Guide to BS 7799 Risk Assessment

Guidance aimed at those responsible for carrying out risk management

BSI
Business Information

Guide to BS 7799 Risk Assessment

This revision has been edited by:
Ted Humphreys (XiSEC Consultants Ltd)
Dr Angelika Plate (AEXIS Security Consulting)

Contents

WHAT THIS GUIDE IS ABOUT

Purpose and Scope of the Guide

This guide addresses the topic of risk assessment in the context of ISO/IEC 17799:2000 'Code of Practice for Information Security Management, [1]' and BS 7799-2:2002 'Information security management systems – specification with guidance for use, [2]'. This guide aims at providing a common basis and understanding of the terminology used and underlying concepts behind risk assessment and the overall process of involved in carrying out a risk assessment. This document will be useful to those:

- Establishing and maintaining an Information Security Management System (ISMS),
- Preparing for ISMS certification,
- Involved in auditing an organization's ISMS (first party, second party and third party audits and certification).

It is important that the results of risk assessment activities are used by the organization to explain and justify, in particular as a key part of the certification process, why certain control objectives and controls from Annex A of BS 7799-2 have been selected, why some of them have not been selected and (where applicable) why controls additional to those in BS 7799-2 have been selected.

What is an ISMS

The information security management system (ISMS) is that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, maintain and improve information security. The management system includes organization structure, policies, planning activities, responsibilities, practices, procedures, processes and resources. The scope of an ISMS can be defined in terms of the organization as a whole, or parts of the organization, covering the relevant assets, systems, applications, services, networks and technology employed to process, store and communicate information. This includes information as an asset itself. For the purposes of this guide this collection of information related items is called an 'information system' or 'information systems'. In this context an ISMS could encompass:

- All of an organization's information systems;
- Some of an organization's information systems; or
- A specific information system.

The scope of an ISMS as determined by the organization is the subject of certification as indicated in the table at the end of this section. An organization may need to define a different ISMS for different parts or aspects of its business. For example, an ISMS may be defined for an organization's specific trading relationship with another company. Another example might be where an organization structures its business to ensure suitable separation of business interests are taken care of, in which case this could be covered by establishing one or more different ISMS. There are different scenarios that are possible which could be covered by one or more ISMS.

The PDCA Model

The model, known as the "Plan-Do-Check-Act Model" (PDCA Model), is used in the BS 7799-2:2002 standard. This model is used as the basis for establishing, implanting, monitoring, reviewing, maintaining and reviewing an ISMS. More details of this model are given in BS 7799-2:2002 and PD3001.

Target Readership

This guide will be useful for organizations:

- That need to understand the process of risk assessment in the context of ISO/IEC 17799 and BS 7799-2,
- Establishing and maintaining their Information Security Management System,
- Preparing for certification or re-certification of their Information Security Management System.

It is also intended to be used by those organizations involved in conducting certification, which need to understand the process of assessing risks.

There are a number of other guides, which also provide helpful guidance with regard to BS 7799 and ISMS development and certification:

- Preparing for BS 7799 certification (PD 3001) - Guidance on implementation of ISMS process requirements to organizations preparing for certification
- Guide to BS 7799 Risk Assessment (PD 3002) - Guidance aimed at those responsible for carrying out risk management
- Are you ready for a BS 7799 Part 2 Audit? (PD 3003) - A compliance assessment workbook
- Guide to the implementation and auditing of BS 7799 controls (PD 3004) - Guide to the implementation and auditing of BS 7799 controls
- Guide on the selection of BS 7799 Part 2 controls (PD 3005)

How the Guide is Set Out

This guide is divided into two parts:

- **Sections 1 and 2 'Getting Started'** - *This part provides an overview of:*
  - *What is information security,*
  - *Why action needs to be taken, and*
  - *How to achieve suitable protection.*
- **Sections 3 and 4 'Assessing the Risks** - *This part describes:*
  - *The components of risk assessment, and the relationships between them,*
  - *A detailed description of what is involved in the risk assessment processes, and*
  - *The various options an organization can take in its overall approach, or strategy, for risk assessment.*

Furthermore, there are several annexes giving more detailed examples of threats and vulnerabilities in relation to the ISO/IEC 17799 and BS 7799-2 control objectives and controls, and information about tools and methods for risk assessment and risk treatment.

More about ISO/IEC 17799 and BS 7799 Part 2

Scope and Objectives of ISO/IEC 17799

ISO/IEC 17799:2000 (see [1]) provides guidance on best practice for information security management. The prime objectives of ISO/IEC 17799:2000 are to provide:

- A common basis for organizations to develop, implement and measure effective security management practice;
- Confidence in inter-organizational dealings.

ISO/IEC 17799 defines a set of control objectives together with a comprehensive set of security controls that can be implemented to support the control objectives. These controls are based on information security controls currently being implemented by commercial, industrial and governmental organizations both in the UK and internationally.

These controls are recommended as good information security practice, subject of course to limiting factors such as environmental or technological constraints. Some controls are not applicable to every business environment and they should be used selectively, according to local circumstances.

Scope and Objectives of BS 7799 Part 2

BS 7999 Part 2 (see [2]) specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the

organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure adequate and proportionate security controls to adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image.

Assessing the Risks and Selecting Controls in the Context of BS 7799 Part 2

An organization needs to assess its security risks taking into account the business value of the information and other assets at risk for those information systems defined to be in the scope of the ISMS being established and maintained. The control objectives and controls which are selected by an organization, and documented in an ISMS, related to its particular business situation and environment, will need to be determined through a process of identifying and assessing the security risks using a risk assessment process (see also Section 3.1 – 3.5).

Based on the results of risk assessment, suitable controls can be selected from Annex A of BS 7799 Part 2 to protect the organization's assets encompassed by an ISMS against the identified risks. In order to get an ISMS certified, an organization needs to be able to demonstrate that the control objectives and controls they selected to achieve information security are appropriate to protect against the identified risks.

Controls not in BS 7799 Part 2

The process of selecting control objectives and controls does not preclude the identification and implementation of controls, which are not included in Annex A of BS 7799 Part 2. It could be the case that the assessed risks justify other controls not in BS 7799 Part 2. These may then be selected from other security control catalogues, libraries, standards and other sources. Justification for controls not in BS 7799 Part 2 needs to be documented for the purpose of certification in the same way as those controls selected from BS 7799 Part 2.

Details of the Plan-Do-Check-Act Process

Section 4.2 of BS 7799 Part 2 describes the establishment and management of a documented ISMS. Organizations seeking to be certified or re-certified as complying to BS 7799 Part 2 shall apply the Plan-Do-Check-Act Model to the ISMS processes as described in the following table (more details are given in Section 3 of this document):

Topic/Task	Task for the Organization
Establish the ISMS (Section 4.2.1)	a) Defined the scope of the ISMS; b) Define the ISMS policy; c) Define a systematic approach to risk assessment; d) Identify the risks; e) Assess the risks; f) Identify and evaluate options for the treatment of risk; g) Select control objectives and controls; h) Prepare a Statement of Applicability; i) Obtain management approval.
Implement and operate the ISMS (Section 4.2.2)	a) Formulate a risk treatment plan; b) Implement the risk treatment plan; c) Implement all selected control objectives and controls; d) Implement the training and awareness programme; e) Manage operations; f) Manage resources.
Monitor and review the ISMS (Section 4.2.3)	a) Execute monitoring procedures; b) Undertake regular reviews of the effectiveness of the ISMS; c) Review the level of residual risk and acceptable risk; d) Conduct internal ISMS audits; e) Undertake management reviews of the ISMS on a regular basis; f) Record all events that have an effect on the performance of the ISMS.
Maintain and improve the ISMS (Section 4.2.4)	a) Implement the identified improvements; b) Take appropriate preventive and corrective action; c) Communicate the results to all interested parties; d) Ensure that the improvements achieve the intended objectives.

Note: The clause references listed in parenthesis in the first column of this table refer to the related clauses in Section 4.2 of BS 7799 Part 2 [2].

