Guide on the selection of BS 7799 Part 2 controls

BSi
Business Information

Guide on the Selection of BS 7799 Part 2 Controls

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

CONTENTS

Introduction

All types of organization, whether large, medium or small, will have requirements for protecting its information. These security requirements will depend on the nature of its business, how it organises its business, its business processes, what technology it uses, the business partners it trades with, the services and service providers it uses and the risks it is facing. One way of fulfilling security requirements is to select control objectives and controls from BS 7799 Part 2 to protect the organization's assets.

Security requirements

The identification of security requirements gives important input into the control selection. Security requirements describe the aims of, and needs for, the security that need to be fulfilled to allow an organization successful and secure conduct of business. For the purpose of this guide, the three main sources of security requirements[1] are those:

- derived from **risks to the organization and its information processing facilities** – consideration should be given to the assets, the vulnerabilities associated with the assets, the threats exploiting these vulnerabilities and the possible impact/damage that the resulting risks may have on the business of the organization, e.g.

  - disclosure of confidential information because of a hacker gaining access into the organization's network,
  - modification of payment details being sent across the Internet,
  - destruction of information because of a system crash;

- **legal, statutory and regulatory requirements and contractual obligations** that an organization, its trading partners, contractors and service providers have to satisfy, e.g.

  - rules for software copying,
  - safe keeping of organizational records,
  - data protection;

- other forms of requirement associated with **business processes, standards and objectives** for information processing that an organization has developed or needs to implement to support its operations, e.g.

  - assurance that the program that calculates construction details for a product delivers correct outputs,
  - compliance with health and safety standards,
  - use of electronic mail within the organization to exchange information.

Risk assessment

One of the main ways of identifying requirements for protecting the organization's information is by conducting risk assessments (see also PD 3002 'Guide to BS 7799 Risk Assessment' for more information). Having identified the risks for the information processing facilities considered, an organization is able to:

- review the consequences of these risks (e.g. what their impact on and damage to the organization's business might be);

[1] *See also ISO/IEC 17799:2000 Introduction*

- make decisions on how to manage these risks, i.e.

  - knowingly and objectively accepting risks, providing that the criteria for risk acceptance are fulfilled;
  - avoid the risks,
  - transfer the business risks to other parties, or
  - reduce the risks to the acceptable level;

- take whatever action is necessary to treat the risks by implementing the decisions made, including selecting control objectives and controls selected from ISO/IEC 17799 to reduce the risks.

The process[2] of identifying risks, identifying and evaluating options for the treatment of risks, selecting control objectives and controls to reduce specific risks, and taking appropriate action to implement the other options for risk treatment, should take account of the economic, commercial and legal conditions of the business.

Risk assessment and risk treatment are important parts of applying the "Plan-Do-Check-Act" model to the ISMS process as defined in BS 7799 Part 2, and also relates to the application of the best practice advice given in ISO/IEC 17799. PD 3002 is a Guide on BS 7799 Risk Assessment that provides a good basis for understanding and applying risk assessment and risk treatment to BS 7799 Part 2 and ISO/IEC 17799.

The Plan-Do-Check-Act Model

The model, known as the "Plan-Do-Check-Act Model" (PDCA Model), is used in the BS 7799 Part 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 Part 2:2002 and PD 3001.

As also described in PD 3002, the process of risk assessment – and therewith the process of selecting control objectives and controls that is part of the risk assessment exercise – is an element of the "Plan" part of the PDCA model, as well as the "Check" part. In the "Plan" part, the selection of control objectives and controls simply has the function of satisfying security requirements, as explained in more detail below and dealt with in this guide in Section 3.

In the "Check" part of the PDCA process, the situation is slightly different. The controls that have been implemented (in the "Do" part as a result of the "Plan" activity) to fulfil the security requirements are now checked as to how well – or not – they are doing so. Controls where the existing protection is not sufficient (e.g. as shown by incident reports, audit findings, or other problems that are notified in the day-to-day work environment) should be identified in the "Check" process. This is supported by the link between ISO/IEC 17799 controls and security concerns given in Section 4 of this guide.

Selecting your control objectives and controls

Assessment of the security requirements should include consideration of the impacts in terms of the loss and damage to the organization's business processes and operations if these requirements are not met. This assessment should cover all assets within the scope of the ISMS considered, especially information processed by the organization, and, where applicable, including information or other assets processed by its business partners and its service providers.

[2] *A process is a set of linked activities that take an input and transform it to create an output. An example of a process is the identification of a set of risks followed by a sequence of linked business decisions to decide how to manage these risks resulting in a set of controls to reduce these risks.*

After all applicable security requirements for the assets and all related risks have been identified; the options for treating the risks and thereby fulfilling the security requirements should be identified and evaluated. If the business decision is to go for risk reduction, for some or all of the risks, then the process of selecting an appropriate set of control objectives and controls should take place. There are many different ways to satisfy these requirements through the selection and implementation of BS 7799 Part 2[3] control objectives and controls (see also ISO/IEC 17799 Introduction).

This guide provides an approach to this selection process in support of the organization's task of choosing a suitable set of control objectives and controls to meet its needs. This approach could be used by an organization as the basis for developing its own selection process customised to its particular business environment. It might be integrated into an existing approach an organization might have used in the past in assessing its security control objectives and controls according to the results of a risk assessment.

In accordance with BS 7799 Part 2, an organization needs to indicate in the Statement of Applicability the control objectives and controls that are applicable with suitable justification why they are needed and they also need to indicate which controls are not needed with appropriate justification why they are not needed.

Security concerns

Once the control objectives and controls from BS 7799 Part 2 have been implemented (as part of the "Do" activity that might also, in the end, lead to BS 7799 Part 2 certification (see PD 3001), it should be checked whether the implemented controls are working well. In Section 4, this guide provides help for this assessment by listing typical security concerns that might arise if a particular control from BS 7799 Part 2 has not been implemented correctly, or does not function well for some other reason. What can be done as part of the "Check" activity is to – for each of the implemented control – look at the list of security concerns that relate to this control. If any of those apply, then this is an indication that further action (re-assessment of risks and consideration of options to treat those risks, e.g. by implementing further controls or enhancing the current implementation) is necessary.

This Guide

This guide covers the selection of BS 7799 Part 2 controls as part of the general process of establishing and maintaining an information security management system (ISMS) and progression towards certification. It is complementary to guide PD 3002, which covers risk assessment.

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*

[3] *This does not discount the case where other controls not included in BS 7799 Part 2 need to be implemented.*

1 Selection Process

1.1 Requirements Assessment

The selection process for BS 7799 Part 2 control objectives and controls should consider the identified security requirements and through a sequence of linked business decisions define which control objectives and controls need to be implemented.

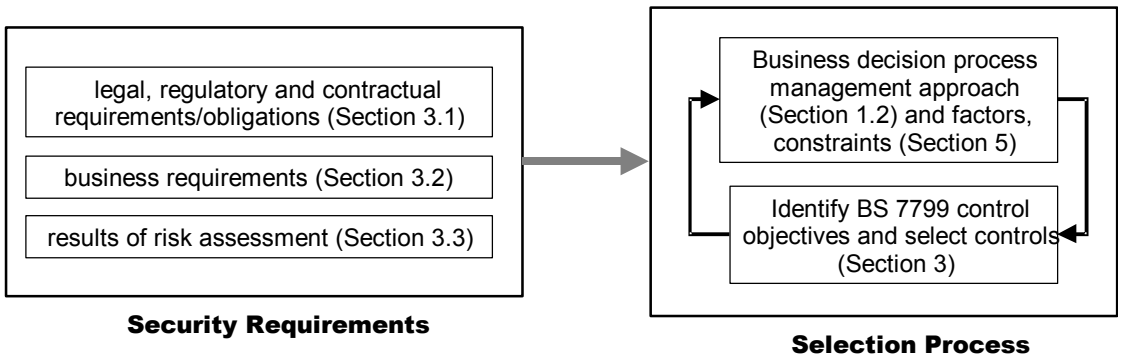

Figure 2: Security requirements and selection process

There are several approaches for the treatment of risk (see also Section 1.2.2 below). Simply speaking, an organization may decide to:

- do something to satisfy a security requirement (different options are explained in Sections 1.2.5 – 1.2.6);
- re-visit the requirement to check whether it could avoid doing something by taking other business actions (e.g. by re-organising, restructuring or re-engineering its business and business processes, see also Section 1.2.4);
- do nothing (on a short or long term basis, see also Section 1.2.3).

