8 risk avoidance

decision not to become involved in, or action to withdraw from, a risk situation [ISO Guide 73:2002]

NOTE The decision may be taken based on the result of risk evaluation.

3.9 risk communication

exchange or sharing of information about risk between the decision-maker and other stakeholders [ISO Guide 73:2002]

NOTE The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

3.10 risk control

actions implementing risk management decisions [ISO Guide 73:2002]

NOTE Risk control may involve monitoring, re-evaluation, and compliance with decisions.

3.11 risk criteria

terms of reference by which the significance of risk is assessed [ISO Guide 73:2002]

NOTE Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

3.12 risk evaluation

process of comparing the estimated risk against given risk criteria to determine the significance of risk [ISO Guide 73:2002]

3.13 risk management

co-ordinated activities to direct and control an organization with regard to risk [ISO Guide 73:2002]

NOTE Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication.

3.14 risk management system

set of elements of an organization's management system concerned with managing risk [ISO Guide 73:2002]

NOTE 1 Management system elements can include strategic planning, decision making, and other processes for dealing with risk.

NOTE 2 The culture of an organization is reflected in its risk management system.

3.15 risk reduction

actions taken to lessen the probability, negative consequences, or both, associated with a risk [ISO Guide 73:2002]

3.16 risk transfer

sharing with another party the burden of loss or benefit of gain, for a risk [ISO Guide 73:2002]

NOTE 1 Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk.

NOTE 2 Risk transfer can be carried out through insurance or other agreements.

NOTE 3 Risk transfer can create new risks or modify existing risk.

NOTE 4 Relocation of the source is not risk transfer.

3.17 risk treatment

treatment process of selection and implementation of measures to modify risk [ISO Guide 73:2002]

NOTE 1 The term risk treatment is sometimes used for the measures themselves.

NOTE 2 Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

NOTE 3 In this British Standard the term "control" is used as a synonym for "measure".

3.18 threat

a potential cause of an incident, that may result in harm to system or organization [BS ISO/IEC 13335-1:2004]

3.19 vulnerability

a weakness of an asset or group of assets than can exploited by one or more threats [BS ISO/IEC 13335-1:2004]

4 Information security risks in the organizational context

4.1 Information security management system scope and policy

4.1.1 Business case

As the implementation of an ISMS requires the deployment of significant resources, all organizations need to be clear about their reasons for implementing such a system. Different organizations will have different business drivers for undertaking the implementation of an ISMS. These drivers will derive from their regulatory or legal position, their status as a large or small business, a publicly-funded or government organization, their geographical location, the type of business they are in, or the service they offer. The business case for implementing an ISMS should be clearly documented, and should set out the likely costs balanced against the benefits that can be derived from an increase in the ability to manage information risk.

The ISMS should not be established in isolation, but should take account of the organizational risks and the overall business strategies in the organization. Annex B explains the relationships between the different types of risk.

4.1.2 ISMS scope

Defining the ISMS scope is one of the most important decisions in the whole process, as the definition of the scope sets the scene for what will be involved in the ISMS. The definition of the scope of the ISMS is entirely up to the organization. The scope of an ISMS can be the whole organization, or suitable part(s) of the organization, or only a specific business process or information system. The scope of the ISMS should be defined in terms of the characteristics of the business, its location, assets and technology (see BS ISO/IEC 27001:2005, **4.2.1** a)), and it should be well defined and complete, addressing the different elements mentioned in BS ISO/IEC 27001:2005.

The decision on the ISMS scope needs to take account of the interfaces and dependencies this ISMS has with other parts of the organization (not within the ISMS scope), other organizations, third party suppliers, or with any other entity outside the ISMS. An example is an ISMS that consists only of a particular business process. In this case, the other parts of the organization that the ISMS needs for its day-to-day functioning (e.g. human resources, finance, sales and marketing or facilities management) are interfaces and dependencies, in addition to all the other interfaces and dependencies that might exist.

The scope of the ISMS should be suitable and appropriate to both the organization's capability and its responsibility to provide information security that meets the requirements determined by its risk assessment and by appropriate legal and regulatory controls. Indeed, such a scope is an absolute necessity for organizations seeking to claim conformity with BS ISO/IEC 27001:2005 (see **1.2** of BS ISO/IEC 27001:2005). Also to claim this conformity nothing should be excluded from the ISMS scope which affects the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by the risk assessment and appropriate regulatory requirements.

4.1.3 ISMS policy

Having determined the scope of its ISMS, an organization should set out a clear and succinct information security policy to support the implementation of information security. BS ISO/IEC 17799:2005 states that the objective of the policy is: "To provide management direction and support for information security." The policy should be approved by management, and it should be ensured that all employees have received the policy and understand its effect on their work. This policy should include a framework for setting objectives, giving management direction and action, and establishing the risk management context and criteria against which risks will be evaluated. Management direction and support is essential because the effective management of information security risk requires the deployment of significant resources.

4.2 Risk approach/philosophy

BS ISO/IEC 27001:2005, **4.2.1** c) requires the organization to identify and adopt a systematic method and approach to risk assessment. It is important that information security risk is managed clearly and consistently throughout an organization. However, managing the risks can employ different risk assessment and management approaches and various degrees of granularity that suit the organization's needs. It is entirely the decision of the organization which risk assessment approach is chosen. Whatever the organization decides on, it is important that the approach to risk management is suitable and appropriate to address all of the organization's requirements.

BS ISO/IEC 27001:2005, **4.2.1** c)–e) sets the framework for the risk assessment approach to be chosen by describing the mandatory elements that the risk assessment process should contain. These mandatory elements are as follows.

- *Determination of the criteria for risk acceptance.* This should describe the circumstances under which the organization is willing to accept the risks.
- *Identification of acceptable levels of risk.* Whatever risk assessment approach is chosen, the levels of risk that the organization considers acceptable need to be identified.
- *Identification and assessment of the risks.* A number of mandatory elements need to be identified and processes carried out, described in more detail in Clause **5** of this document. It is necessary that the risk assessment approach chosen addresses all of the concepts that are discussed in Clause **5**, as listed in **5.1**.

- *Coverage of all aspects of the ISMS scope.* The risk assessment approach chosen needs to cover all control areas in BS ISO/IEC 27001:2005, Annex A. The need for such comprehensive coverage is important, as several risk assessment approaches are in use that concentrate on IT only, and are not suitable for the type of assessment required by BS ISO/IEC 27001:2005.

The risk assessment should achieve a clear understanding of what factors should be controlled, as these factors affect systems and processes that are critical to the organization. Risk management activities should nonetheless be cost-effective and pragmatic. Effective risk management means balancing the expenditure of resources against the required degree of protection and ensuring that the resources expended are correlated with the potential loss and value of the assets protected (**5.4** deals with the valuation of critical information assets).

The chosen approach's level of detail and complexity influence the effort and resources required during the risk assessment process. The risk assessment should be as detailed and complex as necessary to address all of the organization's requirements and what is required for the ISMS scope, but no more. Too much detail might lead to excess work, and a too-high-level view might lead to overlooking important risk aspects. BS ISO/IEC 27001:2005 does not require a highly-technical or detailed approach, as long as all risks are appropriately addressed.

5 Risk assessment

5.1 Risk assessment process

The assessment of information security risks includes risk analysis and risk evaluation, and depends upon the following factors used in these processes. The risk analysis should include:

- identification of assets (see BS ISO/IEC 27001:2005, **4.2.1** d) and **5.2** of this standard);
- identification of legal and business requirements that are relevant for the identified assets (see **5.3**);
- valuation of the identified assets, taking account of the identified legal and business requirements and the impacts resulting from a loss of confidentiality, integrity and availability (see **5.4**);
- identification of significant threats and vulnerabilities for the identified assets (see BS ISO/IEC 27001:2005, **4.2.1** d) and **5.5** of the current standard); and
- assessment of the likelihood of the threats and vulnerabilities to occur (see BS ISO/IEC 27001:2005, Clause **4.2.1** e) and **5.6** of the current standard).

Risk evaluation should include:

- calculation of risk (see BS ISO/IEC 27001:2005, **4.2.1** e)3) and **5.7**); and
- evaluation of the risks against a predefined risk scale (see **5.8**).

5.2 Asset identification

An asset is something that has value or utility for the organization, its business operations and their continuity. Therefore, assets need protection to ensure correct business operations and business continuity. The proper management and accountability of assets[1] is vital, and should be a major responsibility of all management levels.

The important assets within the scope of the ISMS should be clearly identified and appropriately valued (see BS ISO/IEC 27001:2005, **4.2.1** and **5.3** of the current standard), and an inventory of these assets should be put together and maintained. In order to make sure that no asset is overlooked or forgotten, the scope of the ISMS considered should be defined in terms of the characteristics of the business, the organization, its location, assets and technology. Examples of assets and more information about asset identification can be found in **C.1**. Grouping similar or related assets into manageable collections can help to reduce the effort necessary for the risk assessment process.

Accountability for assets helps ensure that adequate information security is maintained. An owner[2] should be identified for each of the identified assets, or groups of assets, and the responsibility for the maintenance of appropriate security controls should be assigned to the owner. Responsibility for implementing security controls may be delegated, although accountability should remain with the nominated owner of the asset.

The asset owner should be responsible for defining the appropriate security classification and access rights for the asset, to agree and document these decisions and to maintain appropriate security controls. It is also the owner's responsibility to periodically review the access rights and the security classifications. In addition, it might be useful to define, document and implement rules for the acceptable use of assets, describing permitted and forbidden actions in the day-to-day use of the asset. The persons using the assets should be aware of these rules as the correct use of the assets is part of their responsibilities.

5.3 Identification of legal and business requirements

5.3.1 Sources of requirement

Security requirements in any organization, large or small, are in effect derived from three main sources and should be documented in the ISMS.