1 THE WHY, WHAT AND HOW

1.1 What is information security

The purpose of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

Information security management enables information to be shared, while ensuring the protection of information and all other assets within the scope of the ISMS (see also Section 3.1). It has three basic components to achieve confidence in and assurance of information:

- Confidentiality: protecting sensitive information from unauthorised disclosure or intelligible interception;
- Integrity: safeguarding the accuracy and completeness of information and software;
- Availability: ensuring that information and vital services are available to users when required.

Information takes many forms. It can be stored on computers, transmitted across networks, printed out or written down on paper, and spoken in conversations. From a security perspective, appropriate protection should be applied to all forms of information, including papers, databases, films, view foils, tapes, diskettes, CD ROMs, conversations (e.g. conversations using technologies such as fixed and mobile telephones) and any other methods and media used to convey knowledge and ideas.

1.2 Why action needs to be taken

An organization's information, and the systems, applications and networks that support it are important business assets. The confidentiality, integrity and availability of the assets may be essential to maintain competitive edge, cash flow, profitability, legal compliance and an organization's image. An organization may be facing increasing security threats from a wide range of sources. An organization's systems, applications and networks may be the target of a range of serious threats (see Section 3.3), including computer-based fraud, espionage, sabotage, vandalism and other sources of failure or disaster. New sources of damage, such as the highly publicised threats from computer viruses and computer hackers, continue to emerge. Such threats to information security are expected to become more widespread, more ambitious and increasingly sophisticated. At the same time, because of increasing dependence on technology based information systems and services, an organization may be becoming more vulnerable to security threats.

The growth in the use of networking presents new opportunities for unauthorised access to computer systems and the trend to distributed computing reduces the scope for centralised, specialist control of an organization's ISMS.

To deal with this, suitable control objectives and controls for protecting an organization's information need to be identified and implemented. In this respect ISO/IEC 17799 and BS 7799 Part 2 provide a good source of controls to meet this need, and for the establishment of ISMSs. In order to identify and select which controls are appropriate, an organization should identify their security requirements (see also Section 3.3 and 3.4) for the information systems included in the ISMS(s) in the context of its business processes and applications.

Organizations of all business types and of all sizes, from the multinational company through to SMEs (Small to Medium sized Enterprises), are vulnerable to security threats. The sooner action is taken to protect an organization's information, the cheaper and more effective security will be for the organization in the long run.

1.3 Overview of the Risk Assessment Process

Generally, risk assessment methods and techniques are applied to a complete ISMS or specific information systems and facilities, but they can also be directed to individual system components or services where this is practicable, realistic and helpful. Assessment of risks involves the systematic consideration of the following (see also the definition in 2.3.9):

- *Consequence* - the business harm likely to result from a significant breach of information security, taking account of the potential consequences of loss or failure of information confidentiality, integrity and availability;
- *Probability* - the realistic likelihood of such a breach occurring in the light of prevailing threats, vulnerabilities and controls.

The process involves:

- The selection of a method of risk assessment *(see Section 4)* that is suitable for the ISMS, and the identified business information security, legal and regulatory requirements, as well as determining criteria for accepting risks and identifying the acceptable levels of risk.
- Identify and assess the risks *(see Section 3)* for the ISMS(s) and the information systems encompassed in ISMS(s), identify and evaluate options for the treatment of risk, select control objectives and controls to reduce the risks to acceptable levels, and – for certification purposes – produce a Statement of Applicability.

Any organization that wants to have adequate security controls in place should use the results of risk assessments to guide and determine the appropriate risk treatment action and priorities for managing information security risks. This process enables an organization to identify the necessary controls from ISO/IEC 17799 or BS 7799 Part 2, Annex A, respectively, to be implemented and operated. Assessment of risks depends upon the following factors:

- The nature of the business information and systems;
- The business purpose for which the information is used;
- The environment in which the system is used and operated;
- The protection provided by the controls in place.

The risk assessment might identify exceptional business security risks requiring stronger controls that are additional to the recommendations given in BS 7799 Part 2. These controls need to be justified on the basis of the conclusions of the risk assessment. Expenditure on information security controls needs to be balanced against, and appropriate to, the business value of the information and other business assets at risk, and the business harm likely to result from security failures. A periodic review of business risks and security controls, to address changing business requirements and priorities, is therefore a regular feature of information security management.

The resources needed for the risk assessment and management process can vary according to the depth of the review involved, and the security requirements of the organization and the complexity of its business.

Experience has shown that the following factors are often critical to the successful implementation of information security within an organization:

- Security objectives and activities being based on business objectives and requirements, and led by business management;
- Visible support and commitment from top management;
- A good understanding of the security risks*;*
- Effective marketing of security to all managers and employees;
- Distribution of comprehensive guidance on information security policy and standards to all employees and contractors.

1.5 Risk Assessment and Risk Treatment in the PDCA Model

When looking at the PDCA Model and the activities to be carried out in the ISMS process (see also the table in the Introduction), it is obvious that risk assessment is a major part of the "Plan" activity within the PDCA Model. In the same way, risk treatment forms an important element of the "Do" part of the PDCA model. If an organization decides to go for certification, then this should take place after implementing all actions of the "Do" activity.

What might not be as obvious, but is very important to notice is that the "Check" activity includes a re-assessment of all the risks to check that the controls in place are effectively reducing the risks, and that part of the "Act" activity is nothing else but treating the re-assessed risks, therefore similar to the "Do" part. This means that the risk assessment and risk treatment described in the rest of this guide help to support all parts of the PDCA model.

2 REFERENCES AND TERMINOLOGY

2.1 Using Guidelines for the Management of IT Security (GMITS)

'Guidelines for the Management of IT Security' (GMITS) is the internationally recognised ISO/IEC guidelines for the management of IT security, which are referenced in several places in this guide. GMITS provides a set of security management practices and techniques that have been developed and agreed by many leading international companies and organizations.

GMITS forms the basis for many of the ideas, concepts and techniques for the risk assessment and treatment process as described in this guide. Although the title of the GMITS standard refers to IT security, its scope goes beyond this and the principles given in these guidelines can also be applied for information security.

Sections 3 and 4 of this guide explains how the advice and guidance given the different parts of GMITS can be used to support the risk assessment and treatment processes for the general application of ISO/IEC 17799 and BS 7799 Part 2 and also in combination with the BS 7799 Part 2 certification process.

The following is a brief summary of the five different parts of the GMITS standard (see [3] - [7]).
NOTE: At the time this guide was published Parts 1 to 3 of GMITS are under revision in ISO/IEC JTC1/SC27. Revised versions of these Parts will be published by ISO/IEC in due course therefore the reader needs to check what the latest version of GMITS are as the descriptions in 2.1.1-2.1.3 below may

change. The reader should note that Part 4 of GMITS might also be revised at some point in time in the near future.

2.1.1 GMITS Part 1 - Concepts and Models for IT Security

Part 1 of GMITS describes the basic concepts and models, which should be considered with respect to risk assessment. An overview of these concepts is given in Section 3. Users of this guide not familiar with these ideas should consult GMITS, Part 1 for further details and information.

NOTE: At the time this guide was published Part 1 of GMITS is under revision in ISO/IEC JTC1/SC27.

2.1.2 GMITS Part 2 - Managing and Planning IT Security

Part 2 of GMITS addresses the different activities related to the management of IT security within an organization. It can be used to support the selection of management strategies and the assignment of responsibilities in the IT security process. It also describes the various stages of planning, security policy development, risk assessment, implementation of controls and maintenance of IT security from a management point of view. As with GMITS, Part 1, users of this guide should consult Part 2 for detailed information.

NOTE: At the time this guide was published Part 2 of GMITS is under revision in ISO/IEC JTC1/SC27.

2.1.3 GMITS Part 3 - Techniques for the Management for IT Security

Part 3 of GMITS discusses and recommends techniques for the successful management of IT security. This includes the various risk assessment options described in Section 4 and the risk assessment process described in Section 3, including a detailed description of various risk assessment possibilities in an Annex. Hence, GMITS, Part 3 can be used to obtain more detailed information about these topics, especially on how to carry out a risk assessment.