In all three cases the organization will need to consider what are the cost implications. For example, it should consider what investment is needed to implement an appropriate set of control objectives and controls as opposed to doing nothing, and the potential cost to the organization if something goes wrong.

Some requirements may be satisfied using a minimum set of standards or mandatory control objectives and controls, e.g. those set by law, where the decision as whether to implement controls is usually not optional and appropriate investment needs to be made to do something. Other requirements might need further assessment and a more detailed refinement of what is needed, possibly involving further business decisions and greater investment.

There is no standard or common approach to the selection of control objectives and controls. The selection process may not be straightforward and may involve a number of decision steps, consultation and discussion with different parts of the business and with a number of key individuals, as well as a wide-ranging analysis of business objectives. The selection process needs to produce an outcome that best suits the organization in terms of its business requirements, and the protection of its assets and its investment. It needs to be based on a clearly defined set of business goals and objectives or a mission statement.

The identification of the risks and the business and security requirements, and proper assessment of the feasible business investment is always a good security principle. An organization needs to ensure that it achieves the right balance between achieving security and the benefits of protection at the right investment, whilst staying profitable, successful, efficient and competitive.

1.2 Approaches to the Selection Process

1.2.1 General Aspects

The selection of control objectives and controls should be driven by the security requirements that need to be satisfied. The choice should be taken on how best to satisfy these requirements by treating the corresponding risks and the consequences if these requirements are not met.

An organization needs to establish a set of criteria for use in evaluating the options for risk treatment, which will assist in the decision process of deciding what the best options and alternatives are to meet its security requirements. The criteria needs to include all those constraints and factors which might be important to, or have an influence upon, the decision of what to select. Section 5 illustrates some of the factors and constraints that need to be considered.

What approach and methods an organization uses to assess its risks, decide on the appropriate for risk treatment option and selecting controls is entirely up to the organization to decide. It is important that whatever approach, methods and supporting tools an organization uses, that all risks resulting from the three categories of security requirements are assessed, risk treatment options commensurable with the business and security requirements are chosen and controls are selected accordingly.

If the decision has been to reduce a particular risk, the control selection process should be based on the security requirement (legal or business requirement or threat/vulnerability) that causes the risk and needs to:

- Identify and assess the controls (and possible alternatives) which satisfy the requirement commensurate with the business environment and weighed against the probable consequences;
- Select a set of controls that best meet the business criteria.

The sub-sections that follow discuss further the risk treatment options and the selection of controls based on the results of risk identification. More information about the risk assessment process as a whole can also be found in PD 3002 ‘Guide to BS 7799 Risk Assessment’.

1.2.2 Risk Treatment Options

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. The level of risk that has been identified as being acceptable needs to be taken into account.

For the identified risks, there are four possible actions an organization might want to take:

- Applying appropriate controls to reduce the risks (see 1.2.6 below);
- Knowingly and objectively accepting risks, providing they clearly satisfy the organization’s policy and the criteria for risk acceptance (see 1.2.3 below);
- Avoiding the risks (see 1.2.4 below);
- Transferring the associated business risks to other parties (see 1.2.5 below).

For each of the risks, these options should be evaluated to identify the most suitable one.

1.2.3 Knowingly accepting the risk

If it is decided to knowingly accept particular risks, this decision and the reasons for this decision need to be documented. There might be good business reasons to make this decision, but care should be taken that the implications of this decision have been considered, that sufficient security will still be in place, and that management approval of this decision is obtained.

1.2.4 Risk Avoidance

Risk avoidance describes actions where assets or parts of the ISMS or organization are moved away from risky areas (e.g. risky physical areas or risky business processes). This can, for example, 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 organisation 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.

1.2.5 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 better 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 an asset or 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.

1.2.6 Risk Reduction

Risk reduction is based on the selection of control objectives and controls to reduce the identified risks. If the option of risk reduction is chosen, the following types should be selected to achieve the desired reduction in risk and the appropriate level of protection (which of these functions or which

combination of them might be most appropriate depends on the threat/vulnerability, legal or business requirements that relates to the risk considered):

- Controls to reduce the likelihood of the threat occurring;
- Controls to reduce or remove the vulnerability;
- Controls to reduce the impact if the risk happened, i.e. to reduce the impact from a security breach to an acceptable level;
- Controls to detect an unwanted event;
- Controls to recover from an unwanted event.

A combination of these different ways to achieve protection is recommended. It should be ensured that controls complement and support each other; for example, technical controls should often be accompanied by procedural controls to make them more effective. A set of control objectives and controls should be selected from BS 7799 Part 2, Annex A, which are commensurate with the risks to be reduced, and it should be ensured that the risks are reduced to an acceptable level.

1.3 Overview of Selection Process

1.3.1 Selection of Control Objectives and Controls

The selection of control objectives and controls can be based on a number of factors and reasons relating to the three sources of security requirements (as described in the Introduction above), and the different ways of satisfying them. For example, the selection can be based on assessments of threats, vulnerabilities, likely impacts and thence risks, as well as on other factors such as legal and business requirements.

The selection of control objectives and controls is described in Sections 3, and is organised in the following way:

- For the security requirements based on legal and business considerations, a set of typical requirements such as compliance with different relevant laws or typical business needs is considered; each of these requirements is linked to a set of control objectives and controls from BS 7799 Part 2, Annex A, that can be used to fulfil these requirements (see Sections 3.1 and 3.2);
- For the security requirements resulting from the assessment of risks, a set of typical threats and vulnerabilities is considered; each of these threats or vulnerabilities is linked to a set of control objectives and controls from BS 7799 Part 2, Annex A, that can be used to protect against the threat or reduce or remove the vulnerability, respectively (see Section 3.3);
- The list of security concerns in Section 4 can be used for two different purposes: it can be used for a modification or extension of the set of control objectives and controls selected following Section 3.1; and it can be used to support the “Check” activity in the PDCA Model (see also Introduction), identifying what should be looked out for when checking the implemented control objectives and controls.

The lists of legal and business requirements, threats and vulnerabilities used in Sections 3.1 – 3.3 should not be considered as complete lists. They are just example lists and users should identify the applicable requirements, threats and vulnerabilities using the results of their own assessments, and identify additional requirements, threats and vulnerabilities as necessary.