- The unique set of threats and vulnerabilities which could lead to significant losses if they occur (these are considered in **5.5**).
- The legal, statutory and contractual requirements which are applicable to the organization, its trading partners, contractors and service providers.

[1] Clause **7** of BS ISO/IEC 17799:2005 defines two specific objectives with regard to assets: accountability for assets (in **7.1**) and information classification (in **7.2**).

[2] The term "owner" identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets.

- The unique set of principles, objectives and requirements for information processing that an organization has developed to support its business operations and processes, and which apply to the organization's information systems.

Once these legal and business requirements have been identified, it is necessary to consider them in the asset valuation process (see **5.4**) and formulate them in terms of requirements for confidentiality, integrity, and availability.

5.3.2 Legal, regulatory and contractual requirements

The security requirements relating to the set of statutory, regulatory and contractual requirements that an organization, its trading partners, contractors and services providers have to satisfy, should be documented in an ISMS. It is important, e.g. for the control of proprietary software copying, safeguarding of organizational records, or data protection, that the ISMS supports these requirements, and it is vital that the implementation, or absence, of security controls in each of the information systems does not breach any statutory, legal or civil obligations, or commercial contracts. Therefore, the legal statutory and contractual requirements related to each of the assets and to the organization should be identified. More information about legal and regulatory compliance is provided in Annex A.

5.3.3 Organizational principles, objectives and business requirements

The security requirements relating to the organization-wide principles, objectives and requirements for information processing to support its business operations should also be documented in an ISMS. It is important, e.g. for competitive edge, cash flow and/or profitability, that the ISMS supports these requirements, and vital that the implementation, or absence, of security controls in each of the information systems does not impede efficient business operations. For each of the assets and the business activities within the organization, the related business objectives and requirements should be identified.

5.4 Asset valuation

Asset identification and valuation, based on the business needs of an organization, are major factors in risk assessment. In order to identify the appropriate protection for assets, it is necessary to assess their values in terms of their importance to the business or their potential values in different business opportunities. It is also important to take account of the identified legal and business requirements (see **5.3**) and the impacts resulting from a loss of confidentiality, integrity and availability.

One way to express asset values is to use the business impacts that unwanted incidents, such as disclosure, modification, non-availability and/or destruction, would have to the asset and the related business interests that would be directly or indirectly damaged. These incidents could, in turn, lead to loss of revenue or profit, market share, or image and reputation, and these considerations should be reflected in the asset values.

The input for the valuation of assets should be provided by owners and users of assets, who can speak authoritatively about the importance of assets, particularly information, to the organization and its business, and how the assets are used to support the business processes and objectives. In order to consistently assess the asset values, a valuation scale for assets should be defined. More information about asset valuation scales can be found in **C.5.1**.

For each of the assets, values should be identified that express the potential business impacts if the confidentiality, integrity or availability, or any other important property of the asset is damaged. An individual value should be identified for each of these properties as these are independent and can vary for each of the assets.

Information and other assets, as appropriate, should be classified in accordance with the identified asset value, legal or business requirements and criticality (see BS ISO/IEC 17799:2005, Clause **7.2**). Classification indicates the need, priorities and expected degree of protection when handling the information. It should be the responsibility of the asset owner (see also **5.2**) to define the classification, as well as reviewing it to ensure that the classification remains at the appropriate level.

5.5 Identification and assessment of threats and vulnerabilities

5.5.1 Implemented controls

At some point, either prior to starting the risk assessment activities or before starting the identification of threats and vulnerabilities, the already implemented security controls should be identified. This is necessary for a complete identification and realistic valuation of the threats and vulnerabilities, and is also important when considering the risk treatment options and what to do to manage the risks (see also Clause **6**). If this identification of already implemented controls has not yet taken place, it is recommended to do it prior to starting the threat/vulnerability assessment.

5.5.2 Identification of threats and vulnerabilities

Assets are subject to many kinds of threats. A threat can cause an unwanted incident which could result in harm to the organization and its assets. This harm can occur from an attack on the organization's information, e.g. resulting in its unauthorized disclosure, modification, corruption, destruction and unavailability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit one or more vulnerabilities of the systems, applications or services used by the organization in order to successfully cause harm to assets. Threats may originate from within the organization as well as external to it. Examples of threats are given in **C.2** and **C.3**.

Vulnerabilities are security weaknesses associated with an organization's assets. These weaknesses could be exploited by one or more threats causing unwanted incidents that might result in loss, damage or harm to these assets and the business of the organization. The vulnerability in itself does not cause harm, it is merely a condition or set of conditions that might allow a threat to exploit it and cause harm to the assets and the business they support. The vulnerability identification should identify the weaknesses related to the assets in the:

- physical environment;
- personnel, management and administration procedures and controls;
- business operations and service delivery;
- hardware, software or communications equipment and facilities.

Examples of vulnerabilities are given in **C.4**.

It should be noted that threats and vulnerabilities need to come together to cause incidents that might damage the assets. It is therefore necessary to understand the relationship between threats and vulnerabilities, i.e. which threat might exploit which of the vulnerabilities.

5.6 Assessment of the threats and vulnerabilities

After identifying the threats and vulnerabilities it is necessary to assess the likelihood that they will come together and cause a risk. This includes assessing the likelihood of threats occurring, and how easily vulnerabilities can be exploited by the threat. More information about the valuation scales that can be used for the assessment of threats and vulnerabilities is contained in **C.5.2**.

The assessment of the likelihood of threats should take account of the following.

- *Deliberate threats.* The likelihood of deliberate threats depends on the motivation, knowledge, capacity and resources available to possible attackers, and the attractiveness of assets to sophisticated attacks.
- *Accidental threats.* The likelihood of accidental threats can be estimated using statistics and experience. The likelihood of these threats might also be related to the organization's proximity to sources of danger, such as major roads or rail routes, and factories dealing with dangerous material such as chemical materials or petroleum. Also the organization's geographical location will affect the possibility of extreme weather conditions. The likelihood of human errors (one of the most common accidental threats) and equipment malfunction should also be estimated.
- *Past incidents*. That is, incidents that have taken place in the past, which illustrate problems in the current protective arrangements.
- *New developments and trends*. This includes reports, news and trends obtained from the Internet, news groups or other organizations that help to assess the threat situation.

Based on this assessment and based on the scale that has been chosen for the threat and vulnerability assessment (see **C.5.2**), the likelihood of the threats occurring should be assessed. The overall likelihood of an incident occurring also depends on the vulnerability of the assets, i.e. how easily the vulnerability could be exploited. Vulnerabilities should also be rated using the appropriate vulnerability valuation scale (see **C.5.2**).

Information used to support the assessment of threat and vulnerability likelihood is best obtained from those directly involved with the business processes at risk. It might also be useful to use threat and vulnerability lists (e.g. in **C.2, C.3** and **C.4**) and links between threats and controls from BS ISO/IEC 17799:2005 given in Annex C.

5.7 Risk calculation and evaluation

The objective of the risk assessment is to identify and assess the risks, based on the results of **5.2** to **5.6**. The risks are calculated from the combination of asset values expressing the likely impact resulting from a loss of confidentiality, integrity and/or availability, and the assessed likelihood of related threats and vulnerabilities to come together and cause an incident.

It is up to the organization to identify a method for risk assessment that is most suitable for its business and security requirements. The calculated levels of risk provide a means to rank the risks and to identify those risks that are most problematic for the organization.

There are different ways of relating the values assigned to the assets, and those assigned to the vulnerabilities and threats to obtain measures of risks. **C.5.3** and **C.5.4** give examples of how risks might be calculated based on these factors. Common aspects of all these different methods of calculating the risk are as follows.

A risk has two contributing factors, one expressing the impact if the risk occurred, and one expressing the likelihood that the risk might occur.

The impact factor of the risk is based on the asset valuation. The impact factor can be derived from the asset valuation in different ways, though care should be taken to ensure that this is done consistently within an organization. Two examples are to:

- distinguish between risks for confidentiality, integrity and availability using the respective asset value as the impact value, therewith considering three different risks for each asset;
- combine[3)] the three asset values that have been assessed into one, e.g. by using the maximum or the sum of these three values.

The likelihood factor of the risk is based on the threats and vulnerabilities, and the values that have been assessed for them. The threat and vulnerability values can be used in different ways, e.g.

- adding or multiplying the threat and the vulnerability value and using the combined[3)] value;
- not combining the threat and vulnerability value and using them individually, as for example shown in **C.5.3**.

[3)] When combining asset, threat or vulnerability values, care should be taken that no important information gets lost.

How the two contributing factors (the impact and the likelihood value) are combined to calculate the risk is up to the organization and the particular risk assessment method chosen. The only thing that needs to be ensured is that the risk level increases if any of these contributing factors increase.

The next part of the risk evaluation is to compare the calculated levels of risk with the risk level scale that was defined when the risk assessment method was selected. The risk levels should be expressed in terms of loss for the business and recovery time, such as "serious damage for the organization's business, from which the organization cannot recover in less than half a year". Relating the risk levels to the organization's business is necessary to realistically assess the impact the calculated risks have on the organization's business and helps to convey the meaning of the risk levels to management.

This risk evaluation should also identify the generally acceptable risk levels, i.e. those risk levels where the estimated damage is small enough for the organization to cope with in continuing their day-to-day business, and where therefore further action is not necessary. All other risks require further action and should be subject to the risk treatment and management decision making discussed in Clause **6**.

The results of the risk assessment process (i.e. the results of the processes described in **5.2, 5.3, 5.4, 5.5, 5.6** and **5.7**) should be documented in a risk assessment report (see also BS ISO/IEC 27001:2005, **4.3.1**).