NOTE: At the time this guide was published Part 3 of GMITS is under revision in ISO/IEC JTC1/SC27.

2.1.4 GMITS Part 4 - Selection of Safeguards

Part 4 of GMITS provides information about the selection of controls according to different assessment methods (as, for example, are described in Section 4). Part 4 can help to select controls from codes of practice like ISO/IEC 17799 as well as the selection of controls according to a detailed risk assessment. It can be used to support the selection of controls described in Section 3 of this guide.

2.1.5 GMITS Part 5 - Safeguards for External Connections

Part 5 of GMITS provides guidance to an organization connecting its information systems to external networks. This part of GMITS includes the selection and use of security controls to provide security for the external connections and the services supported by those connections, and additional controls required for the systems because of the connections. Part 5 can also support the selection of security controls from ISO/IEC 17799 if external connections are involved.

2.2 References

[1] ISO/IEC 17799:2000 Code of practice for information security management

[2] BS 7799-2:2002 Information security management systems – specification with guidance for use

[3] BS ISO/IEC TR 13335-1:1996 Guidelines for the Management of IT Security (GMITS) Part 1: Concepts and Models for IT Security

[4] BS ISO/IEC TR 13335-2:1997 Guidelines for the Management of IT Security (GMITS) Part 2: Managing and Planning IT Security

[5] BS ISO/IEC TR 13335-3:1998 Guidelines for the Management of IT Security (GMITS) Part 3: Techniques for the Management of IT Security

[6] BS ISO/IEC TR 13335-4:2000 Guidelines for the Management of IT Security (GMITS) Part 4: Selection of Safeguards

[7] BS ISO/IEC PDTR 13335-5:2001 Guidelines for the Management of IT Security (GMITS) Part 5: Safeguards for External Connections

[8] Protecting Business Information 'Understanding the risks', published by the DTI, URN 96/939, 1996

[9] Protecting Business Information 'Keeping it Confidential', published by the DTI, URN 96/938, 1996

[10] Information Security Assurance Guidelines for the commercial sector, published by the DTI, URN 99/697, 1999

[11] ISO Guide 73: 2002 Risk Management – Vocabulary – Guidelines for use in standards

[12] OECD Guide on security for information systems and networks, September 2002

2.3 Definitions and Terminology

2.3.1 Asset
Anything that has value to the organization, its business operations and their continuity.

2.3.2 Impact *(source GMITS Part 1 ref. [3])*
The result of an unwanted incident.

2.3.3 Information
The meaning that is currently assigned to data by means of the conventions applied to those data.

2.3.4 Information security *(source ISO/IEC 17799 ref. [1])*
Protection of information for:

- Confidentiality: protecting sensitive information from unauthorised disclosure or intelligible interception;
- Integrity: safeguarding the accuracy and completeness of information and computer software;
- Availability: ensuring that information and vital services are available to users when required.

2.3.5 Information security management
Provision of a mechanism to enable the implementation of information security.

2.3.6 Information security policy
Rules, directives and practices that govern how assets, including sensitive information, are managed, protected and distributed within an organization.

2.3.7 Residual risk *(source Guide 73 ref. [11])*
The risk remaining after risk treatment.

2.3.8 Security control
A practice, procedure or mechanism that reduces security risks.

2.3.9 Risk *(source Guide 73 ref. [11])*
Combination of the probability of an event and its consequence.

2.3.10 Risk assessment *(source Guide 73 ref. [11])*
The overall process of risk analysis (systematic use of information to identify sources and to estimate the risk) and risk evaluation (process of comparing the estimated risk against given risk criteria to determine the significance of risk).

2.3.11 Risk management *(source Guide 73 ref. [11])*
Coordinated activities to direct and control an organization with regard to risk.

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

2.3.12 Risk treatment *(based on Guide 73 ref. [11][1])*

[1] *Guide 73 used the word 'measure' for what is called 'control' in ISO/IEC 17799 and BS 7799-2, the rest of the definition is exactly the same.*

Process of selection and implementation of controls to modify risk.

2.3.13 Statement of applicability *(source BS 7799 Part 2 ref. [2])*

Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS, based on the results and conclusions of the risk assessment and risk treatment processes.

2.3.14 Threat *(source GMITS Part 1 ref. [3])*

A potential cause of an unwanted incident, which may result in harm to a system or organization.

2.3.15 Vulnerability *(source GMITS Part 1 ref. [3])*

A weakness of an asset or group of assets, which can be exploited by a threat.

3 RISK ASSESSMENT PROCESS

The assessment of risk depends upon the following factors:

- Identification and valuation of assets (see 3.1 and 3.2);
- Identification of all security requirements, i.e. threats and vulnerabilities, legal and business requirements (see 3.3);
- Assessment of the likelihood of the threats and vulnerabilities to occur, and the importance of legal and business requirements (see 3.4);
- Calculation of risk resulting from these factors (see 3.5);
- Selection of the appropriate risk treatment option (see 3.6); and
- Selection of controls to reduce the risks to an acceptable level (see 3.7).

3.1 Asset Identification

An asset is something that has value or utility to 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[2] is vital in order to maintain appropriate protection of an organization's assets. These two aspects should be a major responsibility of all management levels[3]. It is important that an inventory is drawn up of the major assets. 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.

Each asset within this boundary should be clearly identified and appropriately valued (see also Section 3.2 below), and its ownership and security classification agreed and documented (see ISO/IEC 17799 [1] Section 5, and [8]/[9]). Examples of assets includes:

- ***Information assets***: databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fallback arrangements;
- ***Paper documents***: contracts, guidelines, company documentation, documents containing important business results;
- ***Software assets***: application software, system software, development tools and utilities;

---

[2] *Section 3 of ISO/IEC 17799 defines two specific objectives in regard to assets: (I) 3.1 Accountability for assets, and (ii) 3.2 Information classification.*

[3] *Accountability for assets helps ensure that adequate information security is maintained. Owners should be identified for major assets and assigned the responsibility for the maintenance of appropriate security controls. Responsibility for implementing security controls may be delegated, though accountability should remain with the nominated owner of the asset.*

- ***Physical assets***: computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation;
- ***People***: personnel, customers, subscribers;
- ***Company image and reputation***;
- ***Services***: computing and communications services, other technical services (heating, lighting, power, air-conditioning).

Result of Step 3.1:
The result of this step should be an inventory containing all major assets in the ISMS considered, their location and their owner.

3.2 Asset Valuation

Asset identification and valuation, based on the business needs of an organization, is a major factor 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 given certain opportunities. These values are usually expressed in terms of the potential business impacts of unwanted incidents such as the disclosure, modification, non-availability and/or destruction of information, and other assets. These incidents could, in turn, lead to financial losses, loss of revenue, market share, or company image.

The input for the valuation of assets should be provided by owners and users of assets, those who can speak authoritatively about the importance of assets, particularly information, to the organization and its business.

The values assigned should be related to the cost of obtaining and maintaining the asset, and the impacts the loss of confidentiality, integrity and availability could have to the business of the organization. In order to consistently assess the asset values and to relate them appropriately, a value scale for assets should be applied.

For each of the assets, values should be identified that express the business impacts if the confidentiality, integrity or availability, or any other important property[4] of the asset is damaged. An example of such a valuation scale could be:

- A distinction between low, medium and high;

[4] *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. In such cases, an additional criterion should be introduced to match these requirements.*

- In more detail: negligible - low - medium - high - 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.

Giving a good interpretation of what the values mean in terms of the business of the organization is very important when speaking to owners and users to gain input for the asset valuation.

Result of Step 3.2:
As the result of this step, the asset inventory should be extended to include, for each of the identified assets, a value for each of the criteria, i.e. for confidentiality, integrity and availability, and any other criteria, if applicable.

3.3 Identification of Security Requirements

3.3.1 Sources of Requirement

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

- The unique set of threats and vulnerabilities which could lead to significant losses in business if they occur;
- The statutory and contractual requirements which have to be satisfied by the organization, its trading partners, contractors and service providers;
- The unique set of principles, objectives and requirements for information processing that an organization has developed to support its business operations and processes, and apply to the organization's information systems.