The following figure gives an overview of the selection process

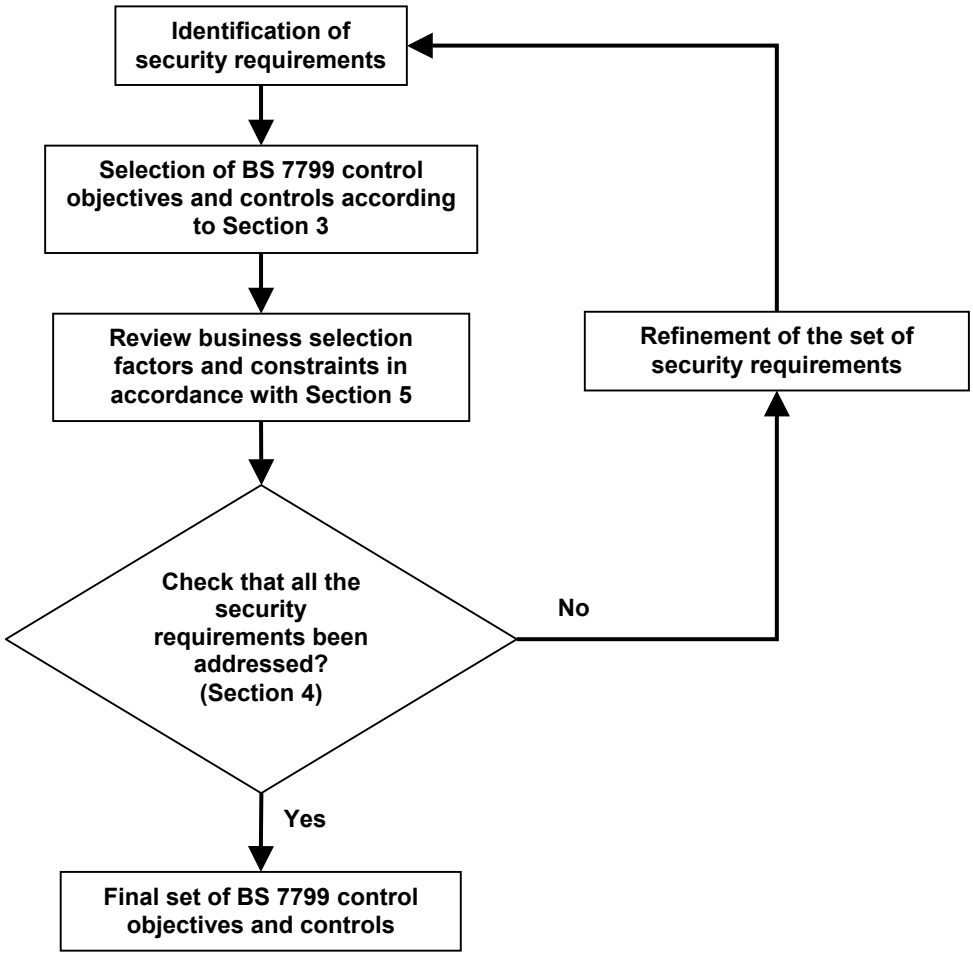

Figure 1: Control selection process

After going through Section 3.1 – 3.3, the reader should have identified a set of BS 7799 Part 2 control objectives and controls that are applicable to fulfil the relevant legal and business requirement, and protect against the assessed risks.

This set of control objectives and controls can be modified or extended to better fit the security requirements of the information processing facilities (either after having selected control objectives and controls, or as a result of the "Check" activity) with help of Section 4. If a particular security concern shown in Section 4 is not addressed by the set of control objectives and controls selected, additional control objectives or controls should be selected. If, on the other hand, all security concerns related to a particular control are not applicable for the specific assessment considered, the selection of this particular control is not necessary.

1.3.2 Selection Considerations

1.3.2.1 Factors and Constraints

The set of control objectives and controls selected to fulfil the security requirements should now be considered in the light of the selection factors and constraints described in Section 5. Such

selection factors and constraints can be financial or technical constraints or existing controls that have to be taken into account, and incorporated in the set of selected controls.

This is also important when an organization is preparing for the certification of its ISMS, constraints, like those described in Section 5, can be the reason behind the decision to not implement a specific BS 7799 Part 2 control objective or control. Such decisions and justifications should be stated in the statement of applicability.

Finally, it should be assessed whether the control objectives and controls selected address all of the security requirements that have been identified (see also 5.2.2). If all security requirements are satisfied, the selected controls should be implemented as soon as possible to achieve the required protection.

1.3.2.2 Use of risk assessment tools

Section 3.1 links legal and business requirements, threats and vulnerabilities to BS 7799 control objectives and controls. An organization may choose to use an automated risk assessment tool to assist in identifying and assessing its security requirements and risks.

There are many commercially available risk assessment tools to aid and assist organizations in this respect and it is a decision of the organization which tool it should employ (see also PD 3002 for information on tools) or whether it chooses not to use a tool at all. If the organization decides to use a tool, then the choice will depend on a number of factors (again see PD 3002 for more information). Some tools are more complex than others, some are more comprehensive in their analysis, some provide more functionality and reporting facilities, and some are relatively simple and straightforward in their approach. The list of tools and their features and characteristics is quite extensive. It is not the purpose of this guide to suggest or recommended any particular tool or approach, it is the decision of the organization to make that decision.

It should be noted that the terminology used to describe sets of threats, vulnerabilities, impacts and risks can and does vary across the range of tools available. It is also important to note that the terminology used in this guide is strictly that used in ISO/IEC 17799 and BS 7799 Part 2, although the reader should find that what is used has a high degree of commonality with that used in the majority of tools. It is not the purpose of this guide to enumerate all possible variants of the terminology used. Hence the reader will need to interpret where there are differences in terminology although in practice the scale of such differences is likely to be small.

1.3.2.3 Achieving the desired level on control

It should be noted that the control objectives and controls listed in Section 3.1 to achieve legal or business requirements or protect against threats or vulnerabilities are only suggestions based on the elements of best practice described in ISO/IEC 17799.

In many cases, there might not be a need to select all suggested control objectives and controls. Control objectives and controls should be selected to achieve the desired level of protection, based on the results of the risk identification.

Some controls might be applicable to high-risk situations and others might be applicable to low or medium risk situations. What is considered to be a high risk as opposed to what is considered a low risk depends on the specific judgement of the organization and its business. The loss of an asset of a certain monetary value to one organization may be devastating, to another sustainable and to another quite acceptable. In all three cases the organizations may classify what is a high and a low risk in different ways, as they might define what level of loss is tolerable or sustainable according to the size and scale of their business operations and their financial state.

Clearly some controls are, relatively speaking, loosely associated with any ranking scheme for risks. Having virus protection installed in systems is good common sense. Where as the need for

encryption to protect sensitive information is not, in general, a common requirement. Which applications and assets need to be protected by encryption will depend on the perceived level of threat and risk (more on the topic of risk assessment and risk reduction can be found in PD 3002).

Some of the controls in BS 7799 Part 2, or some parts of them, might not be necessary to be implemented in all circumstances since, e.g. they might be designed for large organizations or only applicable for some specific businesses e.g. involving networking, or providing a high level of protection.

Given the possible number of permutations and ranking schemes that could be used by organizations in accordance with their judgement of the risk, this guide does not go into that level of detail. However it is very important that in the selection process an organization does take into account the perceived level of risk in order to select the right control objectives and controls for the purpose. For example, there might be a need to implement an identification and authentication system. There are several controls that will satisfy this requirement ranging from passwords and similar techniques through to token based challenge and response techniques and cryptographic based techniques. Which controls are selected will depend on the level of perceived risk. In one environment password control may be sufficient, in another a token-based set of controls might be better. The perceived risk, which control and the cost of implementing the various control options will be a management decision which needs to weigh up all these factors.

2 References and Definitions

2.1 References

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

[2] BS 7799 - Part 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 TR 13335-5:2001 Guidelines for the Management of IT Security (GMITS) Part 5: Safeguards for External Connections

[8] ISO Guide 73 Risk Management – Vocabulary – Guidelines for use in standards, 2002

2.2 Definitions

2.2.1 Asset

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

2.2.2 Impact *(source GMITS Part 1 ref. [3])*

The result of an unwanted incident.

2.2.3 Information

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

2.2.4 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

2.2.5 Information security management

Provision of a mechanism to enable the implementation of information security.

2.2.6 Information security policy

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

2.2.7 Security control

A practice, procedure or mechanism that reduces security risks.

2.2.8 Risk *(source Guide 73 ref. [8])*

Combination of the probability of an event and its consequence.

2.2.9 Risk assessment *(source Guide 73 ref. [8])*

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).