5.8 The risk assessor

The person who performs the information security risk assessments should have the following characteristics:

- a basic understanding of how the business works and the risk appetite of the business;
- an understanding of the basic concepts of risk, e.g. how ratings of threat, vulnerability and impact come together to give a risk value;
- an understanding of IT to a sufficient level to enable IT threats and vulnerabilities to be understood, e.g. what hosts, workstations, storage devices, operating systems, applications, communication networks, websites, viruses, and worms are and how they work and inter-relate;
- an understanding of the different types of security controls, how they work and any limitations, e.g. firewalls, intrusion detection systems, identification and authentication mechanisms, access controls, encryption, CCTV, and logging and monitoring;
- a practical understanding of a suitable risk assessment method and any associated tools, software or forms;
- analytic abilities, i.e. able to isolate what is relevant;
- the ability to identify the people in the organization who will be able to provide the necessary information;
- sufficient interpersonal skills to obtain the necessary information from the people in the organization and to communicate the results of the risk assessment in a way that is easily understood by decision-making management.

The risk assessor might be an information or IT professional, a security or information security professional, a business person from within the business, or an external security consultant.

6 Risk treatment and management decision-making

6.1 General

Risks can be managed through a combination of prevention and detection controls, avoidance tactics and acceptance, or by transference to another organization. This clause discusses each of these approaches, together with useful decision-making processes for determining an appropriate approach to treating the risk.

6.2 Decision-making

Once a risk has been assessed a business decision needs to be made as to how the risk is to be treated. Different business circumstances will dictate what kind of decision is made. For example, a new technology based start-up business might accept higher risks than a traditional, well-established organization.

The two main factors that might influence the decision are:

a) the possible impact if the risk is realized, i.e. the cost each time it happens;

b) how frequently it is expected to happen.

These will give an indication of the loss that might be expected to occur, if nothing is done to mitigate the assessed risk. Information security risks can be difficult to quantify in terms of the probability of occurrence due in part to the lack of publicly available statistics on frequency of occurrence. The decision makers should therefore carefully judge the accuracy and reliability of the information upon which they are making a decision and the degree of loss which they are willing to accept.

In addition to considering estimated losses from security incidents (**5.7**), the organization will need to consider the cost of acting on the risk treatment decision. For example, the investment needed to implement an appropriate set of control objectives and controls as opposed to doing nothing, and the potential cost to the organization if something goes wrong. An organization needs to ensure that it achieves the right balance between achieving security and the benefits of protection, at the right investment, whilst staying profitable, successful, efficient and competitive.

Other factors that might also influence the risk management decision making process are:

- the willingness to accept risks (also known as the risk tolerance or appetite for risk);
- the ease of implementation of control;
- the resources available;
- the current business/technology priorities;
- organizational and management politics.

6.3 Reduce the risk

For all those risks where the option to reduce the risk has been chosen, appropriate controls should be implemented to reduce the risks to the level that has been identified as acceptable, or at least as much as is feasible towards that level. In identifying the level of controls it is important to consider the security requirements related to the risks (i.e. the threats and vulnerabilities, legal and business requirements), and all other results from the risk assessment. Controls can reduce the assessed risks in many different ways, for example by:

- reducing the likelihood of the vulnerability being exploited;
- reducing the possible impact if the risk occurs by detecting unwanted events, reacting, and recovering from them.

Which of these ways (or a combination of them) an organization chooses to adopt to protect its assets is a business decision and depends on the business requirements, the environment and the circumstances in which the organization needs to operate. It is always important to match the controls to the specific needs of an organization, and to justify their selection.

There is no universal or common approach to the selection of control objectives and controls. The selection process is likely to involve a number of decision steps, consultation and discussion with different parts of the business and with a number of key individuals, as well as a wide-ranging analysis of business objectives. The selection process needs to produce an outcome that best suits the organization in terms of its business requirements for the protection of its assets and its investment, its culture and risk tolerance. It needs to be based on a clearly defined set of business goals and objectives or a mission statement.

Controls can be selected from BS ISO/IEC 17799:2005 or BS ISO/IEC 27001:2005, Annex A, and also from additional sources, as and when necessary. This selection should be supported by the results of the risk assessment, for example, the results of vulnerability and threat assessment might indicate where protection is needed, and what form it should take. Any such links to the risk assessment should be documented to justify the selection (or otherwise) of the controls. Documenting selected controls, together with the control objectives that they seek to achieve, in a statement of applicability is important in supporting certification and also enables the organization to track control implementation and continued effectiveness. Further guidance on the statement of applicability can be found in BS ISO/IEC 27001:2005, Clause **4**.

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

- ease of use of the control;
- the reliability and repeatability of the control (whether formally structured or ad-hoc, and whether performed manually or programmed);
- the relative strength of the controls; and
- the types of functions performed (prevention, deterrence, detection, recovery, correction, monitoring, and awareness).

6.4 Knowingly and objectively accept the risk

It is likely that some risks will exist for which either the organization cannot identify controls or for which the cost of implementing a control outweighs the potential loss through the risk occurring. In these cases, a decision may be made to accept the risk and live with the consequences if the risk occurs. Organizations should document these decisions, so that management is aware of its risk position, and can knowingly accept the risk.

All key stakeholders should be made aware of, and agree to accept, the risk. When making a decision to accept a risk, it is therefore important that individuals with differing perspectives are consulted and as much reliable information as possible is gathered. Different perspectives might be obtained from individuals from outside of the organization from other industries, or perhaps from within the organization from other functions or other geographical locations. Wider consultation can avoid possible bias in decision-making or group-think whereby all the individuals within a decision group are blinded to specific facts or elements of the risk.

Where a risk is accepted as being the worst-case the consequences of the risk occurring should be evaluated and discussed with the key stakeholders to gain their acceptance. This could, for example, mean that a risk is deemed to be highly unlikely to occur but, if it occurred, the organization would not survive. When taking this type of risk, management might need to consult with key owners, shareholders, government agencies, suppliers and/or customers who might be affected in this worst case scenario in order to gain their acceptance of the risk. Once again, the discussion process and outcome of these discussions should be documented so that any doubt over the decisions and the outcome can be clarified and to ensure that responsibilities for accepting risks are clearly allocated. The outcome of such discussions may be documented in the statement of applicability.

Where such a risk is deemed to be unacceptable by key stakeholders, but too costly to mitigate through controls, the organization could decide to transfer the risk.

6.5 Transfer of the risk

Risk transfer is an option where it is difficult for the company to reduce or control the risk to an acceptable level or it can be more economically transferred to a third party.

There are several mechanisms for transferring risk to another organization, for example, the use of insurance. Insurers in consideration of a premium can provide this after all the relevant underwriting information is supplied (insurance is where an indemnity is provided if the risk occurs that falls within the policy cover provided).

However, even with insurance there is still an element of residual risk because there will be conditions and exclusions which will be applied dependent on the type of occurrence for which an indemnity is not provided. Transfer of risk by insurance needs to be analysed to identify how much of the actual risk is being transferred. Generally, insurance does not mitigate non-financial impacts and does not provide immediate mitigation in the event of an incident.

Another possibility is to use third parties or outsourcing partners to handle critical business assets or processes if they are suitably equipped for doing so. In this case, care should be taken to ensure that all security requirements, control objectives and controls are included in associated contracts to ensure that sufficient security will be in place. In addition, it is advisable to specify the security activities that should be undertaken in service levels, together with specific performance measures, so that activity and performance can be measured. What should be kept in mind is that residual risk is again present in that the ultimate responsibility for the security of the outsourced information and information processing facilities remains with the original organization, and that through the act of outsourcing, new risks may be introduced which will need to be assessed and managed by the organization undertaking the outsourcing.

6.6 Avoid the risk

Risk avoidance describes any action where the business activities or ways to conduct business are changed to avoid any risk occurring. For example, risk avoidance can be achieved by:

- not conducting certain business activities (e.g. not using e-commerce arrangements or not using the Internet for specific business activities);
- moving assets away from an area of risk (e.g. not storing sensitive files in the organization’s Intranet or moving assets away from areas that are not sufficiently physically protected); or
- deciding not to process particularly sensitive information, e.g. with third parties, if sufficient protection cannot be guaranteed.

Risk avoidance needs to be balanced against business and financial needs. For example, it might be inevitable for an organization to use the Internet or e-commerce because of business demands, despite any concerns about hackers, or it might be not feasible from a business process point of view to move certain assets to a safer place. In such situations, one of the other options, i.e. risk transfer or risk reduction, should be considered.

6.7 Residual risk

After the risk treatment decision(s) have been implemented, there will always be risks remaining. It should be assessed how much the risk treatment decisions help to reduce the risk, and how much of a residual risk remains. This residual risk can be difficult to assess, but at least an estimate should be made to ensure that sufficient protection is achieved.

If the residual risk is unacceptable, a business decision needs to be made about how to resolve this situation. One option is to identify different risk treatment options, or more controls, insurance arrangements, etc. to finally reduce the risk to an acceptable level. Whilst it is generally good practice not to tolerate unacceptable risks, it might not always be possible or financially feasible to reduce all risks to an acceptable level. In these circumstances, it might be necessary to knowingly and objectively accept the risk. The accepted residual risks should be documented and approved by management.

6.8 Risk treatment plan

Once the risk treatment decisions have been taken, the activities to implement these decisions need to be identified and planned. Each implementation activity should be clearly identified and broken into as many sub-activities as are needed to be able to allocate clear responsibilities to individuals, estimate resource requirements, set milestones and deadlines, identify deliverables and monitor progress.

The planning process needs to include the identification of key stakeholders such as resource owners and a consultation process to ensure that resource requirements are properly estimated and can be made available, and that the relevant levels of management approval to spend the resources have been obtained.