Once these security requirements have been identified, it is helpful to formulate them in terms of requirements for confidentiality, integrity, and availability.

At some point, either prior to starting the risk assessment activities, or before starting this step, 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 to select additional controls (see also Step 3.6) that are working well with those already in place. The Guide PD

3003 gives a possibility of checking the existing security status against ISO/IEC 17799 and BS 7799 Part 2.

3.3.2 Identification of Threats and Vulnerabilities

Assets are subject to many kinds of threats. A threat has the potential to cause an unwanted incident which may result in harm to a system or organization and its assets. This harm can occur from a direct or an indirect attack on an organization's information e.g. its unauthorised destruction, disclosure, modification, corruption, and unavailability or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit a vulnerability (see below) of the systems, applications or services used by the organization in order to successfully cause harm to the asset. Examples of threats are given in Annex A.1 and A.2 of this guide, and GMITS Part 3 and the publication 'Protecting Business Information' (see [8] and [9]), provides additional information on threats.

Vulnerabilities are weaknesses associated with an organization's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets. A vulnerability in itself does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset. The vulnerability identification should identify the weaknesses related to the assets in the:

- Physical environment,
- Personnel, management and administration procedures and controls,
- Hardware, software or communications equipment and facilities,

that may be exploited by a threat source to cause harm to the assets, and the business they support. Examples of vulnerabilities are given in Annex A.3 of this guide, and GMITS Part 3 provides additional information on vulnerabilities.
Please note: Depending on the risk assessment methodology used (see also Section 4 and Annex B.2), threats and vulnerabilities might or might not be assessed together. Both variations are possible, and should be decided upon when deciding on the overall risk assessment approach.

3.3.3 Legal, Regulatory and Contractual Requirements

The security requirements relating the set of statutory 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 vital that the

implementation, or absence, of security controls in each of the information systems do not breach any statutory, criminal or civil obligations, or commercial contracts. Therefore, the legal statutory and contractual requirements related to each of the assets should be identified.

3.3.4 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 do not impede efficient business operations. For each of the assets, the related business objectives and requirements should be identified.

Result of Step 3.3:
The result of Step 3.3 should be list of identified threats and vulnerabilities, legal/contractual and business requirements, for each of the assets identified in Step 3.1.

3.4 Assessment of the Security Requirements

Like for the valuation of assets, it is necessary for the valuation of security requirements to identify a scale for this valuation that is suitable to the risk assessment methodology applied (see also Section 4). In many cases, a simple three level scale, such as

- Low
- Medium
- High

will be sufficient, in order to not make the process overly complex.

3.4.1 Assessment of Threats and Vulnerabilities

After identifying the threats and vulnerabilities it is necessary to assess the likelihood that a combination of the threats and vulnerabilities occur.
Please note: Depending on the whether the threats and vulnerabilities are assessed separately or together, a separate valuation of threats and vulnerabilities or a combined assessment should be used.

The assessment of the likelihood of threats should take account of:

- Deliberate threats: the motivation, the capabilities perceived and necessary, resources available to possible attackers, and the perception of attractiveness;
- Accidental threats - how often it might occur, according to experience, statistics, etc., and geographical factors such as proximity to chemical or petroleum factories, in areas where extreme weather conditions are always possible, and factors that could influence human errors and equipment malfunction.

The overall likelihood for an incident to occur depends as well on the vulnerability of the assets, i.e. how easily they may be exploited. Accordingly, vulnerabilities should be rated with respect to some scale such as:

- Highly probable or probable – it is easy to exploit the vulnerability, there is no or very little protection in place;
- Possible – the vulnerability might be exploited, but some protection is in place;
- Unlikely or impossible – it is not easy to exploit the vulnerability, the protection in place is good.

Information used to support the threat and vulnerability assessment can be obtained from those people involved with the ISMS, and related business processes being considered. These people could be for example, personnel department staff, facility planning and IT specialists, as well as people responsible for security within the organization. It might also be useful to use threat and vulnerability lists (e.g. in Annex a and in GMITS, Part 3) and links between threats and controls from ISO/IEC 17799 given in Annex A in this guide.

3.4.2 Assessment of Legal and Business Requirements

In the same way as the threats and vulnerabilities have been assessed, a value should now be identified for the legal and business requirements (see also 3.3.3 and 3.3.4). This is necessary to allow the calculation of the risks related to these security requirements.

In order to assign a value to a specific legal or business requirement, it is necessary to identify:

- How serious the impact to the business is if the legal/contractual or the business requirement is not fulfilled;
- What consequences this might have for the asset considered, and the whole ISMS; and
- How likely this is to happen.

The results of these considerations should be used to identify for each asset and for each legal/contractual and each business requirement the appropriate value on the value scale for the security requirements.

Result of Step 3.4:
As the result of this step, a value should be assigned for all identified security requirements (see also Step 3.3 above).

3.5 Calculation of Security Risks

The objective of the risk assessment is to identify and assess the risks, based on the results of Steps 3.1 – 3.4. The risks are calculated from the combination of asset values and assessed levels of related security requirements.

There are different ways of relating these factors; for example, the values assigned to the assets, vulnerabilities and threats, and legal and business requirements are combined to obtain measures of risks. Several different ways to obtain these values are described in Annex B.2 'Types and Examples of Risk Assessment and Risk Management Methods', which are based on the concepts described in Section 3 of this guide.

It is important to note that there are no ‘right’ or ‘wrong’ ways of calculating the risks, as long as the concepts described in the previous sections are combined in a sensible way, and it is up to the organization to identify a method for risk assessment that is suitable to their business and security requirements.

Result of Step 3.5:
The result of this step should be a list of measured risks for each of the impacts of disclosure, modification, non-availability, and destruction for each of the assets within the scope of the ISMS being considered.

3.6 Identification and Evaluation of Options for Risk Treatment

When the risks have been identified and assessed, the next task for the organization is to identify and evaluate the most appropriate action of how to deal with these risks. This decision should be made based on the assets involved and the impacts on the business. Another important input into this decision

is the acceptable level of risk that has been identified following the selection of the appropriate risk assessment methodology (see also Section 4).

For the identified and assessed risks (as a result of the actions described in Steps 3.1 – 3.5), there are four possible actions an organization might want to take:

- Applying appropriate controls to reduce the risks (see also Section 3.7 below);
- Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and the criteria for risk acceptance (see also Section 4);
- Avoiding the risks (see 3.6.1 below);
- Transferring the associated business risks to other parties (see 3.6.2 below).

For each of the risks, these options should be evaluated to identify the most suitable one. The results of this activity should be documented, and later on in the process used to develop a risk treatment plan.

3.6.1 Risk Avoidance

Risk avoidance describes any action where assets are moved away from risky areas (e.g. physical areas or business processes). This can, for example, 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.

When evaluating the option of risk avoidance, this needs to be balanced against business and monetary needs. For example, it might be inevitable for an organization to use the Internet or e-commerce because of business demands, despite of all their concerns about hackers, and 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.

3.6.2 Risk Transfer

Risk transfer might be the best option if it seems impossible to avoid the risk, and it is difficult, or too expensive, to achieve appropriate reduction of risk. For example, risk transfer can be achieved by taking

out insurance to a value commensurate with the assessed asset values and related risks, taking also into account the importance for the business processes of the organization.

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 that all security requirements, control objectives and controls are included in associated contracts to ensure that sufficient security will be in place. What should be kept in mind is that, in many cases, the ultimate responsibility for the security of the outsourced information and information processing facilities remains with the original organization.

Another example of risk transfer might be where assets at risk are moved outside the scope of the ISMS. This can make the protection of particularly sensitive information easier and cheaper, but care should be taken to include all assets needed for the business carried out in the ISMS via interfaces and dependencies.

Result of Step 3.6:
As a result of this step, the suitable risk treatment option should be identified and documented for all risks that have been assessed following the process described in Steps 3.1 – 3.5.