2.2.10 Risk management *(source Guide 73 ref. [8])*

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.

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

Process of selection and implementation of controls to modify risk.

2.2.12 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.

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

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

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

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

3 Selection of Part 2 Control Objectives and Controls

This section describes how to select BS 7799 Part 2 control objectives and controls[4] that can be used satisfy security requirements identified from the three sources described in the Introduction. As explained in Section 1.3.1, the controls selected in this section are subject to further consideration, taking into account selection factors and constraints, and finally it should be assessed whether these controls are sufficiently address all security requirements and control objectives.

3.1 Legal requirements

As described in BS 7799 Part 2 Control A.12.1.1, legal requirements applicable to the organization or the ISMS considered should be identified and documented. These requirements can be supported by BS 7799 Part 2 controls. The following table describes which BS 7799 Part 2 control objectives and controls can be used to support, or should be considered with, the legal requirements given in ISO/IEC 17799, Clause 12. It should be noted that this is not a complete list of legal requirements.

The following legal requirements are addressed in this Guide.

Requirement	Guide Reference
Intellectual property rights (IPR) and software copyright	3.1.1
Safeguarding of organizational records	3.1.2
Data protection and privacy of personal information	3.1.3
Prevention of misuse of information processing facilities	3.1.4
Regulation of cryptographic controls	3.1.5
Evidence	3.1.6

This is not a definitive list of requirements and should be used only as a basis for developing an organization's own list of requirements based on its specific business environment. Each organization should identify the set of legal, statutory or regulatory requirements, using the above list as a start from which the applicable ones should be identified, followed by an identification of all applicable additional requirements that need to be satisfied. Some of these requirements will form part of the contractual obligations with other business partners. There might also be other contractual requirements, which may need to be considered, e.g. in the case of outsourcing or third party service delivery. It should be ensured that controls are in place to support these requirements.

3.1.1 Intellectual property rights (IPR) and software copyright

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation

[4] *The numbers used to refer to control objectives and controls are the numbers used in BS 7799 Part 2, Annex A. To obtain the ISO/IEC 17799 numbers, just remove the 'A.' at the beginning of the number.*

BS 7799 Part 2 Control Objectives and Controls
A.4.2 Security of third party access *To maintain the security of organizational information processing facilities and information assets accessed by third parties* A.4.2.1 Identification of risks from third party access A.4.2.2 Security requirements in third party contracts
A.4.3 Outsourcing *To maintain the security of information when the responsibility for information processing has been outsourced to another organization* A.4.3.1 Security requirements in outsourcing contracts
A.5.1 Accountability for assets *To maintain appropriate protection of organizational assets* A.5.1.1 Inventory of assets
A.5.2 Information classification *To ensure that information assets receive an appropriate level of protection* A.5.2.1 Classification guidelines A.5.2.2 Information labelling and handling
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.5 Disciplinary process
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy A.7.3.2 Removal of property
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.6 External facilities management

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchange agreements A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems
A.9.1 – A.9.6 Access control All control objectives and controls in Clauses A.9.1 – A.9.6 apply.
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.5 Outsourced software development
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.2 Intellectual property rights (IPR)

3.1.2 Safeguarding of organizational records

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.5.1 Accountability for assets *To maintain appropriate protection of organizational assets* A.5.1.1 Inventory of assets
A.5.2 Information classification *To ensure that information assets receive an appropriate level of protection* A.5.2.1 Classification guidelines A.5.2.2 Information labelling and handling

BS 7799 Part 2 Control Objectives and Controls
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process
A.7 Physical and environmental security All control objectives and controls in Clause A.7 apply.
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.1 Management of removable computer media A.8.6.3 Information handling procedures
A.9.1 – A.9.6 Access control All control objectives and controls in Clauses A.9.1 – A.9.6 apply.

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption A.10.3.3 Digital signatures A.10.3.5 Key management
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.3 Safeguarding of organizational records

3.1.3 Data protection and privacy of personal information

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.5.2 Information classification *To ensure that information assets receive an appropriate level of protection* A.5.2.1 Classification guidelines A.5.2.2 Information labelling and handling
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.3 Confidentiality agreements A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process

BS 7799 Part 2 Control Objectives and Controls
A.7 Physical and environmental security *All control objectives and controls in Clause A.7 apply.*
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.4 Segregation of duties
A.8.3 Protection from malicious *To protect the integrity of software and information software* A.8.3.1 Controls against malicious software
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.1 Management of removable computer media A.8.6.2 Disposal of media A.8.6.3 Information handling procedures
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* All controls in Clause A.8.7 apply.
A.9.1 – A.9.6 Access control All control objectives and controls in Clauses A.9.1 – A.9.6 apply.
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption A.10.3.3 Digital signatures A.10.3.5 Key management

BS 7799 Part 2 Control Objectives and Controls
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.4 Data protection and privacy of personal information

3.1.4 Prevention of misuse of information processing facilities

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.4 Authorisation process for information processing facilities
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.2 Personnel screening and policy A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process
A.7 Physical and environmental security All control objectives and controls in Clause A.7 apply.
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.1 Documented operating procedures A.8.1.4 Segregation of duties A.8.1.5 Separation of development and operational facilities
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software

BS 7799 Part 2 Control Objectives and Controls
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems A.8.7.7 Other forms of information exchange
A.9.1 – A.9.6 Access control All control objectives and controls in Clauses A.9.1 – A.9.6 apply.
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.5 Prevention of misuse of information processing facilities
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.2 Protection of system audit tools

3.1.5 Regulation of cryptographic controls

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.2 Personnel screening and policy A.6.1.4 Terms and conditions of employment

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems A.8.7.7 Other forms of information exchange
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* All controls in Clause A.10.3 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.6 Regulation of cryptographic controls

3.1.6 Evidence

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.3 Allocation of information security responsibilities A.4.1.6 Co-operation between organizations
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up A.8.4.2 Operator logs A.8.4.3 Fault logging
A.9.2 User access management *To prevent unauthorised access to information systems* A.9.2.1 User registration A.9.2.3 User password management
A.9.3 User responsibilities *To prevent unauthorised user access* A.9.3.1 Password use
A.9.4 Network access control *Protection of networked services* A.9.4.3 User authentication for external connections A.9.4.4 Node authentication
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.2 Terminal logon procedures A.9.5.3 User identification and authentication A.9.5.4 Password management system
A.9.7 Monitoring system access and use *To detect unauthorised activities* All controls in Clause A.9.7 apply.

BS 7799 Part 2 Control Objectives and Controls
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.7 Collection of evidence
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.1 System audit controls A.12.3.2 Protection of system audit tools

3.2 Business requirements

Most business requirements resulting from business processes, standards and objectives for information processing are specific to the organization and the ISMS considered. Nevertheless, there are some typical requirements that might be relevant in several cases, such as compliance with policies or standards, or outsourcing requirements in order to reduce costs. The following table contains an example list of business requirements and the BS 7799 Part 2 control objectives and controls that can be used to support them.

Requirement	Guide Reference
Outsourcing and use of third party contractors	3.2.1
Compliance with standards	3.2.2
Compliance with the security policy	3.2.3
Co-ordination of security activities	3.2.4
Availability of information processing facilities and information	3.2.5

This is not a definitive list of requirements. It should be used as a basis for an organization to identify its own list of business requirements based on its specific needs and business environment.