The time when each activity can be undertaken depends on the overall priority in relation to the other activities in the programme, the resource availability (including consideration of funding and availability of people) and whether it is dependant on any other activity to be completed before the process can be started. Other business and IT change programmes of work will usually have to be carefully co-ordinated with the risk treatment plan to ensure that any dependencies are identified and taken into account.

Prioritising activities is a management function and is usually closely aligned with the risk assessment activity discussed in Clause **5**. Priorities for action are usually set to ensure that activity is focused on the largest risks, though other political processes might also influence these priorities, such as the need to demonstrate quick wins to senior management.

In summary, the following activities need to be undertaken when formulating a risk treatment plan.

- Limiting factors and dependencies should be identified.
- Priorities should be established.
- Deadlines should be identified and milestones should be agreed.
- Resource requirements should be estimated and resources identified.
- Approvals to spend or allocate resources should be obtained.
- The critical path should be identified.

Once the risk treatment plan has been formulated, resources can be allocated and activity to implement the risk management decisions can be started. It is necessary at this stage to ensure that there is a clear review process in place to ensure that activity is undertaken as planned, that deliverables are of the desired quality, that milestones are met and that resource estimates are not exceeded (see also **7.3**).

7 Ongoing risk management activities

7.1 Ongoing security risk management

Management of security risk is an ongoing activity that should be assigned to an individual or a team within the organization (BS ISO/IEC 27001:2005, **5.1**). As part of a contractual arrangement an outsourcing business partner may manage some of the risk, however, responsibility for risk management as a whole should remain in-house. For a small organization responsibility may be taken by a single individual as part of a job portfolio. In most organizations a security manager with responsibility for the ISMS should be clearly identified.

The person or team that manages security risk should have the following characteristics.

- Systematic and organized in their approach to monitoring known risks and suggesting appropriate action.
- Business-focused and aware of the current state of the business and its priorities.
- Tenacious and independently-minded but able to see opposing points of view and accommodate them if it is best for the business.
- Able to present a case in convincing manner (e.g. a case for expenditure to reduce a high risk);
- Able to communicate at all levels in the organization;
- Having a good understanding of risk, and security technology and measures.

7.2 Maintenance and monitoring

Implemented security controls should be regularly monitored and reviewed to ensure that they function correctly and effectively and that changes in the environment have not rendered them ineffective (see also BS ISO/IEC 27001:2005, Clause **4.2.3**). Over time there is a tendency for the performance of any service or mechanism to deteriorate. Monitoring is intended to detect this deterioration and initiate corrective action.

The majority of security controls will require maintenance and administrative support to ensure their correct and appropriate functioning during their life. These activities should be planned and performed on a regular, scheduled basis. In this manner their overhead can be minimized, and the relevance of the security controls preserved. Maintenance activities include:

- the checking of log files;
- modifying parameters to reflect changes and additions;
- reviewing controls and the compliance with them;
- updating controls, policies and procedures with new versions.

Many controls produce an output that should be checked for security significant events e.g., logs, alarm reports, incident management reports, vulnerability management processes, and application reviews. General system audit functions can provide useful information, which can be used in this regard. Automated review and analysis of system logs or a secondary human review is an effective tool for helping to ensure the intended performance.

7.3 Management reviews

Management needs to review the ISMS to ensure its continuing suitability, adequacy and effectiveness. In order to ensure the adequacy of the ISMS, management needs to consider the changing risk situation and the ability of the ISMS to deal with these changed risks. The scope of the ISMS might require redefinition due to changed business objectives or other important modifications. Regular management reviews should take place. Organizations should tune the ISMS by reviewing appropriate targets and metrics. Either qualitative or quantitative targets could be appropriate depending on the nature of the ISMS.

Reviews should be based on information from users of the ISMS, results from previous reviews, audit reports, records of procedures, and internal and external benchmarking. The output of the review should be specific about changes to the ISMS, for example by identifying modifications to procedures that affect information security, and to ensure adequacy of coverage. The output should also show where efficiency improvements can be made. The review should be clear about required resources, both to implement the improvements and to maintain them.

7.4 Risk reviews and re-assessments

The results from an original security risk assessment and management review need to be regularly reviewed for change. There are several factors that could change the originally assessed risks. Any new business function could mean new or changed information assets, and any changes documented and considered in the risk assessment and management process. Other changes in the risk situation might occur from review of the organization, business objectives and/or processes, a review of the correctness and effectiveness of the implemented security controls, and external changes (e.g., environmental, social and political). New or changed threats and/or vulnerabilities may also be identified.

After all these different changes have been taken into account, the risk should be re-calculated and necessary changes to the risk treatment decisions and security controls identified and documented. These changes should be agreed with management and implemented.

A risk register should be maintained that includes the date of the last assessment, a description of the risk, an estimate of the impact and the likelihood, any mitigating controls, and a statement of action required, with target date and owner. A maintained risk register provides a useful vehicle for communication (see also **7.8**).

7.5 Audits

Regular internal audits should be scheduled and should be conducted by an independent party (BS ISO/IEC 27001:2005, Clause **6**). The independent party does not need to be from outside the organization. However, audits by an external body are essential for certification under BS ISO/IEC 27001:2005. Internal auditors should not be under the supervision or control of those responsible for the implementation or daily management of the ISMS. Where internal audits discover a need for actions to be taken to adjust the ISMS these should be fully documented, responsibility should be assigned and a target date determined.

7.6 Documentation controls

Complete, accessible and correct documentation and a controlled process to manage documents are necessary to support the ISMS, although the scope and detail will vary from organization to organization. Responsibility for overseeing the process of managing documentation needs to be clearly assigned and agreed.

Documentation includes policies, standards, guidelines, procedures, checklists, the risk register and other guidance in support of the ISMS. A list of required documentation can be found in BS ISO/IEC 27001:2005, **4.3.1**. These documents, and any other documentation and records that are necessary to operate the ISMS and to provide evidence that the ISMS is operating correctly and efficiently should be maintained, and these documents should be current and relevant. Some documentation which is relevant to enforcing the ISMS controls will be owned by functions other than information security. Documentation controls which apply to the ISMS should also apply equally to security documentation which is embedded somewhere outside the ISMS.

The requirements for documentation and record control are contained in BS ISO/IEC 27001:2005, **4.3.2** and **4.3.3**. These requirements are directly aligned with the documentation requirements of other management systems, such as BS EN ISO 9001. These aligned requirements help to combine different management systems and to consistently apply necessary documentation control. Effective document control also supports consistent dissemination of information, whilst removing the potential for confusion over the state of the ISMS at any point.

7.7 Corrective and preventative action

Action should be taken as a result of monitoring, reviews and audits (BS ISO/IEC 27001:2005, **8.2**, **8.3**). These actions need to be independently verified to ensure that they:

- relate to the identified root cause and appropriately address the problem;
- have actually been implemented;
- are effective in preventing recurrence of the problem.

The verification evidence needed might require a repetition of the "Plan-Do-Check-Act" cycle. Thus an accurate picture of the efficacy of corrective and preventative action will be built over time.

7.8 Reporting and communications

7.8.1 Communication plan

An ISMS requires co-operation with, and input by all levels and functions of an organization (BS ISO/IEC 27001:2005, **7.2**). Effective risk reporting and communications are therefore essential.

A communication plan should be established, which identifies key players and decision-makers as well as mechanisms for disseminating decisions and for collecting feedback (see **7.8.2**). The plan should include mechanisms for regular updating of risk information as part of the ongoing security awareness programme. It should also include procedures for dealing with public relations issues that might arise from publicity about security incidents.

7.8.2 Feedback and involvement

Feedback is an essential ingredient in making an ISMS more effective. The aim is to ensure that the ISMS becomes part of the organizational culture. Identification and reporting of problems, increased risks and security incidents should be encouraged. Effective suggestions for remediation strategies should be rewarded. These should be collected and evaluated systematically. For example, an employee suggestion form can be used. The following suggests how a feedback and involvement process should be conducted.

- Use a suggestion form that is simple and easy to complete.
- Define a clear scope for suggestions focusing on the ISMS and related business activities.
- Identify contacts for suggestions, questions and queries.
- Acknowledge all input.
- Keep an open mind and be flexible about suggestions.
- Involve the person who made the suggestion in the problem solving process, where possible.
- Provide a reward system for useful input.
- Implement suggested improvements quickly and effectively.
- Publicise successful improvements.
- Issue periodic reminders about the improvement process.

An effective ISMS needs to draw information from all possible sources, including management and all employees and contractors, irrespective of their function, as well as people from outside such as outsourcers, suppliers and customers, where relevant. Participating in the ISMS improvement process should be part of every employee's job description.

7.9 The security risk manager

Management of security risk is an ongoing activity that should be assigned to an individual or a team within the business or to an outsourcing business partner as part of a contractual arrangement. For a small organization it might be one of a number of responsibilities for an individual. For a large organization the responsibility may be the shared full time activity of a team. It could be the responsibility of a security manager.

The person or team that manages security risk should have the following characteristics.

- Systematic and organized in their approach to monitoring known risks and suggesting appropriate action.
- Business-focused and aware of the current state of the business and its priorities.
- Tenacious and independently-minded but able to see opposing points of view and accommodate them if it is best for the business.
- Able to present a case in a convincing manner, e.g. a case for expenditure to reduce a high risk.
- Able to work at all levels in the organization.
- A good understanding of risk, technology and security controls.

Annex A (informative) Examples of legal and regulatory compliance

A.1 General

Organizations increasingly face the need to comply with a range of legislation and regulation that has an impact on their management of information. There are four main drivers for this.

- *National security.* This is as a result of the increase in global terrorism.
- *Corporate governance.* This is as a result of high-profile failures of corporate governance.
- *Electronic commerce.* This is as a result of the need to ensure the development of trust in on-line trading.
- *Identity theft and data protection.* This is as a result of apparent lapses in corporate security that have resulted in exposing consumers to identity theft or caused data protection problems.