3.7 Selection of Security Controls

3.7.1 About the Selection of Security Controls

In order to reduce the assessed risks within the scope of the ISMS being considered, appropriate and justified security controls should be identified and selected. Controls can be selected from ISO/IEC 17799 or BS 7799 Part 2, Annex A, and also from additional sources, as and when necessary. The aim of control selection is to reduce risks to a level that is acceptable for the organization. This selection should be supported by the results of the risk assessment, for example, the vulnerabilities with associated threats indicate where protection may be needed, and what form it should take. Especially for the purpose of certification, the links to the risk assessment should be documented to justify the selection (or otherwise) of the controls.

Already implemented controls should be re-examined in terms of cost comparisons, including maintenance, with a view to removing or improving them if they are not effective enough. Here it should be noted that sometimes it is more expensive to remove an inappropriate control than to leave it

in place, and maybe add another control. This process should include the results of the "Check" activity in the PDCA model, if a previous risk assessment has been made.

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

- Ease of use of the control,
- Transparency to the user,
- The help provided to the users to perform their function,
- The relative strength of the controls, and
- The types of functions performed - prevention, deterrence, detection, recovery, correction, monitoring, and awareness.

Generally, a control will fulfil more than one of these functions and the more it can fulfil the better. When examining the overall security, or set of controls to be used, a balance should be maintained between the types of functions if at all possible. This helps the overall security to be more effective and efficient. Control selection should also always include a balance of operational (non-technical) and technical controls supporting and complementing each other. Operational controls include those, which provide physical, personnel, and administrative security.

Besides the very important risk reduction (see also Section 3.7.2 below), also the cost factor should be considered for control selection. It would be inappropriate to recommend controls, which are more expensive to implement and maintain than the previously agreed budget assigned for security, and cheaper alternatives should be sought. However, great care should be taken if the budget reduces the number or quality of controls to be implemented since this can lead to an unwanted acceptance of risks. The established budget for controls should only be used as a limiting factor with considerable care.

Examples are provided in Annex A on the selection of specific controls from ISO/IEC 17799 in accordance with a number of example threats. More about control selection can also be found in PD 3005.

3.7.2 Risk Reduction and Acceptance

For all those risks where the option 'risk reduction' has been chosen in Section 3.6 above, appropriate controls need to be selected to reduce the risks to the level that has been identified as acceptable. For the identification of controls it is useful 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 threat or vulnerability that causes the risk;
- Ensuring the fulfilment of legal or business requirements;
- Reducing the possible impact if the risk occurs;
- Detect unwanted events, react, and recover from them.

Which of these ways (or a combination of them) an organization chooses to adopt to protect its assets within the ISMS is a business decision and depends on the business environment and 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.

After identifying suitable controls to reduce a specific risk to the acceptable level, it should be assessed how much these controls, if implemented, will reduce the risk – this reduced risk is called residual risk. This residual risk is generally difficult to assess, but at least an estimation on how much the controls reduce the level of the associated security requirements value should be identified, to ensure that sufficient protection is achieved.

If the residual risk is unacceptable, a business decision needs to be made on how to deal with this. One option is to select more controls in order to finally reduce the risk to an acceptable level. Whilst it is generally good practice to not tolerate unacceptable risks, it might not always be possible or financially feasible to reduce all risks to the acceptable level.

After the implementation of the selected controls, there will always be risks remaining. This is because organization's information systems can ever be made absolutely secure. Because of this, it is necessary to check the implementation, and the outputs of the controls (such as incident reports or log files) to finally assess how well the controls implemented are working. These actions are part of the "Check" phase in the PDCA model, and the identified improvements should then be implemented in the "Act" phase to achieve more effective security.

Result of Step 3.7:

As a result of this step, controls should have been selected to reduce all those risks that have been identified to be treated with this option in Step 3.6. In addition, the links to the risk assessment results should be documented, and it should be ensured that all risks are reduced as far as possible.

4 APPROACHES TO RISK ASSESSMENT

4.1 Introduction

Section 3 provides a description of the overall risk assessment processes. As already mentioned in Section 3, it is up to the organization to select the appropriate approach for the risk assessment, so this section describes different options for an organization-wide approach for risk assessment. The different approaches vary in the time and effort involved and the depth of detail explored. Despite of the fact that the organization is free to chose the risk assessment approach, it needs to be ensured that the risk assessment method(s) applied are suitable and detailed enough for the organization's business and security requirements.

If, for example, an organization or the ISMS and its assets have at most low to medium security requirements, a Basic Risk Assessment (see 4.2) approach might be sufficient. If the security requirements are higher, requiring more detailed and special assessment, then a Detailed Risk Assessment (see 4.3 and 4.4) approach may be necessary. In any case, it should be ensured that the chosen approach fulfils all criteria from Section 4.2.1 in BS 7799 Part 2, namely:

- identifying the assets (see also 3.1);
- identifying threats and vulnerabilities, and any other applicable security requirements (see also 3.3);
- identifying the impacts that losses of confidentiality, integrity and availability might have on the assets (see also 3.2);
- based on this information, assessing the harm and the likelihood of risks occurring, and estimating the levels of risk (see also 3.4 and 3.5);
- identifying the most appropriate risk treatment option (see also 3.6); and
- select control objectives and controls to reduce the risks to an acceptable level (see also 3.7).

4.2 Basic Risk Assessment

The Basic approach involves the selection of a set of security controls based on a simple and straightforward application of the process described in Section 3.

This approach enables an organization to establish its ISMS(s) by achieving a basic level[5] of protection, based on the identification and assessment of the basic and essential needs and requirements of the organization. The basic level of security achieved, using this straightforward and easy to use approach,

[5] *Sometimes referred to as a baseline level of security.*

may be suitable for a part of an organization with low security requirements, or – in some cases – even for the whole organization if its security requirements are sufficiently low. What is important for any organization regarding BS 7799 Part 2 certification is that they are able to justify why the baseline approach is sufficient, if this is what has been chosen.

A typical example of the use of this approach might be a part of an organization whose business operations are not very complex and whose dependency on information processing and networking is not that extensive. This might also be the case with some SMEs, however, there may be SMEs whose business environment is more complex and they are dependent on extensive use of technology based information systems, and are involved in the processing of commercially sensitive information.

In the context of BS 7799-2, this approach would involve making a systematic assessment of the organization's security requirements (see Section 3.3 and 3.4) for the information and the assets being considered, identifying those control objectives that should be satisfied and then a selection of a set of controls to meet these objectives.

This basic risk assessment approach involves the following activities based on the processes described in Section 3 and should take into account the security requirements from all sources.

Risk Assessment and Management Tasks	Basic Risk Assessment Activities
Asset Identification and Valuation (3.1 and 3.2)	List those assets associated with the business environment, operations and information being assessed within the scope of the ISMS, and identify their values, using a simple valuation scale.
Identification and Assessment of Security Requirements (3.3 and 3.4)	The security requirements should be identified (this can be supported by the use of checklists of generalised or commonly known threats and vulnerabilities), and all identified security requirements should be valued, using a simple valuation scale
Risk Calculation (3.5)	Calculate the risks, based on the information on assets and security requirements, using a simple calculation scheme.
Identification and Evaluation of the Risk Treatment Options (3.6)	Identify the suitable risk treatment action for each of the identified risks; document the results for the risk treatment plan.
Selection of Security Controls and Risk Reduction and Acceptance (3.7)	For each of the identified assets identify the control objectives and controls in ISO/IEC 17799:2000 that are relevant. Ensure that the control objectives and controls selected reduce the risks to an acceptable level.

Using lists of generalised or commonly known threats and vulnerabilities can help to guide and direct the thinking process behind the assessment activities. More details of this basic approach and associated control selection are described in GMITS Part 4 and PD 3005.

This approach can be applied by using a simplified version of the matrix method given in Annex B (see B.2.2). Such an approach could involve, for example, two levels of security requirements (e.g. High and Low), and a valuation of assets using a predefined scale (e.g. High Value, Medium Value and Low Value).

The numbers in the table below represent a measure of risks (e.g. 0 to 4).