3.2.1 Outsourcing and use of third party contractors

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.6 Co-operation between organizations
A.4.2 Security of third party access *To maintain the security of organizational information processing facilities and information assets accessed by third parties* All controls in Clause A.4.2 apply.
A.4.3 Outsourcing *To maintain the security of information when the responsibility for information processing has been outsourced to another organization* A.4.3.1 Security requirements in outsourcing contracts
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.3 Confidentiality agreements
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures A.8.1.6 External facilities management
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchange agreements A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy
A.9.2 – A.9.6 Control objectives and controls from Clauses A.9.2 – A.9.6 should be applied as required to enforce A.9.1.1

BS 7799 Part 2 Control Objectives and Controls
A-10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* All controls in Clause A.10.3 apply.
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.5 Outsourced software development
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.2 Intellectual property rights (IPR) A.12.1.4 Data protection and privacy of personal information A.12.1.5 Prevention of misuse of information processing facilities A.12.1.6 Regulation of cryptographic controls A.12.1.7 Collection of evidence

3.2.2 Compliance with standards

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.3 Allocation of information security responsibilities
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.3 Securing offices, rooms and facilities

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection A.7.2.2 Power supplies A.7.2.3 Cabling security
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation

3.2.3 Compliance with the security policy

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.3 Allocation of information security responsibilities A.4.1.7 Independent review of information security
A.5 Asset classification and control All control objectives and controls in Clause A.5 apply.
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* All controls in Clause A.6.1 apply.
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* All controls in Clause A.6.3 apply.
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.1 Documented operating procedures A.8.1.3 Incident management procedures
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.2 Operator logs A.8.4.3 Fault logging
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy
A.9.2 – A.9.6 Control objectives and controls from Clauses A.9.2 – A.9.6 should be applied as required to enforce A.9.1.1
A.9.7 Monitoring system access and use *To detect unauthorised activities* All controls in Clause A.9.7 apply.
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* All controls in Clause A.12.1 apply.
A.12.2 Reviews of security policy and technical compliance *To ensure compliance of systems with organizational security policies and standards* A.12.2.1 Compliance with security policy

BS 7799 Part 2 Control Objectives and Controls
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.1 System audit controls

3.2.4 Co-ordination of security activities

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.4.1 Information security infrastructure *To manage information security within the organization* All controls in Clause A.4.1 apply.
A.5 Asset classification and control All control objectives and controls in Clause A.5 apply.
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.1 Documented operating procedures A.8.1.3 Incident management procedures A.8.1.4 Segregation of duties
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.3 Information handling procedures
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy
A.9.2 – A.9.6 Control objectives and controls from Clauses A.9.2 – A.9.6 should be applied as required to enforce A.9.1.1

BS 7799 Part 2 Control Objectives and Controls
A.10.1 Security requirements of systems *To ensure that security is built into information systems* A.10.1.1 Security requirements analysis and specification
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation

3.2.5 Correct business processing

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.4 Authorisation process for information processing facilities
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* All controls in Clause A.6.3 apply.
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.2 Operational change control A.8.1.5 Separation of development and operational facilities
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* All controls in Clause A.10.2 apply.
BS 7799 Part 2 Control Objectives and Controls

A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation
A.12.2 Reviews of security policy and technical compliance *To ensure compliance of systems with organizational security policies and standards* A.12.2.2 Technical compliance checking
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* All controls in Clause A.12.3 apply.

3.2.6 Availability of information processing facilities and information

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* All controls in Clause A.6.3 apply.
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection A.7.2.2 Power supplies A.7.2.3 Cabling security A.7.2.4 Equipment maintenance
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.1 Documented operating procedures A.8.1.3 Incident management procedures A.8.1.5 Separation of development and operational facilities
A.8.2 System planning and acceptance *To minimise the risk of systems failures* All controls in Clause A.8.2 apply.
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software

BS 7799 Part 2 Control Objectives and Controls
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.3 Information handling procedures A.8.6.4 Security of system documentation
A.10.4 Security of system files *To ensure that IT projects and support activities are conducted in a secure manner* All controls in Clause A.10.4 apply.
A.10.5 Security in development and support processes *To maintain the security of application system software and information* All controls in Clause A.10.5 apply.
A.12.2 Reviews of security policy and technical compliance *To ensure compliance of systems with organizational security policies and standards* A.12.2.2 Technical compliance checking
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.1 System audit controls

3.3 Requirements derived from risk identification

To fulfil the security requirements that are identified from risk identification, it is necessary to consider what causes the risks, i.e. the identified threats and vulnerabilities. Therefore, a list of typical threats and vulnerabilities derived from the text in the controls of ISO/IEC 17799 is considered which are matched against the control objectives and controls from BS 7799 Part 2 that can be applied to protect against them.

As described in Section 1.3, the results of the risk identification should be matched against this list of threats and vulnerabilities, and those that are applicable for the risk considered point to control objectives and controls that can be applied to reduce the risk.

Section 4 provides a relationship between security concerns and BS 7799 Part 2 controls. Apart from supporting the “Check” activity in the PDCA model, this information can also be used to check the selection of controls for completeness and consistency.

The following threats and vulnerabilities are addressed in this Guide. It should not be assumed that these threats and vulnerabilities form a definitive list of possible threats and vulnerabilities that might be applicable to a particular asset. There are most likely other threats and vulnerabilities not

in this list which are applicable to an organization or its business partner/trading environment and which need to be identified for each of the assets to allow appropriate protection. With help of the risk identification process, the organization should derive a list of all applicable threats and vulnerabilities for the assets considered.

Threats and Vulnerabilities	Guide Reference
Security breaches Security policy Lack of awareness Lack of security organization and co-ordination Unclear responsibilities Security weaknesses Insufficient security built into the system Third party arrangements Outsourcing arrangements Unprotected assets Incorrect classification, labelling or handling of information Deliberate action and lack of disciplinary action	3.3.1
Legislation Non-compliance Inability to provide evidence Fraud	3.3.2
Incidents and failures Damage from or re-occurrence of incidents Damage from software malfunctions System failure	3.3.3
Misuse Unauthorised use of information processing facilities Misuse of information processing facilities Misuse of system utilities or audit tools Unauthorised removal of property or media	3.3.4
Unauthorised changes Unauthorised installation of or changes to software Unauthorised changes to information processing facilities Mixing of test, development and operational facilities Unauthorised copying of proprietary information or software	3.3.5
Unauthorised access Information (in general) Confidential information Modification or destruction of information Access because of privileges Password selection and/or management Information processing facilities (in general) Computers Networks and network services Equipment System documentation Program source libraries	3.3.6
Malicious code	3.3.7
Inaccurate information Input of information Processing errors Output of information	3.3.8

Threats and Vulnerabilities	Guide Reference
Security of information and software exchanged between organizations Lack of exchange agreements Unauthorised access, misuse or corruption of media in transit Risks from electronic commerce, electronic office systems and publicly available systems (in general) Repudiation Mis- or re-routing of messages Mis-dialling (phone or fax) Unauthorised changes and corruption to messages Denial of service Loss of service	3.3.9
Lack or inappropriate use of cryptographic controls Lack of policy governing the use of cryptographic controls Unauthorised access to information, systems and networks due to lack of unique and appropriate identification and authentication Unauthorised disclosure of information Unauthorised modification of information Inappropriate level of cryptographic protection Interception and eavesdropping Lack or inappropriate management of cryptographic keys	3.3.10
Mobile computing and teleworking Risks from mobile computing Risks from teleworking	3.3.11
User errors	3.3.12
Physical security Unauthorised physical access Theft Lack of equipment security Lack of media security Fire Flood, water Environmental contamination Power supply or air conditioning failure, electric anomalies Damage to cables Physical interception and eavesdropping Interference Hardware failure	3.3.13
Business continuity Disaster Interruption of business activities Unavailability of information, services and information processing facilities Lack of business continuity plans and procedures, clearly defined responsibilities, testing and training	3.3.14

3.3.1 Security breaches

3.3.1.1 Security breaches related to the security policy

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation

BS 7799 Part 2 Control Objectives and Controls
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.1 Documented operating procedures
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy
A.12.2 Reviews of security policy and technical compliance *To ensure compliance of systems with organizational security policies and standards* A.12.2.1 Compliance with security policy