Other drivers can be health and safety, making provision for employees and customers with disabilities, intellectual property, the need to protect tax revenue and the need to avoid discrimination in employment. The intention of such legislation and regulation is to ensure that organizations put in place effective mechanisms for controlling and auditing the flow of information (personal, financial and operational) through their establishment. Most legislation and regulation of this kind sees risk assessment as an essential element of these effective control mechanisms.

A.2 Legal framework

Making sense of the increasing number of legal and regulatory instruments requires a clear framework that reflects and simplifies their main purpose. For this reason, legal and regulatory instruments are considered as falling into one of six groups based on shared functionality. The first four groups result from the drivers mentioned earlier in this annex:

- national security;
- corporate governance;
- electronic commerce and the civil and criminal legal framework;
- identity theft and data protection.

The other two groups deal with legislation and regulation that relates to:

- intellectual property protection; and
- sector (industry)-specific provisions.

In this annex each of these groups is explained in more detail, and examples are given of appropriate legislation and regulations from Europe and North America, as these are the instruments that are of primary interest to UK organizations (although such changes are occurring world-wide and should be monitored, if of interest).

A.3 National security

A.3.1 General

National Security provisions are intended to protect citizens from threats to the critical national infrastructure arising from perils such as terrorists (however motivated), state-sponsored intervention, or natural disaster.

A.3.2 Europe

European provisions in this area tend not to involve statutory instruments. Most governments have an agency, or agencies that are tasked with the protection of the critical national information infrastructure (such as the Network Infrastructure Security Co-ordination Centre (NISCC) in the UK). In 2004 the EU set up the European Network Information Security Agency (ENISA).

A.3.3 North America

The USA has given the Department of Homeland Security (DHS) overall responsibility for protecting the critical national infrastructure, and has implemented a number of statutory instruments, tasked industry organizations or government agencies to deal with some aspects of the task. These include:

- Federal Information Security Management Act (FISMA) [1];
- USA Patriot Act (USAPA) [2];
- North American Electric Reliability Council;
- Federal Energy Regulatory Commission.

A.4 Corporate governance

A.4.1 General

Legislation and regulation in this area is primarily directed at publicly traded companies, requiring them to demonstrate due diligence in the disclosure of financial information, to manage their operational risk transparently and to implement a series of internal controls and procedures that will enable them to do so. The intent here is to assure potential and current investors that they can justifiably rely on the records of the business to present a true picture of the organization.

A.4.2 Europe

In Europe corporate governance has, in general, been seen as an issue that is dealt with through regulations such as the Combined Code for Internal Control (Turnbull) [3], for companies quoted on the London Stock Exchange (LSE); the Basel II operation risk control provisions for banks that trade internationally; and the “Financial Services Authority (FSA) Handbook” for Banks and Financial Services Organizations in the UK [4]. However, control of audit processes has become part of statutory law in the UK with the 2004 Companies (Audit, Investigation and Community Enterprise) Act [5]. The legislation and regulation’s intent is to assure potential and current investors that they can rely on published financial statements of the business to present a true picture.

A.4.3 North America

In the USA[4] the Sarbanes-Oxley Act (SOX) [6] has put corporate governance on a strong statutory footing, by holding corporate officers personally liable for improprieties with penalties of imprisonment for CEOs and CFOs in the event of non-compliance.

A.5 Electronic commerce, legal framework

A.5.1 General

The legislation under this heading is that which is intended to govern the use of information technology and networked systems, particularly in order to increase trust in online transactions. For example:

- use of electronic records and electronic signatures;
- creation, modification, storage and transmission of electronic data; and
- criminal misuse of computers and IT systems.

A.5.2 Europe

Most countries in Europe have an equivalent of the UK's Computer Misuse Act [7]. The EU has been active in considering the legal framework in this area and examples include:

- Electronic Signatures Directive [8];
- Consumer Protection and Distance Selling Directive [9];
- Directive on Privacy and Electronic Communications [10];
- Council of Europe, Convention on CyberCrime.

A.5.3 North America

The USA has been less active in this area. Implementation has been sector-specific. For example, the Food and Drug Administration (FDA) provisions governing the use of Electronic Records and Signatures in the pharmaceutical industry (21CFR11) [11]. The Securities and Exchange Commission (SEC) has been active in the area of document life cycle management and has proffered US federal regulations which have been adopted by several states as well.

A.6 Identity theft, data protection

A.6.1 General

Instruments in this area are intended to identify the rights and obligations of individuals and organizations with respect to the collection, use, retention and disclosure of personal information. Notification in the event of inappropriate disclosure is required.

[4] Note that SOX applies to any company that is publicly-listed in the USA, which may include companies headquartered elsewhere.

A.6.2 Europe

In the European Union all countries have implemented national legislation on the basis of the European Union Data Protection Directive [12].

A.6.3 North America

Canada has adopted an approach similar to that of the European Union with the Personal Information Protection and Electronic Document Act (PIPEDA) [13].

In the USA a piecemeal approach has been adopted. Privacy legislation has been directed at specific areas, such as:

- Gramm-Leach-Bliley Act (GLBA) [14];
- Health Insurance Portability and Accountability Act (HIPAA) [15].

Or it has been targeted at specific types of crime, for example:

- California Security Breach Information Act (Senate Bill No. 1386) (targeted at identity theft) [16];
- Children's Online Privacy Protection Act (COPPA) [17];
- Family Educational Rights and Privacy Act (FERPA) [18].

A.7 Intellectual property protection

Legislation under this heading is intended to protect the intellectual property of individuals and organizations, such as trade secrets and patentable ideas. All countries have some form of trade secret, copyright and patent law.

A.8 Sector-specific

Sector-specific regulations are those targeted at specific industries, intended to control aspects of their operation that are unique to that sector and that might impinge on their security, or the security of the wider public. Examples include the FDA provisions for pharmaceutical companies and data retention laws that affect telecommunications providers and ISPs. The regulations applicable to credit card companies also apply to organizations dealing with these companies.

Sector-specific regulations are very important to many organizations, but because they are so widely varied, they are not discussed in detail here. Organizations should determine which sector-specific regulations are relevant in the jurisdictions in which they operate, and factor them into the risk evaluations.

Annex B (informative) Information security risks and organizational risks

B.1 Organizational processes and interrelationships

B.1.1 General

All organizations should be aware of the need to manage information security risks. Viruses, distributed denial of service attacks, and the potential for system and network compromise could be seen as purely an IT issue. However, the ubiquitous nature of communications and information technologies means that the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [19] states the need for "... much greater emphasis on security by governments, businesses, other organizations and individual users who develop, own, provide, manage, service, and use information systems and networks". This greater emphasis is reflected in worldwide regulatory and legal instruments that place requirements on organizations to improve the management of the confidentiality, availability and integrity of their information throughout the business process. As a result, all businesses that use any form of information processing facilities, such as IT or the Internet, have a significant role to play in the management of information security.

Organizations of any size have a number of processes, some internally-facing and some externally-facing. In small organizations a number of these processes could be carried out by the same team or even the same person (see also the relationship between roles and responsibilities for organizational processes and assets described in Annex D). As information risk assessment is a responsibility of the whole organization, all parts of a business need to identify the information assets that are critical to their ability to function, and should ensure that the related risks are assessed and the appropriate security controls are implemented and maintained to manage the identified risks. However, certain risks are specific to certain types of organizational processes, and examples of these are described later in this annex.

B.1.2 Externally-facing organizational processes

Risks specific to particular externally-facing organizational processes are as follows.

- *Sales and marketing*. These activities are a vital interface between an organization and the public. In any organization, there is potential risk from failure to protect the confidentiality of sensitive information during sales and marketing operations and of damaging the reputation of the organization through failure to ensure the accuracy and availability of information.
- *Production and operations*. Information used by the production and operations processes needs to be highly accurate and consistent, and available when required. The risks of failure should be clearly identified and addressed for those assets that are critical to the production and operations processes.
- *Customer service*. This process requires accurate information that is available when required. The consequences of failure are damage to the reputation of the organization, and consequent loss of business.

B.1.3 Internally-facing organizational processes

Risks specific to particular internally-facing organizational processes are as follows.

- *Human resources*. Information security risk is inherent in the interaction between employees and information systems. All employees therefore have a significant role in the risk situation of the organization, which needs to be addressed from the recruitment, training, reward, discipline, and termination or change of employment.
- *Research and development*. These activities can be a significant risk if there is uncontrolled connectivity between development and production/operations environments. Research and development can also create very sensitive information, such as that related to products under development. Those involved in such processes should therefore be aware of these risks, and of their responsibility for managing them.
- *Administration and IT*. These processes are often regarded as having principal responsibility for the assessment and management of information security risk. However, it is essential that the interrelationship between information risk and organizational risk (see later in this annex) is understood, and as a consequence that information security risk assessment is undertaken by all functions and information security risks are not seen purely as an "IT problem".
- *Finance and accounts*. Information security risk assessment is of primary importance to the financial and accounting processes of any organization. Good corporate governance (see **B.3**) requires consistent and accurate financial information that can be traced from its point of origin to its point of use, through a transparent audit trail. The confidentiality of price-sensitive information, undisclosed financial results, and financial forecasts should also be maintained consistent with business and regulatory requirements.

These are examples of specific information security risks in relation to organizational processes. However, all organizational functions need to work together to address organizational risk (see **B.2**) through the use of an integrated and coherent strategy, as described in this standard.

B.2 Organizational risk

Organizations are exposed to various types of business risk. These risks can be categorized in a number of ways. One approach is to consider the source of the risk, examples being investment, legal, operational and market risks. Another is to consider the nature of the asset which is at risk, examples being people, property and information. A further approach is to consider the consequence of a risk in respect of its implications for the long, medium and short-term activities of the business, examples being strategic, tactical and operational risks.