	Level of Security Requirements	**Low**	**High**
Asset Value	**Low Value**	0	2
	Medium Value	1	3
	High Value	2	4

The risk measures can be used to decide what risks should be dealt with first and need the most attention, and what the appropriate risk treatment options might be. For those risks where the option of risk reduction is chosen, an acceptable level of risk needs to be identified that is suitable to the business and security requirements for the ISMS considered. For the above example matrix it is recommendable that the acceptable level of risk is not chosen higher than 2.

There are a number of advantages with the Basic Risk Assessment approach, such as:

- A minimum of resources is needed for risk assessment, and the time and effort spent on control selection is reduced. Normally, no significant resources are needed to identify appropriate controls,
- The same or similar controls can be adopted for several assets without great effort. If a large number of an organization's assets operate in a common environment, and if the business and security requirements are comparable, these controls may offer a cost-effective solution.

The disadvantages of this approach include:

- If the security level is set too high, there might be too expensive or too restrictive controls selected for some assets, and if the level is too low, the security implemented might be not be sufficient for some assets,
- There might be difficulties in managing security relevant changes (as required in the 'Check' and the 'Act' part of the PDCA model). For instance, if changes to the overall ISMS business occur, it might be difficult to assess whether the original controls are still sufficient.

4.3 Detailed Risk Assessment

This approach involves conducting detailed risk assessment, which include the detailed identification and valuation of assets, and identification and assessment of the levels of security requirements. This information is used to assess the risks and is subsequently used for the identification and selection of security controls.

The selection of these controls is justified by the identified risks to the assets, and it is ensured that the risks are reduced to the acceptable level, if this risk treatment option was chosen.

Detailed risk assessment can be a very resource intensive process, and therefore needs careful establishment of boundaries of the business environment, operations, information and assets within the scope of the ISMS to be assessed. It is also an approach that requires constant management attention.

According to the risks assessed, controls can be selected from ISO/IEC 17799 in relation to those control objectives that should be satisfied. This overall approach is different from the Basic Risk Assessment approach given in Section 4.2 in that much more detailed analysis of the assets and the security requirements is carried out, using the concepts that have been described in Section 3, and assessment method like one of those given in Annex B, in order to relate the various values and to calculate the risks.

Risk Assessment and Management Tasks	**Detailed Risk Assessment Activities**
Asset Identification and Valuation (3.1 and 3.2)	Identify and list all those assets associated with the business environment, operations and information within the scope of the ISMS, define a value scale and for each asset assign values from this scale (one value for each: confidentiality, integrity and availability, and any other value, if applicable).
Security Requirements Identification (3.3)	Identify all security requirements (threats and vulnerabilities, legal and business requirements) associated with the list of assets within the scope of the ISMS.
Security Requirements Assessment (3.4)	Identify an appropriate valuation scale for the security requirements, and assign the appropriate value for each of the identified security requirements.
Calculation of Risks (3.5)	Calculate the risks (based on the assets and security requirements, and their values resulting from the above assessments) using, for example, one of the risk assessment methods outlined in Annex B, or any variant or similar type of method that is appropriate for the security requirements of the ISMS considered.
Identification and Evaluation of Options for the Treatment of Risks (3.6)	Identify a suitable risk treatment action for each of the identified risks. Evaluate that the identified option is realistic, suitable and in line with all business and security requirements, and document the results for the risk treatment plan
Selection of Security Controls, Reducing the Risks and Risk Acceptance	Determine the acceptable level of risk for the risk assessment methodology chosen, and ensure that this level of acceptable risk is appropriate for the business and security requirements of the ISMS considered. For those risks where the option of risk reduction was chosen, select, suitable control

	objectives and controls from ISO/IEC 17799 that will reduce these risks to an acceptable level. Assess how much the controls selected reduce the identified risks. For each of those risks that cannot be reduced to the acceptable level, identify additional action to deal with it (either management approval to accept the risk for business reasons, or to reduce it further).

The advantages of this approach are:

- An accurate and detailed view of the security risks is obtained leading to the identification of security levels which reflect the organization's security requirements of the assets and the ISMSs,
- The management of security relevant changes (as required in the 'Check' and the 'Act' part of the PDCA model) will benefit from the additional information obtained from a detailed risk assessment.

The disadvantage of this approach is:

- It takes a considerable amount of time, effort and expertise to get viable results.

4.4 Combined Approach

This approach involves first identifying those assets within the scope of the ISMS which are potentially at high risk or critical to business operations. Based on these results, the assets within the scope of the ISMS are categorised into those which require a Detailed Risk Assessment approach (see 4.3) to achieve appropriate protection and those for which the Basic Risk Assessment approach (see 4.2) is sufficient. This approach is a combination of the advantages of the approaches described in 4.2 and 4.3 above. Consequently, it provides a good balance between minimising the time and effort spent in identifying controls, while still ensuring that all of an organization's assets are assessed and protected appropriately.

In addition to having the combined advantages of the two approaches it also has the advantage that:

- Resources and money can be applied where they will be most beneficial, and an organization's information systems, which are likely to be at high risk, can be addressed early.

The disadvantage of this approach is:

- This may lead to inaccurate results if the identification of those information systems at high risk is incorrect, i.e. if systems for which a Detailed Risk Assessment is needed have been considered by only by a Basic Assessment approach.

4.5 Selection of a Suitable Risk Assessment/Management Approach

4.5.1 Selection Factors

As explained in the previous clauses of this section, there are different overall, organization-wide, approaches an organization can take to risk assessment. The previous clauses have indicated some of

the advantages and disadvantages of these approaches. Which approach is suitable for an organization is dependent on a number of factors, including:

- Their business environment and the kind of business conducted;
- The dependency on information processing and applications supporting their business;
- The complexity of the business and supporting systems, applications and services;
- The number of trading partners and external business and contractual relationships.

These factors should be generally common to all businesses, therefore when selecting an appropriate organization-wide, approach an organization needs to consider these factors together with the advantages and disadvantages of the approaches. It is up to the organization to make the decision of which approach to take, as long as the criteria set out in BS 7799 Part 2 (see also 4.1 above) are satisfied. As a general rule of thumb the more important and essential security is to the organization and for its business, and the more there is to lose, the more time and resources should be devoted to security.

4.5.2 BS 7799 ISMS Certification

With regard to certification of a BS 7799 Information Security Management System (ISMS) there is a requirement to do appropriate risk assessment review(s) and to document the results of this assessment in a Statement of Applicability (see Section 2). This is an important part of the certification process and it is therefore equally important that the organization has selected the most appropriate organization-wide, approach to risk assessment. More about this can also be found in the first part of Guide PD 3003.

4.6 Risk Assessment and SMEs

There is no general rule that says which approach to risk assessment is suitable to SMEs, since this decision is based on the business and information security requirements, and not necessarily on the size of the organization. The following are some notes for SMEs based on some general ideas of how SMEs might relate to the factors given in 4.5.1 above.

It is certainly the case that the less complex the business operations are and the fewer systems there are, the simpler the information security requirements might be, and this situation probably holds true for the majority of SMEs.

However, there are some SMEs whose business requirements could be quite involved. An SME might be a supplier to many other organizations and there may be a contractual agreement to implement a range of ISO/IEC 17799 controls. For example, the SME will need to consider those aspects of Section

4.2 of ISO/IEC 17799 (Security of Third Party Access), and whether any aspects of Section 8.7 (Data and Software Exchange), Sections 9.3/9.4/9.5 (Network/Computer/Application Access Control), and Section 10 (Systems Development and Maintenance) applies in their capacity as a supplier of a range of different services and products. In addition, they will certainly need to consider what aspects of Section 12 (Compliance) apply.

An SME's dependency on the use of information processing and computing systems may be very high and their business may be highly reliant on the use of such systems. For example, an SME might use such systems to produce information products for the entertainment industry where the content and design has a high market value in terms of intellectual property.