3.3.1.2 Security breaches due to a lack of awareness

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.5 Disciplinary process

3.3.1.3 Security breaches due to a lack of security organization and co-ordination

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.1 Management information security forum A.4.1.2 Information security co-ordination A.4.1.3 Allocation of information security responsibilities A.4.1.5 Specialist information security advice

3.3.1.4 Security breaches due to of unclear responsibilities

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.1 Management information security forum A.4.1.2 Information security co-ordination A.4.1.3 Allocation of information security responsibilities
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.1 Including security in job responsibilities A.6.1.4 Terms and conditions of employment

3.3.1.5 Security breach due to security weaknesses (e.g. incorrectly or not implemented controls)

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.7 Independent review of information security
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.2 Reporting security weaknesses
A.8.2 System planning and acceptance *To minimise the risk of systems failures* A.8.2.2 System acceptance

BS 7799 Part 2 Control Objectives and Controls
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.3 Fault logging
A.12.2 Reviews of security policy and technical compliance *To ensure compliance of systems with organizational security policies and standards* A.12.2.1 Compliance with security policy A.12.2.2 Technical compliance checking

3.3.1.6 Security breaches due to insufficient security built in the system (e.g. wrongly assessed requirements)

BS 7799 Part 2 Control Objectives and Controls
A.10.1 Security requirements of systems *To ensure that security is built into information systems* A.10.1.1 Security requirements analysis and specification

3.3.1.7 Security breaches related to third party arrangements

BS 7799 Part 2 Control Objectives and Controls
A.4.2 Security of third party access *To maintain the security of organizational information processing facilities and information assets accessed by third parties* A.4.2.1 Identification of risks from third party access A.4.2.2 Security requirements in third party contracts
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.4 Working in secure areas

3.3.1.8 Security breaches related to outsourcing arrangements

BS 7799 Part 2 Control Objectives and Controls
A.4.3 Outsourcing ***To maintain the security of information when the responsibility for information processing has been outsourced to another organization*** A.4.3.1 Security requirements in outsourcing contracts

BS 7799 Part 2 Control Objectives and Controls
A.10.5 Security in development and support processes ***To maintain the security of application system software and information*** A.10.5.5 Outsourced software development

3.3.1.9 Security breaches due to unprotected assets

BS 7799 Part 2 Control Objectives and Controls
A.5.1 Accountability for assets *To maintain appropriate protection of organizational assets* A.5.1.1 Inventory of assets

3.3.1.10 Security breaches due to incorrect classification, labelling or handling of information

BS 7799 Part 2 Control Objectives and Controls
A.5.2 Information classification *To ensure that information assets receive an appropriate level of protection* A.5.2.1 Classification guidelines A.5.2.2 Information labelling and handling

3.3.1.11 Security breaches due to deliberate action and lack of disciplinary action

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.5 Disciplinary process
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.5 Prevention of misuse of information processing facilities

3.3.2 Legislation (see also 3.1.1 for more details)

3.3.2.1 Non-compliance with legislation

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.5 Disciplinary process
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchange agreements A.8.7.6 Publicly available systems
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption A.10.3.3 Digital signatures A.10.3.5 Key management
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.5 Outsourced software development
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* All controls of Clause A.12.1 apply.

3.3.2.2 Inability to provide evidence (e.g. due to a lack of monitoring)

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.3 Allocation of information security responsibilities A.4.1.6 Co-operation between organizations
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.5 Disciplinary process
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up A.8.4.2 Operator logs A.8.4.3 Fault logging
A.9.2 User access management *To prevent unauthorised access to information systems* All controls in Clause A.9.2 apply.
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.3 User identification and authentication A.9.5.4 Password management system

BS 7799 Part 2 Control Objectives and Controls
A.9.7 Monitoring system access and use *To detect unauthorised activities* All controls in Clause A.9.7 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.1 Identification of applicable legislation A.12.1.7 Collection of evidence
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.1 System audit controls A.12.3.2 Protection of system audit tools

3.3.2.3 Fraud

BS 7799 Part 2 Control Objectives and Controls
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.2 Personnel screening and policy
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.4 Segregation of duties A.8.1.5 Separation of development and operational facilities
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security

3.3.3 Incidents and failures

3.3.3.1 Damage from or re-occurrence of incidents

BS 7799 Part 2 Control Objectives and Controls
A.3.1 Information security policy *To provide management direction and support for information security* A.3.1.1 Information security policy document A.3.1.2 Review and evaluation

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.5 Specialist information security advice A.4.1.6 Co-operation between organizations
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.1 Reporting security incidents A.6.3.4 Learning from incidents
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures

3.3.3.2 Damage from software malfunctions

BS 7799 Part 2 Control Objectives and Controls
A.6.3 Responding to security incidents and malfunctions *To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents* A.6.3.3 Reporting software malfunctions

3.3.3.3 System failure (e.g. because of insufficient resources, system overload or corruption)

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.4 Authorisation process for information processing facilities
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.5 Separation of development and operational facilities
A.8.2 System planning and acceptance *To minimise the risk of systems failures* A.8.2.1 Capacity planning A.8.2.2 System acceptance

BS 7799 Part 2 Control Objectives and Controls
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.9.7 Monitoring system access and use *To detect unauthorised activities* A.9.7.2 Monitoring system use
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* A.10.2.1 Input data validation
A.10.4 Security of system files *To ensure that IT projects and support activities are conducted in a secure manner* A.10.4.1 Control of operational software A.10.4.3 Access control to program source library
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.1 Change control procedures

3.3.4 Misuse

3.3.4.1 Unauthorised use of information processing facilities

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.4 Authorisation process for information processing facilities

3.3.4.2 Misuse of information processing facilities

BS 7799 Part 2 Control Objectives and Controls
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.4 Segregation of duties
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.2 Teleworking

BS 7799 Part 2 Control Objectives and Controls
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.5 Prevention of misuse of information processing facilities

3.3.4.3 Misuse of system utilities or audit tools

BS 7799 Part 2 Control Objectives and Controls
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.5 Use of system utilities
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.2 Protection of system audit tools

3.3.4.4 Unauthorised removal of property or media

BS 7799 Part 2 Control Objectives and Controls
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.2 Removal of property
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.1 Management of removable computer media

3.3.5 Unauthorised Changes

3.3.5.1 Unauthorised installation of or changes to software

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.4 Authorisation process for information processing facilities
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.1 Change control procedures A.10.5.3 Restrictions on changes to software packages

3.3.5.2 Unauthorised changes to information processing facilities

BS 7799 Part 2 Control Objectives and Controls
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.2 Operational change control A.8.1.5 Separation of development and operational facilities
A.10.4 Security of system files *To ensure that IT projects and support activities are conducted in a secure manner* A.10.4.1 Control of operational software
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.2 Technical review of operating system changes

3.3.5.3 Mixing of test, development and operational facilities

BS 7799 Part 2 Control Objectives and Controls
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.5 Separation of development and operational facilities
A.10.4 Security of system files *To ensure that IT projects and support activities are conducted in a secure manner* A.10.4.2 Protection of system test data
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.1 Change control procedures

3.3.5.4 Unauthorised copying of proprietary information or software

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.6 Secure disposal or re-use of equipment
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.2 Intellectual property rights

3.3.6 Unauthorised access

3.3.6.1 Unauthorised access[5] to information (more specific possibilities of unauthorised access are discussed below)

BS 7799 Part 2 Control Objectives and Controls
A.4.2 Security of third party access *To maintain the security of organizational information processing facilities and information assets accessed by third parties* A.4.2.1 Identification of risks from third party access A.4.2.2 Security requirements in third party contracts
A.4.3 Outsourcing *To maintain the security of information when the responsibility for information processing has been outsourced to another organization* A.4.3.1 Security requirements in outsourcing contracts
A.5.2 Information classification *To ensure that information assets receive an appropriate level of protection* A.5.2.1 Classification guidelines A.5.2.2 Information labelling and handling
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.4 Terms and conditions of employment
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.4 Working in secure areas A.7.1.5 Isolated delivery and loading areas
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.5 Security of equipment off-premises
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy

[5] *Unauthorised access in this context includes consecutive security problems such as disclosure of confidential information and modification and/or damage to and loss/destruction of information.*

BS 7799 Part 2 Control Objectives and Controls
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.6 External facilities management
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.1 Management of removable computer media A.8.6.3 Information handling procedures
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchange agreements A.8.7.2 Security of media in transit A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems
A.9 Access control All control objectives and controls of Clause A.9 apply.
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.3 Safeguarding of organizational records

3.3.6.2 Disclosure of confidential information

BS 7799 Part 2 Control Objectives and Controls
A.4.1 Information security infrastructure *To manage information security within the organization* A.4.1.6 Co-operation between organizations

BS 7799 Part 2 Control Objectives and Controls
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.2 Personnel screening and policy A.6.1.3 Confidentiality agreements
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.4 Equipment maintenance A.7.2.5 Security of equipment off-premises A.7.2.6 Secure disposal or re-use of equipment
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.2 Disposal of media
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchange agreements A.8.7.2 Security of media in transit A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.7 Other forms of information exchange
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption A.10.3.5 Key management
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.4 Covert channels and Trojan code
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.4 Data protection and privacy of personal information

3.3.6.3 Unauthorised modification or destruction of information

BS 7799 Part 2 Control Objectives and Controls
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* All controls in Clause A.10.2 apply.
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.3 Digital signatures A.10.3.5 Key management
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.4 Covert channels and Trojan code
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.4 Data protection and privacy of personal information

3.3.6.4 Unauthorised access because of privileges

BS 7799 Part 2 Control Objectives and Controls
A.9.2 User access management *To prevent unauthorised access to information systems* A.9.2.2 Privilege management

3.3.6.5 Unauthorised access because of password selection and/or management

BS 7799 Part 2 Control Objectives and Controls
A.9.2 User access management *To prevent unauthorised access to information systems* A.9.2.3 User password management
A.9.3 User responsibilities *To prevent unauthorised user access* A.9.3.1 Password use
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.3 User identification and authentication A.9.5.4 Password management system

3.3.6.6 Unauthorised access to information processing facilities (general, more specific see below)

BS 7799 Part 2 Control Objectives and Controls
A.9.1 Business requirement for access control *To control access to information* A.9.1.1 Access control policy

3.3.6.7 Unauthorised access to computers

BS 7799 Part 2 Control Objectives and Controls
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy
A.9.5 Operating system access control *To prevent unauthorised computer access* All controls of Clause A.9.5 apply.
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.1 Change control procedures

3.3.6.8 Unauthorised access to networks and network services

BS 7799 Part 2 Control Objectives and Controls
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.6 Publicly available systems
A.9.4 Network access control *Protection of networked services* All controls of Clause A.9.4 apply.
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.2 Terminal logon procedures

3.3.6.9 Unauthorised access to equipment

BS 7799 Part 2 Control Objectives and Controls
A.9.3 User responsibilities *To prevent unauthorised user access* A.9.3.2 Unattended user equipment

3.3.6.10 Unauthorised access to system documentation

BS 7799 Part 2 Control Objectives and Controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.4 Security of system documentation

3.3.6.11 Unauthorised access to program source libraries

BS 7799 Part 2 Control Objectives and Controls
A.10.4 Security of system files *To ensure that IT projects and support activities are conducted in a secure manner* A.10.4.3 Access control to program source library

3.3.7 Malicious code

BS 7799 Part 2 Control Objectives and Controls
8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* 8.1.5 Separation of development and operational facilities
A.8.3 Protection from malicious software *To protect the integrity of software and information* A.8.3.1 Controls against malicious software
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.4 Security of electronic mail
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing
A.10.5 Security in development and support processes *To maintain the security of application system software and information* A.10.5.4 Covert channels and Trojan code

3.3.8 Inaccurate information

3.3.8.1 Inaccurate input of information

BS 7799 Part 2 Control Objectives and Controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.3 Information handling procedures
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* A.10.2.1 Input data validation

3.3.8.2 Processing errors

BS 7799 Part 2 Control Objectives and Controls
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* A.10.2.2 Control of internal processing

3.3.8.3 Inaccurate output of information

BS 7799 Part 2 Control Objectives and Controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.3 Information handling procedures
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* A.10.2.4 Output data validation

3.3.9 Security of information and software exchanged between organizations

3.3.9.1 Lack of exchange agreements

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.1 Information and software exchanges

3.3.9.2 Unauthorised access, misuse or corruption of media in transit

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.2 Security of media in transit

3.3.9.3 Risks from electronic commerce, electronic office systems and publicly available systems (in general)

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems

3.3.9.4 Repudiation

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.4 Non-repudiation services

3.3.9.5 Miss- or re-routing of messages

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems

3.3.9.6 Miss-dialling (phone or fax)

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.7 Other forms of information exchange

3.3.9.7 Unauthorised changes and corruption to messages

BS 7799 Part 2 Control Objectives and Controls
A.10.2 Security in application systems *To prevent loss, modification or misuse of user data in application systems* A.10.2.3 Message authentication

3.3.9.8 Denial of service

BS 7799 Part 2 Control Objectives and Controls
A.8.5 Network management *To ensure the safeguarding of information in networks and the protection of the supporting infrastructure* A.8.5.1 Network controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security A.8.7.4 Security of electronic mail A.8.7.5 Security of electronic office systems A.8.7.6 Publicly available systems A.8.7.7 Other forms of information exchange

3.3.9.9 Loss of service

BS 7799 Part 2 Control Objectives and Controls
A.8.1 Operational procedures and responsibilities *To ensure the correct and secure operation of information processing facilities* A.8.1.3 Incident management procedures
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.

3.3.10 Use of cryptographic controls

3.3.10.1 Lack of policy governing the use of cryptographic controls

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls

BS 7799 Part 2 Control Objectives and Controls
A.12.1 Compliance with legal requirements *To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements* A.12.1.6 Regulation of cryptographic controls

3.3.10.2 Unauthorised access to information, systems and network services due to a lack of unique and appropriate identification and authentication

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.3 Electronic commerce security
A.9.2 User access management *To prevent unauthorised access to information systems* A.9.2.1 User registration
A.9.4 Network access control *Protection of networked services* A.9.4.3 User authentication for external connections A.9.4.4 Node authentication
A.9.5 Operating system access control *To prevent unauthorised computer access* A.9.5.3 User identification and authentication
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing

3.3.10.3 Unauthorised disclosure of information

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption

3.3.10.4 Unauthorised modification of information

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.3 Digital signatures

3.3.10.5 Inappropriate level of cryptographic protection (e.g. due to inappropriate algorithm, key length or mode of operation)

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.1 Policy on the use of cryptographic controls A.10.3.2 Encryption A.10.3.3 Digital signatures

3.3.10.6 Interception and eavesdropping

BS 7799 Part 2 Control Objectives and Controls
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* All controls in Clause A.8.7 apply.
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.2 Encryption

3.3.10.7 Lack or inappropriate of management of cryptographic keys

BS 7799 Part 2 Control Objectives and Controls
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* All controls in Clause A.10.3 apply.