An organization will also be exposed to a range of information security risks. These might be recognised as a major category of business risk in their own right or they could be subsumed in other categories such as strategic and operational risks. An information security risk management system should be capable of dealing with all risks of this kind, irrespective of the way in which they are categorized in business terms.

Information security risk requires the effective control of processes, people and systems, and the monitoring of, and response to, external events. This standard aims to give guidance on assessing and managing levels of information security risk. Establishing, implementing and operating, monitoring and reviewing, and maintaining and improving the management system for information security risks is the subject of the related standard, BS ISO/IEC 27001:2005.

B.3 Corporate governance

According to the OECD's Principles of Corporate Governance [20], good corporate governance "... should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring." While this directive clearly applies to large, publicly-quoted companies, it is obviously in the best interests of all businesses that their information risk should be assessed and managed. But most importantly, effective business process monitoring depends on effective measurement of information security risk.

While corporate governance can be seen to concern itself, in the main, with the assurance of shareholders' and/or stakeholders' rights within a public company, the corporate governance principles apply to any organization, particularly to those that form part of the supply chain for a public company, and especially if any part of their business is conducted on-line. The principles concerned are those of disclosure and transparency. An organization's ability to assure all business partners that its information is secured is part of supporting the governance principles of disclosure and transparency.

Specifically, the disclosure and transparency principles demand that information is prepared and disclosed in accordance with high quality standards and that channels for disclosure enable unimpeded, easy access to all appropriate information. Moreover, they demand that foreseeable risk factors are disclosed implying an effectively implemented risk assessment process.

In summary, an organization's effectiveness, corporate governance, operational risk management and the legal and regulatory environment all serve as drivers to the implementation of an effective ISMS. The ISMS is as important to the operation of an organization as efficient and appropriate information and communications technology systems.

Annex C (informative) Examples of assets, threats, vulnerabilities and risk assessment methods

C.1 Asset identification

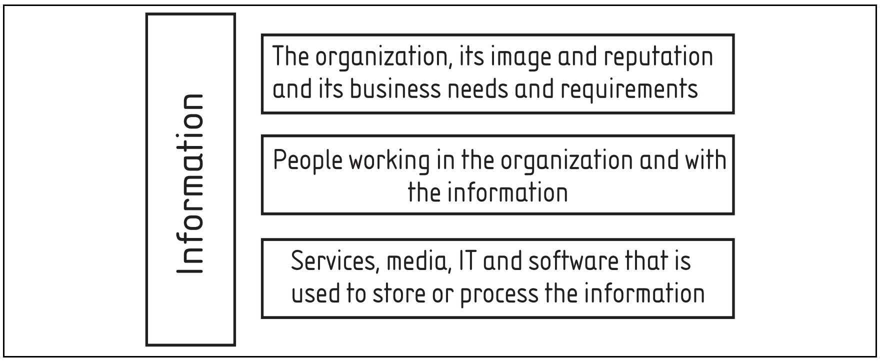
One of the most valuable and important types of asset is information, and information needs to be protected irrespective of which form it takes, for example in databases and data files, company or system documentation, contracts, user manuals, training material, operational or support procedures, guidelines, documents containing important business results, continuity plans, or fallback arrangements.

In addition, there are other assets that are used to store or process information, or have an impact on the security of the information assets. These other assets include the following.

- *Processes and services:* including business processes, application specific activities, computing and communications services and other technical services supporting the processing of information (heating, lighting, power, air-conditioning services);
- *Software:* including application software, system software, development tools and utilities;
- *Physical items:* including computer and communications equipment, media (paper, tapes, CDs and disks), and other technical equipment (power supplies, air-conditioning units), furniture and accommodation that are used to support the processing of information;
- *People:* including personnel, customers, subscribers, and any other person within the ISMS that is involved with storing or processing of information.

For a comprehensive assessment, it is also important to identify organizational assets that might be influenced by information security, such as the organization's image and reputation. Figure C.1 illustrates the different types of assets and how these different assets relate to information security.

Figure C.1 **Types of assets**


Information
The organization, its image and reputation and its business needs and requirements
People working in the organization and with the information
Services, media, IT and software that is used to store or process the information

C.2 Example list of threats

The following list provides some examples of the threats and vulnerabilities associated with the BS ISO/IEC 17799:2005 control objectives and controls. This is not an exhaustive list of threats and vulnerabilities and these should only be taken as examples to illustrate the concepts and the relationship with the controls given in BS ISO/IEC 17799:2005.

Again the most important principle is that an organization needs to adopt risk assessment and risk management approaches that will appropriately address and identify the complete range of threats and vulnerabilities relevant to their business environment, which could include some or all of the threats and vulnerabilities given in the following list.

The following is an example list of threats derived from selected parts of BS ISO/IEC 17799:2005. This list of threats is presented here for illustrative purposes and should not be taken as being definitive and complete:

- acts of terrorism;
- air conditioning failure;
- airborne particles/dust;
- bomb attack;
- breach of legislation or regulations;
- breaches of contractual obligations;
- compromise of assets;
- compromise of security;
- damage caused by penetration tests;
- damage caused by third parties;
- destruction of records;
- destruction of the business continuity plans;
- deterioration of media;
- disasters (natural or man-made);
- disclosure of information;
- disclosure of passwords;
- disruption to business processes;
- dust;
- earthquake;
- eavesdropping;
- environmental contamination (and other forms of natural or man-made disasters);
- equipment failure;
- errors;
- failure of communications services;
- failure of supporting utilities (such as electricity, water supply, sewage, heating, ventilation, and air conditioning)

- falsification of records;
- fire;
- flooding;
- fraud;
- hardware failure;
- hurricane;
- introduction of unauthorized or untested code;
- illegal import/export of software;
- illegal use of software;
- industrial action;
- information leakage;
- information security incidents;
- interception;
- interference;
- interruption to business activities and processes;
- lightning;
- loss of integrity;
- loss of records;
- loss of service;
- maintenance error;
- malfunctions of supporting utilities;
- malicious code;
- masquerading of user identity;
- misuse of audit tools;
- misuse of information processing facilities;
- misuse of resources or assets;
- network access by unauthorized persons;
- operational support staff error;
- power fluctuation;
- security failure;
- software failure;
- system failure;
- system misuse (accidental or deliberate);
- theft;
- unauthorized access;
- unauthorized access to audit logs;
- unauthorized access to audit tools;
- unauthorized modification of audit logs;
- unauthorized or unintentional modification;
- unauthorized physical access;

- unauthorized use of IPR material;
- unauthorized use of software;
- unavailability;
- unsuccessful changes;
- use of network facilities in an unauthorized way;
- use of software by unauthorized users;
- use of software in an unauthorized way;
- user error;
- vandalism;
- violation of intellectual property rights;
- wilful damage.

Depending on the type of threat, its occurrence could result in a number of different outcomes, such as:

- accidental or unintended changes to software and data sharing facilities in a computing environment;
- breach of security due to non-compliance with operational procedures;
- breach of security due to inaccurate, incomplete or inappropriate operating procedures or the definition of responsibilities, or insufficient updating of such procedures;
- breach of security due to non-compliance with incident handling procedures;
- compromise, damage of loss of data at a contractor's site;
- damage due to inaccurate, incomplete or inappropriate continuity plans, insufficient testing or insufficient updating of plans;
- denial of service, system resources, information;
- email bombs;
- forgery;
- fraud;
- negligent or deliberate misuse of facilities due to lack of segregation and execution of duties;
- unauthorized disclosure of the location of sites/buildings/offices containing critical and/or sensitive computing and processing facilities;
- unauthorized disclosure of information.

C.3 Threat examples and BS ISO/IEC 17799:2005

C.3.1 General

The following illustrates by example how the various threats given earlier in this annex relate to selected control objectives given in BS ISO/IEC 17799:2005.

C.3.2 Physical and environmental security

C.3.2.1 Secure areas

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***9.1.***

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information. Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls.

The following threats relate to this objective:

- fire;
- bomb attack;
- earthquake;
- environmental contamination (and other forms of natural or man-made disasters);
- flooding;
- hurricane;
- industrial action;
- interference;
- theft;
- unauthorized physical access;
- wilful damage.

C.3.2.2 Equipment security

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***9.2***.

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities. Equipment should be protected from physical and environmental threats.

The following threats relate to this objective:

- airborne particles/dust;
- air conditioning failure;
- bomb attack;
- compromise of assets;
- dust;
- environmental contamination (and other forms of natural or man-made disasters);
- eavesdropping;
- failure of supporting utilities (such as electricity, water supply, sewage, heating, ventilation, and air conditioning);
- fire;
- flooding;
- hardware failure;
- information leakage;
- interception;

- interference;
- interruption of activities;
- lightning;
- maintenance error;
- malfunctions of supporting utilities;
- malicious code;
- power fluctuation;
- theft;
- unauthorized physical access;
- user error;
- vandalism;
- wilful damage.

C.3.3 Communications and operations management

C.3.3.1 Operational procedures and responsibilities

*NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause **10.1***

Objective: To ensure the correct and secure operation of information processing facilities. Responsibilities and procedures for the management and operation of all information processing facilities should be established.

The following threats relate to this objective:

- disclosure of information;
- fraud;
- introduction of unauthorized or untested code;
- malicious code;
- masquerading of user identity;
- misuse of resources or assets;
- operational support staff error;
- software failure;
- system misuse (accidental or deliberate);
- system failure;
- theft;
- unauthorized access;
- unauthorized or unintentional modification;
- unsuccessful changes;
- use of software by unauthorized users;
- use of software in an unauthorized way;
- user error;
- wilful damage.