An SME needs to balance what resources it would need to devote to risk assessment in accordance with one of the three approaches (see Sections 4.2, 4.3 and 4.4) and the implementation of security controls to meet its own security requirements and those of its customers. As a minimum an SME will need to implement some security controls, whatever their business is, and the Basic Risk Assessment approach will enable them to establish what this should be. Certainly there is a need to have some form of security policy in place, to have some forms of access control and to be compliant with statutory and regulatory requirements. In addition, there may be a need to give special treatment to some specific requirements resulting from its business relationships, using some or all of a Detailed Risk Assessment approach, as described in Section 4.3.

ANNEX A EXAMPLES OF THREATS AND VULNERABILITIES

The following lists provide some examples of the threats and vulnerabilities associated with the ISO/IEC 17799 control objectives and controls. These do not represent an exhaustive list of threats and vulnerabilities and should only be taken as examples to illustrate the concepts and the relationship with the controls given in ISO/IEC 17799.

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. This may include some or all of the threats and vulnerabilities given in the lists below.

A.1 Example List of Threats

The following is an example list of threats derived from GMITS Part 3. This list of threats is presented here for illustrative purposes and should not be taken as definitive and complete.

Airborne particles/dust
Air conditioning failure
Bomb attack
Communications infiltration
Damage to communication lines/cables
Deterioration of storage media
Earthquake
Eavesdropping
Environmental contamination (and other forms of natural or man-made disasters)
Extremes of temperature and humidity
Failure of communications services
Failure of network components
Failure of power supply
Failure of water supply
Fire
Flooding
Hardware failure
Hurricane
Illegal import/export of software
Illegal use of software
Industrial action
Lightning
Maintenance error
Malicious software (e.g. viruses, worms, Trojan Horses)
Masquerading of user identity
Misrouting or rerouting of messages
Misuse of resources
Network access by unauthorized persons
Operational support staff error
Power fluctuation
Repudiation (e.g. of services, transactions, sending/receiving messages)
Software failure
Staff shortage
Theft
Traffic analysis
Traffic overloading
Transmission errors
Unauthorized use of software
Unauthorized use of storage media
Use of network facilities in an unauthorized way
Use of software by unauthorized users
Use of software in an unauthorized way
User error
Wilful damage

Depending on the type of threat, their 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	Unauthorised disclosure of the location of sites/buildings/offices containing critical and/or sensitive computing and processing facilities
Unauthorised disclosure of information	

A.2 Threat Examples and BS 7799

The following illustrates by example how the various threats given above relate to the control objectives given in BS 7799.

A.2.1 Section 5 Physical and Environmental Security

5.1 Secure areas

Objective: To prevent unauthorised access, damage and interference to IT services. IT facilities supporting critical or sensitive business activities should be housed in secure areas.

Fire	Flooding
Bomb attack	Hurricane
Earthquake	Industrial action
Environmental contamination (and other forms of natural or man-made disasters)	Lightning
	Theft
	Wilful damage

5.2 Equipment security

Objective: To prevent loss, damage or compromise of assets and interruption to business activities. Equipment should be physically protected from security threats and environmental hazards.

Airborne particles/dust	Hardware failure
Air conditioning failure	Maintenance error
Bomb attack	Malicious software (e.g. viruses, worms, Trojan Horses)
Environmental contamination (and other forms of natural or man-made disasters)	Network access by unauthorized persons
	Power fluctuation
Failure of power supply	Theft
Fire	User error
Flooding	Wilful damage

A.2.2 Section 6: Computer and network management

6.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of computer and network facilities. Responsibilities and procedures for the management and operation of all computers and networks should be established.

Air conditioning failure	Masquerading of user identity
Bomb attack	Misrouting or rerouting of messages
Communications infiltration	Misuse of resources
Earthquake	Network access by unauthorized persons
Failure of power supply	Operational support staff error
Fire	Software failure
Flooding	Theft
Hardware failure	Traffic overloading
Hurricane	Transmission errors
Industrial action	Use of software by unauthorized users
Lightning	Use of software in an unauthorized way
Maintenance error	User error
Malicious software (e.g. viruses, worms, Trojan Horses)	Wilful damage

A.2.3 Section 9: Business continuity planning

9.1 Aspects of business continuity planning

Objective: To have plans available to counteract interruptions to business activities. Business continuity plans should be available to protect critical business processes from the effects of major failures or disasters.

Bomb attack	Hurricane
Earthquake	Industrial action
Environmental contamination (and other forms of natural or man-made disasters)	Lightning
Failure of communications services	Staff shortage
Fire	Wilful damage
Flooding	

A.2.4 Section 10: Compliance

10.1 Compliance with legal requirements

Objective: To avoid breaches of any statutory, criminal or civil obligations and of any security requirements. The design, operation and use of IT systems may be subject to statutory and contractual security requirements.

Bomb attack	Misuse of resources
Communications infiltration	Network access by unauthorized persons
Eavesdropping	Theft
Illegal import/export of software	Unauthorized use of software
Illegal use of software	Use of network facilities in an unauthorized way
Masquerading of user identity	Use of software in an unauthorized way

10.2 Security reviews of IT systems

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

Bomb attack	Misuse of resources
Communications infiltration	Network access by unauthorized persons
Eavesdropping	Theft
Failure of communications services	Unauthorized use of software
Illegal import/export of software	Use of network facilities in an unauthorized way
Illegal use of software	Use of software by unauthorized users
Malicious software (e.g. viruses, worms, Trojan Horses)	Use of software in an unauthorized way
Masquerading of user identity	Wilful damage

10.3 System audit considerations

Objective: To minimise interference to/from the system audit process. There should be controls to safeguard operational systems and audit tools during system audits.

Communications infiltration	Masquerading of user identity
Eavesdropping	Misuse of resources
Failure of communications services	Network access by unauthorized persons
Illegal import/export of software	Theft
Illegal use of software	Unauthorized use of software
Malicious software (e.g. viruses, worms, Trojan Horses)	Use of network facilities in an unauthorized way

A.3 Example List of Vulnerabilities

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 may also exploit these vulnerabilities.

A.3.1 Personnel Security (BS 7799 Part 1: Section 4)

Vulnerability	The vulnerability could be exploited by
Absence of personnel	staff shortage
Unsupervised work by outside or cleaning staff	theft
Insufficient security training	operational support staff error
Lack of security awareness	user errors
Poorly documented software	operational support staff error
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
Inadequate recruitment procedures	wilful damage

A.3.2 Physical and Environmental Security (BS 7799 Part 1: Section 5)

Vulnerability	The vulnerability could be exploited 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

A.3.3 Computer and network Management (BS 7799 Part 1: Section 6)

Vulnerability	The vulnerability could be exploited by
Unprotected communication lines	eavesdropping
Poor joint cabling	communications infiltration
Lack of identification and authentication mechanisms	masquerading of user identity

Transfer of passwords in clear	network access by unauthorized users
Lack of proof of sending or receiving a message	repudiation
Dial-up lines	network access by unauthorized users
Unprotected sensitive traffic	eavesdropping
Single point of failure	failure of communications services
Inadequate network management	traffic overloading
Lack of care at disposal	theft
Uncontrolled copying	theft
Unprotected public network connections	use of software by unauthorized users

A.3.4 System access control/Systems development and maintenance (BS 7799 Part 1: Sections 7 and 8)

Vulnerability	The vulnerability could be exploited by
Complicated user interface	operational staff error
Disposal or reuse of storage media without proper erasure	use of software by unauthorized users
Lack of audit-trail	use of software in an unauthorized way
Lack of documentation	operational staff error
Lack of effective change control	software failure
Lack of identification and authentication mechanisms like user authentication	masquerading of user identity
No 'logout' when leaving the workstation	use of software by unauthorized users
No or insufficient software testing	use of software by unauthorized users
Poor password management (easily guessable passwords, storing of passwords, insufficient frequency of change)	masquerading of user identity
Unclear or incomplete specifications for developers	software failure
Uncontrolled downloading and using software	malicious software
Unprotected password tables	masquerading of user identity
Well-known flaws in the software	use of software by unauthorized users
Wrong allocation of access rights	use of software in an unauthorized way

ANNEX B TOOLS AND METHODS

B.1 Tools

A variety of methods exist for undertaking risk assessment and risk management reviews ranging from simple question and answer checklist based approaches 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 based products.