C.3.4 Information security aspects of business continuity management

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***14.1****.*

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets.

The following threats relate to this objective:

- acts of terrorism;
- disasters (natural or man-made);
- destruction of the business continuity;
- plans;
- fire;
- errors;
- equipment failure;
- information security incidents;
- interruption to business activities and processes;
- loss of service;
- security failure;
- system failure;
- theft;
- unavailability.

C.3.5 Compliance

C.3.5.1 Compliance with legal requirements

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***15****.*

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

The following threats relate to this objective:

- breaches of contractual obligations;
- breach of legislation or regulations;
- destruction of records;
- deterioration of media;
- falsification of records;
- illegal import/export of software;
- illegal use of software;
- loss of records;
- misuse of information processing facilities;
- unauthorized access;
- unauthorized use of IPR material;
- unauthorized use of software;
- use of network facilities in an unauthorized way;
- violation of intellectual property rights.

C.3.5.2 Compliance with security policies and standards, and technical compliance

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***15.2****.*

Objective: To ensure compliance of systems with organizational security policies and standards. The security of information systems should be regularly reviewed.

The following threats relate to this objective:

- compromise of security;
- damage caused by penetration tests;
- failure of communications services;
- misuse of resources;
- network access by unauthorized persons;
- theft;
- unauthorized access;
- illegal import/export of software;
- illegal use of software;
- malicious code;
- unauthorized use of software;
- use of network facilities in an unauthorized way;
- wilful damage.

C.3.5.3 Information systems audit considerations

NOTE This subclause corresponds to BS ISO/IEC 17799:2005, Clause ***15.3***.

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process. There should be controls to safeguard operational systems and audit tools during information systems audits.

The following threats relate to this objective:

- damage caused by third parties;
- disclosure of passwords;
- disruption to business processes;
- interference to or from the audit process;
- loss of integrity;
- misuse of audit tools;
- unauthorized access to audit logs;
- unauthorized access to audit tools;
- unauthorized modification of audit logs.

C.4 Vulnerability examples and BS ISO/IEC 17799:2005

C.4.1 General

The following lists give examples for vulnerabilities in various security areas, including examples of threats, which might exploit these vulnerabilities. The lists can provide help during the assessment of vulnerabilities.

It is emphasized that other threats could also exploit these vulnerabilities.

C.4.2 Human resource security (BS ISO/IEC 17799:2005, Clause 8)

The vulnerabilities in Table C.1 relate to human resources security.

Table C.1 **Vulnerabilities related to human resources security**

Vulnerability	**The vulnerability could be exploited by**
Insufficient security training	operational support staff error
Lack of security awareness	user errors
Lack of monitoring mechanisms	use of software in an unauthorized way
Lack of policies for the correct use of telecommunications media and messaging	use of network facilities in an unauthorized way
No removal of access rights upon job termination	unauthorized access
No procedure to ensure return of asset upon job termination	theft
Unmotivated or disgruntled staff	misuse of information processing facilities
Unsupervised work by outside staff or staff working outside normal business hours	theft

C.4.3 Physical and environmental security (BS ISO/IEC 17799:2005, Clause 9)

The vulnerabilities in Table C.2 relate to human resources security.

Table C.2 **Vulnerabilities related to physical and environmental security**

Vulnerability	**The vulnerability could be explained by**
Inadequate or careless use of physical access control to buildings, rooms and offices	wilful damage
Lack of physical protection for the building, doors, and windows	theft
Location in an area susceptible to flood	flooding
Unprotected storage	theft
Insufficient maintenance/faulty installation of storage media	maintenance error
Lack of periodic equipment replacement schemes	deterioration of storage media
Susceptibility of equipment to humidity, dust, soiling	airborne particles/dust
Susceptibility of equipment to temperature variations	extremes of temperature
Susceptibility of equipment to voltage variations	power fluctuation
Unstable power grid	power fluctuation

C.4.4 Communications and operations management (BS ISO/IEC 17799:2005, Clause 10)

The vulnerabilities in Table C.3 relate to communications and operations management.

Table C.3 **Vulnerabilities related to communications and operations management**

Vulnerability	**The vulnerability could be exploited by**
Complicated user interface	operational staff error
Disposal or reuse of storage media without proper erasure	unauthorized access to information
Inadequate change control	security failure
Inadequate network management	traffic overloading
Lack of back-up procedures	loss of information
Lack of proof of sending or receiving a message	repudiation
Lack of updates for malicious code protection software	virus infection
No segregation of duties	system misuse (accidental or deliberate)
No separation of test and operational facilities	unauthorized modification of operational systems
Uncontrolled copying	theft
Unprotected public network connections	use of software by unauthorized users

C.4.5 Access control (BS ISO/IEC 17799:2005, Clause 11)

The vulnerabilities in Table C.4 relate to access control.

Table C.4 **Vulnerabilities related to access control**

Vulnerability	**The vulnerability could be exploited by**
Inappropriate segregation of networks	unauthorized connections in networks
Lack of clear desk and clear screen policy	loss of or damage to information
Lack of identification and authentication mechanisms like user authentication	masquerading of user identity
Lack of protection of mobile computing equipment	unauthorized access to information
No or incorrect access control policy	unauthorized access to information, systems or software
No “logout” when leaving the workstation	use of software by unauthorized users
No or insufficient software testing	use of software by unauthorized users
No review of user access rights	access by users that have left the organization or changed jobs
Poor password management (easily guessable passwords, storing of passwords, insufficient frequency of change)	masquerading of user identity
Default factory accounts and passwords are not disabled or changed	unauthorized access to information, systems or software
Uncontrolled use of system utilities	overriding system or application controls

C.4.6 Information systems acquisition, development and maintenance

The vulnerabilities in Table C.5 relate to information systems acquisition, development and maintenance.

Table C.5 **Vulnerabilities related to systems acquisition, development and maintenance**

Vulnerability	**The vulnerability could be exploited by**
Inappropriate protection of cryptographic keys	disclosure of information
Incomplete policy on the use of cryptography	breach of legislation or regulations
Lack of control of input or output data	error
Lack of validation of processed data	corruption of information
No or insufficient software testing	use of software by unauthorized users
Poorly documented software	operational support staff error
Unclear or incomplete specifications for developers	software failure
Uncontrolled downloading and using software	malicious software
Uncontrolled use of shareware/freeware for corporate applications	legal liability
Well-known flaws in the software	use of software by unauthorized users
Wrong selection of test data	unauthorized access to personal data

C.5 Examples of risk assessment methods

C.5.1 Asset valuation scales

The organization should identify a suitable asset valuation scale to assess the values of its assets. This scale should be appropriate to the organization's business and applied consistently. Examples of asset valuation scales could be:

- a distinction between low, medium and high;
- in more detail, a distinction between negligible, low, medium, high and very high.

An organization should define its own limits for the asset valuation scale. 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.

The asset valuation scales should address confidentiality, integrity or availability, or any other important property[5)] of the asset if damaged. Giving interpretations of the asset valuations in terms that are appropriate to the respective audience is vital in obtaining relevant information and well-focused input into the valuation process, e.g. from asset owners and users.

C.5.2 Valuation scales for threats and vulnerabilities

A scale needs to be identified for the assessment of threats and vulnerabilities that is suitable for the organization's business and the risk assessment method applied. Examples of valuation scales for threats and vulnerabilities could be:

- a distinction between low, medium and high;
- in more detail, a distinction between negligible, low, medium, high and very high.

In many cases, a simple three-level scale will be sufficient but in some other cases, a more detailed scale might be necessary. Whatever level of detail is chosen, care should be taken that the interpretation of the levels can successfully convey the differences between the various levels to the users that are supposed to provide input into this process.

An interpretation of a three-level threat valuation scale is as follows.

- *Low likelihood.* It is not likely that the threat will occur, there are no incidents, statistics, motives, etc. that indicate that this is likely to happen.

[5)] Sometimes, the criteria "confidentiality", "integrity" and "availability" alone are not sufficient to express the importance of an asset, e.g. when considering information where intellectual property rights need to be protected, or where there is a need to have non-repudiation. In such cases, additional criteria should be introduced to match these requirements.

- *Medium likelihood.* It is possible that the threat will occur, there have been incidents in the past, or statistics or other information that indicate that this or similar threats have occurred sometime before, or there is an indication that there might be some reasons for an attacker to carry out such action.
- *High likelihood.* The threat is expected to occur, there are incidents, statistics or other information that indicate that the threat is likely to occur, or there might be strong reasons or motives for an attacker to carry out such action.

An interpretation of a three-level vulnerability valuation scale is as follows.

- *Highly probable or probable.* It is easy to exploit the vulnerability and there is little or no protection in place.
- *Possible.* The vulnerability might be exploited, but some protection is in place.
- *Unlikely.* The vulnerability is hard to exploit and the protection in place is good.

C.5.3 Matrix using asset values and values for threats and vulnerabilities

The asset values, and the threat and vulnerability levels, are matched in a matrix such as that shown in Table C.6, to identify for each combination the relevant measure of risk. When linking the asset values and the threats and vulnerabilities together, consideration needs to be given to whether the threat/vulnerability combination could cause problems to confidentiality, integrity and/or availability. Depending on the results of these considerations, the appropriate asset value(s) should be chosen, i.e. the one that has been selected to express the impact of a loss of confidentiality, or the one that has been selected to express the loss of integrity, or the one chosen to express the loss of availability.

Using this method can lead to one, two or three risks for each of the assets, depending on the particular threat/vulnerability combination considered. If additional properties are used (see also **C.1**), there might be even more than three risks calculated for each of the assets and each threat/vulnerability combination. In this example, the risk values are on a scale of 1 to 8.