B.1.1 Features to Look for in a Risk Assessment Tool

Whatever methods or products are used by the organization, they should at least address the components, relationships between the components, and processes, as described in Sections 3 and 4 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.

What to look for in a risk assessment 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 to 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 may be more difficult to install or learn therefore it may 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, whether it has been installed and configured correctly; therefore availability of guidance on installation andb use may be essential.

B.2 Types and Examples of Risk Assessment Method

B.2.1 Overview of Risk Assessment

The process of risk assessment has a number of stages, which have been discussed in Section 3. Those stages are:

- Asset identification and valuation (see 3.1 and 3.2);
- Identification and valuation of security requirements (i.e. threats and vulnerabilities, legal and business requirements, see also 3.3. and 3.4);
- Risk calculation (see 3.5);
- Identification of a suitable option for risk treatment (see 3.6);
- Selection of control to reduce risks to an acceptable level (see 3.7).

The objective of risk assessment is to identify and assess the risks to which the information system and its assets are exposed, in order to identify and select appropriate and justified security controls. The assessment is thus based on the values of the assets and the levels of the security requirements, taking into account the existing/planned controls. This annex focuses on the first part of the risk assessment where the risks are identified and calculated (Steps 3.1 – 3.5 in Section3).

The asset values, or potential business impacts if an incident occurs, may be assessed in several ways, including using quantitative, e.g. monetary, and qualitative measures (which can be based on the use of adjectives such as moderate or severe), or a combination of both. A difficult part of the risk assessment process can be the assessment of threats and vulnerabilities. The probability of a threat occurring is affected by the following:

- The attractiveness of the asset - applicable when a deliberate human threat is being considered;
- The ease of conversion of the asset into reward - applicable if a deliberate human threat is being considered;
- The technical capabilities necessary to perform the threat - applicable to deliberate human threats;
- The likelihood of the threat;

- The susceptibility of the vulnerability to exploitation, applicable to both technical and non-technical vulnerabilities.

Many risk assessment methods make use of tables, and combine qualitative and quantitative measures. As mentioned before, there is no right or wrong method for risk assessment. Besides ensuring that the method used complies with the requirements laid out in BS 7799 Part 2, it is also important that the organization uses a method with which they are comfortable, have confidence and that will produce repeatable results. A few examples of table-based techniques are given below.

B.2.2 Matrix for Separate Threat/Vulnerability Assessment

In this example, threats and vulnerabilities are not combined as reasons for incidents (as in Section 3.3 or in PD 3005), but considered separately. This is another feasible way of risk assessment and is explained in detail e.g. in GMITS, Part 3, and also supported by several tools. If this method is chosen, care should be taken to give appropriate consideration of legal and business requirements.

The values for assets are obtained by interviewing the selected business personnel (the 'asset owners') who can speak authoritatively about the information, to determine the value and sensitivity of the asset. The interviews facilitate assessment of the value and sensitivity of the assets in terms of the worst case scenarios that could be reasonably expected to happen from incidents such as unauthorised disclosure, unauthorised modification, repudiation, non-availability for varying time periods, and destruction.

In order to take into account legal and business requirements in this method, the valuation for the assets should include issues such as:

- Personal safety;
- Personal information;
- Legal and regulatory obligations;
- Law enforcement;
- Commercial and economic interests;
- Financial loss/disruption of activities;
- Public order;
- Business policy and operations;
- Loss of goodwill.

Based on this valuation, the appropriate level on a valuation scale, in this example a scale from 1 to 4, should be identified for each of the potential losses, and each asset.

The next major activity is the completion of questionnaires for each asset, and for each of the threat s and vulnerabilities that relate to this asset to enable the assessment of the levels of threats (likelihood of occurrence) and levels of vulnerabilities (ease of exploitation by the threats to make incidents happen). Each question answer attracts a score. This identifies threat and vulnerability levels on a predefined scale (in the example below, a Low – Medium – High scale is used, as shown in the matrix below). Information to complete the questionnaires should be gathered from interviews with appropriate technical, personnel and accommodation people, possible physical location inspections and reviews of documentation.

The asset values, and the threat and vulnerability levels, are matched in a matrix such as that shown below, to identify for each combination the relevant measure of risk on a scale of 1 to 8:

	Levels of Threat	Low			Medium			High		
	Levels of Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	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. If there is a vulnerability without a corresponding threat, or a threat without corresponding vulnerability, there is presently no risk (but care should be taken in case this situation changes!). Now the appropriate row in the matrix is identified by the asset value, and the appropriate column is identified by the severity of the threat and the vulnerability. For example, if the asset has the value 3, the threat is 'high' and the vulnerability '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. Additional columns and rows will necessitate additional risk measures. Once a risk assessment review has been completed for the first time, the results of the review (assets and their values, threat/vulnerability 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.

B.2.3 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 (taking account of threats and vulnerabilities or any other security requirements that might cause a particular incident). The first step is to evaluate the impact (asset value) on a predefined scale, e.g., 1 through 5, of each asset (column "b" in the table below). The second step is to evaluate the likelihood of incident occurrence on a predefined scale, e.g., 1 through 5, of each incident (column "c" in the table below). The third step is to calculate the measure of risk by multiplying (b x c). Finally the incidents can be ranked in order of their "exposure" factor. Note that in this example 1 is taken as the lowest impact and the lowest likelihood of occurrence.

Incident descriptor (a)	Impact (asset) value (b)	Likelihood of incident 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

As shown above, this is a procedure which permits different incidents with differing impact and likelihood of occurrence to be compared and ranked in order of priority, as shown here. In some instances it will be necessary to associate monetary values with the empirical scales used here.

B.2.4 Assessing the Risks for Systems

In this example, the emphasis is placed on determining which systems should be given priority, taking into account incidents and their impacts. This is done by assessing two values for each asset and risk, which in combination will determine the score for each asset. When all the asset score for the systems are summed, a measure of risk to that information system is determined.

First, a value is assigned to each asset. This value relates to the potential damage, which can arise if the asset is threatened. For each applicable threat to the asset, this asset value is assigned to the asset.

Next a frequency value is assessed for each incident, like described above in B.2.3. Then, an asset/incident score is assigned by finding the intersect of asset value and frequency value in the table below.

Asset Value	0	1	2	3	4
Incident Frequency Value					
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

The final step is to total all the asset total scores for the assets of the system, producing a system score. This can be used to differentiate between systems and to determine which system's protection should be given priority. The following is an example:

Suppose System S has three assets A1, A2 and A3. Also suppose there are two incidents I1 and I2 applicable to systems S. Let the value of A1 be 3, similarly let the asset value of A2 be 2 and the asset value of A3 be 4.

If for asset A1 an incident I1 frequency value is 1, the asset/incident score A1/I1 can be derived from the table above as the intersection of asset value 3 and incident frequency value 1, i.e. 4. Similarly, for A1/I2 let the incident likelihood of occurrence be 3, giving an A1/T2 score of 6.

Now the total asset score (A1_total) for all incidents for the particular assets considered can be calculated, and then the total asset score is calculated for each asset and applicable threat. The total system score is calculate by adding A1_total + A2_total + A3_total to give the overall score of the system.

In this way, different systems can be compared to establish priorities.

B.2.5 Distinction between Acceptable and Not Acceptable Risks

Another way of measuring the risks is to only distinguish between acceptable and not acceptable risks. The background of this is that the measures of risks are only used to rank the risks in terms of where action is needed most urgently, and the same can be achieved with less effort.

With this approach, the matrix used simply does not contain numbers but only As and Ns stating whether the corresponding risk is acceptable or not. For example, the matrix in B.2.4 could be changed into:

Damage Value	0	1	2	3	4
Incident Frequency Value					
0	T	T	T	T	N
1	T	T	T	N	N
2	T	T	N	N	N
3	T	N	N	N	N
4	N	N	N	N	N

Again, this is only an example, and it is left to the user where to draw the line between acceptable and not acceptable risks.