Table C.6 **Matrix with risk values**

Asset value	**Level of threat**								
	Low			**Medium**			**High**		
	Level of vulnerability								
	L	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

For each asset, the relevant vulnerabilities and their corresponding threats are considered. Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the values of the threat and the vulnerability. For example, if the asset has the value 3, the threat value is high and the vulnerability value low, the measure of risk is 5.

The matrix can vary in terms of the number of threat levels, vulnerability levels, and the number of asset valuation categories, and can thereby be adjusted to the needs of the organization.

C.5.4 Ranking of incidents by measures of risk

A matrix or table can be used to relate the factors of impact (asset value) and likelihood of incident occurrence (threats and vulnerabilities coming together to cause a particular incident). The first step is to evaluate the impact (asset value) on a predefined scale, e.g. 1 to 5 of each asset (column b in Table C.7). The second step is to evaluate the likelihood of incident occurrence on a predefined scale, e.g. 1 to 5 of each incident (column c in Table C.7). The third step is to calculate the measure of risk by multiplying b by c. Finally the incidents can be ranked in order of their exposure factor. It should be noted that in this example, 1 is taken as being the lowest impact and the lowest likelihood of occurrence.

Table C.7 **Matrix ranking incidents by measures of risk**

Incident desciptor (a)	**Impact (asset) value (b)**	**Likelihood of occurrence (c)**	**Measure of risk (d)**	**Incident ranking (e)**
Incident A	5	2	10	2
Incident B	2	4	8	3
Incident C	3	5	15	1
Incident D	1	3	3	5
Incident E	4	1	4	4
Incident F	2	4	8	3

Annex D (informative) Risk management tools

D.1 General

A variety of methods exist for undertaking risk assessment and risk management reviews ranging from simple question and answer checklist-based approaches (that nonetheless address business risks, and are not mere compliance checklists) through to structured analysis-based techniques. There are many commercially available tools which can be used to assist the assessment process. These include both automated (computer assisted) and manual products.

Whatever methods or products are used by the organization, they should at least address the risk components, relationships between the components, and processes, as described in Clauses **5** and **6** of this guide.

Once a risk assessment review has been completed for the first time, the results of the review (assets and their values, security requirements and risk levels, and identified controls) should be stored and documented, for example, in a database. Software support tools can make this activity, and any future re-assessment activity, much easier.

D.2 Selecting a risk management tool

The following list gives a few ideas of criteria to be considered when selecting a risk assessment tool.

The tool should at least contain modules for:

- data collection;
- analysis;
- output of results.

The method upon which the selected tool works and functions should reflect the organization's policy and overall approach to risk assessment.

Effective reporting of the results of risk assessment is an essential part of the process if management is to weigh the alternatives and make an appropriate, reliable and cost effective selection of controls. Therefore the tool should be capable of reporting the results in a clear and accurate manner.

The ability to maintain a history of the information collected during the data collection phase, and of the analysis, is useful in subsequent reviews or queries.

Documentation describing the tool is essential for its effective use and should be available.

The tool selected should be compatible with the hardware and software in use in the organization.

Automated tools are generally efficient and error free, but some can be more difficult to install or learn. Therefore it might be necessary to consider the availability of training and support for the tool.

The effective use of the tool depends, in part, on how well the user understands the product and whether it has been installed and configured correctly. Therefore the availability of guidance on installation and use might be essential.

Annex E (informative) Relationship between BS ISO/IEC 27001:2005 and BS 7799-3:2006

Table E.1 illustrates the relationship between the clauses of BS ISO/IEC 27001:2005 and this standard. This relationship highlights how this standard can help to interpret the requirements contained in BS ISO/IEC 27001:2005.

Table E.1 **Relationship between BS ISO/IEC 27001:2005 and BS 7799-3:2006**

Clauses from BS ISO/IEC 27001:2005	Clauses from BS 7799-3:2006
1 Scope	1 Scope
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions
4 Information security management system	—
4.1 General requirements	—
4.2 Establishing and managing the ISMS	—
4.2.1 Establish the ISMS	4 Information security risks in the organizational context 5 Risk assessment 6 Risk treatment and management decision making
4.2.2 Implement and operate the ISMS	6 Risk treatment and management decision making
4.2.3 Monitor and review the ISMS	7 Ongoing risk management activities
4.2.4 Maintain and improve the ISMS	7 Ongoing risk management activities
4.3 Documentation requirements	—
4.3.1 General	—
4.3.2 Control of documents	7.6 Documentation controls
4.3.3 Control of records	—
5 Management responsibility	—
5.1 Management commitment	—
5.2 Resource management	—
5.2.1 Provision of resources	—
5.2.2 Training, awareness and competence	—
6 Internal ISMS audits	—
7 Management review of the ISMS	7 Ongoing risk management activities
7.1 General	—
7.2 Review input	—
7.3 Review output	—
8 ISMS improvement	7 Ongoing risk management activities
8.1 Continual improvement	—
8.2 Corrective action	—
8.3 Preventive action	—

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN ISO 9001, *Quality management systems – Requirements*

ISO Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

BS ISO/IEC 13335-1:2004, *Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management*

BS ISO/IEC TR 13335-3:1998, *Information technology – Guidelines for the management of IT security – Part 3: Techniques for the management IT security*

BS ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT security – Part 4: Selection of safeguards*

BS ISO/IEC 17799:2005, *Information technology – Security techniques – Code of practice for information security management*

PD ISO/IEC TR 18044:2004, *Information technology – Security techniques – Information security incident management*

PD 3002, *Guide to BS 7799 risk assessment*

PD 3005, *Guide on the selection of BS 7799-2 controls*

Other publications

[1] UNITED STATES OF AMERICA. Federal Information Security Management Act of 2002. Washington: Government Printing Office.

[2] UNITED STATES OF AMERICA. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001. Washington: Government Printing Office.

[3] Internal control: Guidance for directors on the combined code: The Institute of Chartered Accountants in England and Wales, 2005.

[4] FINANCIAL SERVICES AUTHORITY. Financial Services Authority (FSA) Handbook. London: FSA, 2005.

[5] GREAT BRITAIN. Companies (Audit, Investigation and Community Enterprise) Act 2004. London: The Stationery Office.

[6] UNITED STATES OF AMERICA. Sarbanes-Oxley Act of 2002. Washington: Government Printing Office.

[7] GREAT BRITAIN. Computer Misuse Act. 1990. London: The Stationery Office.

[8] EUROPEAN COMMUNITIES. 1999/93/EC. Council directive of 13 December on a Community Framework for Electronic Signatures. Luxembourg: Office for Official Publications of the European Communities, 1999.

[9] EUROPEAN COMMUNITIES. Directive 97/7/EC of the European Parliament and of the council of 20 May 1997 on the protection of consumers in respect of distances contracts. Luxembourg: Office for Official Publications of the European Communities, 1997.

[10] EUROPEAN COMMUNITIES. 2002/58/EC. Directive of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Luxembourg: Office for Official Publications of the European Communities, 2002.

[11] UNITED STATES OF AMERICA. Code of Federal Regulations: Title 21: Food and Drugs, Part 11: Electronic Records, Electronic Signatures (21CFR11). Washington: Government Printing Office.

[12] 95/46/EC. Directive of the European Parliament on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Luxembourg: Office for Official Publications of the European Communities, 1995.

[13] CANADA. Personal Information Protection and Electronic Documents Act 2000.

[14] UNITED STATES OF AMERICA. Gramm-Leach-Bliley Act of 1999. Washington: Government Printing Office.

[15] UNITED STATES OF AMERICA. Health Insurance Portability and Accountability Act of 1996. Washington: Government Printing Office.

[16] UNITED STATES OF AMERICA. California Senate Bill No.1386. California Security Breach Information Act. Washington: Senate Printing and Document Services, 2002.

[17] UNITED STATES OF AMERICA. Children's Online Privacy Protection Act of 1998. Washington: Government Printing Office.

[18] UNITED STATES OF AMERICA. Family Educational Rights and Privacy Act of 1974, as amended. Washington: Government Printing Office.

[19] OECD Guidelines for the security of information systems and networks: Towards a culture of security, Paris: OECD, 2002.

[20] OECD Principles of Corporate Governance, Paris: OECD, 2004.

This page deliberately left blank

BSI – British Standards Institution

BSI is the independent national body responsible for preparing British Standards. It presents the UK view on standards in Europe and at the international level. It is incorporated by Royal Charter.

Revisions

British Standards are updated by amendment or revision. Users of British Standards should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using this British Standard would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside back cover.
Tel: +44 (0)20 8996 9000. Fax: +44 (0)20 8996 7400.

BSI offers members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of standards.

Buying standards

Orders for all BSI, international and foreign standards publications should be addressed to Customer Services. Tel: +44 (0)20 8996 9001.
Fax: +44 (0)20 8996 7001. Email: orders@bsi-global.com. Standards are also available from the BSI website at http://www.bsi-global.com.

In response to orders for international standards, it is BSI policy to supply the BSI implementation of those that have been published as British Standards, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Library and its Technical Help to Exporters Service. Various BSI electronic information services are also available which give details on all its products and services. Contact the Information Centre. Tel: +44 (0)20 8996 7111.
Fax: +44 (0)20 8996 7048. Email: info@bsi-global.com.

Subscribing members of BSI are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration. Tel: +44 (0)20 8996 7002.
Fax: +44 (0)20 8996 7001. Email: membership@bsi-global.com.

Information regarding online access to British Standards via British Standards Online can be found at http://www.bsi-global.com/bsonline.

Further information about BSI is available on the BSI website at http://www.bsi-global.com.

Copyright

Details and advice can be obtained from the Copyright & Licensing Manager.
Tel: +44 (0)20 8996 7070. Fax: +44 (0)20 8996 7553.
Email: copyright@bsi-global.com.

BSI
British Standards

389 Chiswick High Road
London
W4 4AL