3.3.11 Mobile computing and teleworking

3.3.11.1 Risks from mobile computing

BS 7799 Part 2 Control Objectives and Controls
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing

3.3.11.2 Risks from teleworking

BS 7799 Part 2 Control Objectives and Controls
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.2 Teleworking

3.3.12 User errors

BS 7799 Part 2 Control Objectives and Controls
A.6.2 User training *To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work* A.6.2.1 Information security education and training
A.8.2 System planning and acceptance *To minimise the risk of systems failures* A.8.2.2 System acceptance

3.3.13 Physical security

3.3.13.1 Unauthorised physical access6 (to business premises, information processing facilities, paper and media)

BS 7799 Part 2 Control Objectives and Controls
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.1 Physical security perimeter A.7.1.2 Physical entry controls A.7.1.3 Securing offices, rooms and facilities A.7.1.5 Isolated delivery and loading areas
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up

3.3.13.2 Theft (of information, equipment, information processing facilities)

BS 7799 Part 2 Control Objectives and Controls
A.6.1 Security in job definition and resourcing *To reduce the risks of human error, theft, fraud or misuse of facilities* A.6.1.2 Personnel screening and policy
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* All controls of Clause A.7.1 apply.
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection A.7.2.5 Security of equipment off-premises
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy

[6] *This is including damage to or loss and destruction of business premises, information processing facilities and paper and media*

BS 7799 Part 2 Control Objectives and Controls
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking

3.3.13.3 Lack of equipment security

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection A.7.2.4 Equipment maintenance A.7.2.5 Security of equipment off-premises A.7.2.6 Secure disposal or re-use of equipment
A.9.8 Mobile computing and teleworking *To ensure information security when using mobile computing and teleworking facilities* A.9.8.1 Mobile computing A.9.8.2 Teleworking

3.3.13.4 Lack of media security

BS 7799 Part 2 Control Objectives and Controls
A.8.6 Media handling and security *To prevent damage to assets and interruptions to business activities* A.8.6.1 Management of removable computer media A.8.6.2 Disposal of media
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.2 Security of media in transit

3.3.13.5 Fire

BS 7799 Part 2 Control Objectives and Controls
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.3 Securing offices, rooms and facilities
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection

BS 7799 Part 2 Control Objectives and Controls
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up

3.3.13.6 Flood, water

BS 7799 Part 2 Control Objectives and Controls
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.3 Securing offices, rooms and facilities
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up

3.3.13.7 Environmental contamination (smoke, dust, vibration, chemical effects etc.)

BS 7799 Part 2 Control Objectives and Controls
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.3 Securing offices, rooms and facilities
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.1 Equipment siting and protection

BS 7799 Part 2 Control Objectives and Controls
A.7.3 General controls *To prevent compromise or theft of information and information processing facilities* A.7.3.1 Clear desk and clear screen policy
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up

3.3.13.8 Power supply or air conditioning failure, electric anomalies

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.2 Power supplies

3.3.13.9 Damage to cables

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.3 Cabling security

3.3.13.10 Physical interception and eavesdropping

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.3 Cabling security A.7.2.5 Security of equipment off-premises
A.8.7 Exchanges of information and software *To prevent loss, modification or misuse of information exchanged between organizations* A.8.7.7 Other forms of information exchange
A.10.3 Cryptographic controls *To protect the confidentiality, authenticity or integrity of information* A.10.3.2 Encryption

3.3.13.11 Physical interference

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.3 Cabling security

3.3.13.12 Hardware failure

BS 7799 Part 2 Control Objectives and Controls
A.7.2 Equipment security *To prevent loss, damage or compromise of assets and interruption to business activities* A.7.2.4 Equipment maintenance
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up

3.3.14 Business continuity

3.3.14.1 Disaster (including fire, flood, earthquake, explosives etc.)

BS 7799 Part 2 Control Objectives and Controls
A.7.1 Secure areas *To prevent unauthorised access, damage and interference to business premises and information* A.7.1.3 Securing offices, rooms and facilities
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.

3.3.14.2 Interruption of business activities

BS 7799 Part 2 Control Objectives and Controls
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.

BS 7799 Part 2 Control Objectives and Controls
A.12.3 System audit considerations *To maximise the effectiveness, and to minimise interference to/from the system audit process* A.12.3.1 System audit controls

3.3.14.3 Unavailability of information, services and information processing facilities

BS 7799 Part 2 Control Objectives and Controls
A.8.4 Housekeeping *To maintain the integrity and availability of information processing and communication services* A.8.4.1 Information back-up
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.

3.3.14.4 Lack of business continuity plans and procedures, clearly defined responsibilities, testing and training

BS 7799 Part 2 Control Objectives and Controls
A.11.1 Aspects of business continuity management *To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters* All controls in Clause A.11.1 apply.

4 Security Concerns and BS 7799 Controls

The following tables describe typical security relevant concerns for each of the BS 7799 Part 2 controls that can be protected against and reduced by application of this BS 7799 control. In addition, the tables describe what might be endangered (confidentiality - C, integrity - I, availability - A and legal, regulatory and contractual requirements and obligations – L). The numbers in given parenthesis at the end of each topic heading in the tables below refers to the number of the associated control in Annex A of BS 7799 Part 2.

There are two ways these security concerns can be used:

- The first one is to check the control objectives and controls selected following the process explained din Section 3 for completeness and consistency. The security concerns identified with help of this section can also be used to identify further controls from Section 3.
- Another way of using the security concerns is to look at them in the "Check" activity of the PDCA model, where the implemented control objectives and controls are checked for success and efficiency. If any of the security concerns apply, the risk assessment results should be updated to reflect this, and risk treatment options considered for these newly identified risks. If risk reduction has been chosen, additional control objectives and/or controls should be selected, supported by Section 3.

As already mentioned before, the selection of control objectives and controls following Sections 3 and 4 is subject to further considerations of selection factors and constraints (see Section 5), and is finally selected for implementation when all security requirements are fulfilled.

4.1 Security Policy

4.1.1 Information Security Policy (Clause A.3.1)

Objective: To provide management direction and support for information security.

4.1.1.1 Information security policy document (A.3.1.1)

Security concerns	threatening
Security breaches (lack of compliance with laws, standards, security policy, virus handling, business continuity, etc.) because security policy is unknown to, ignored by or misunderstood by employees	C, I, A, L
Damage from or re-occurrence of incidents because of lack of a good reporting scheme	C, I, A, L
Security breaches (deliberate or accidental) because employees are not aware of the importance of security	C, I, A, L
Security breaches because of lack of management support (e.g. when allocating resources to security)	C, I, A, L

4.1.1.2 Review and evaluation (A.3.1.2)

Security concerns	threatening
Security breaches because security policy is not up to date (e.g. does not include recently purchased information processing facilities)	C, I, A, L
Security breaches because nobody feels responsible for maintaining the security policy	C, I, A, L
Ignorance of the fact that the security policy is not efficient	C, I, A, L

Too high costs because of a lack of security	
Higher costs than necessary for security	

4.2 Organizational Security

4.2.1 Information security infrastructure (Clause A.4.1)

Objective: To manage information security within the organization.

4.2.1.1 Management information security forum (A.4.1.1)

4.2.1.2 Information security co-ordination (A.4.1.2)

4.2.1.3 Allocation of information security responsibilities (A.4.1.3)

Security concerns	threatening
Security breaches because of unclear aims of security within the organization	C, I, A, L
Security breaches because of not up to date controls	C, I, A, L
Damages because of not correctly handled incidents	C, I, A, L
Security breaches because of lack of security co-ordination within the organization	C, I, A, L
Security breaches because of lack of consistency in security arrangements within the organization	C, I, A, L
Security breaches because of unclear or not correctly allocated responsibilities for security	C, I, A, L
Lack of asset protection because of wrongly handled ownership and delegation of responsibility	C, I, A, L
Inability to collect evidence because of unclear defined responsibilities	L

4.2.1.4 Authorization process for information processing facilities (A.4.1.4)

Security concerns	threatening
Purchasing of unsuitable equipment	
System failures because of hardware and/or software incompatibilities	I, A
Unauthorised use of personal information processing facilities for storing or processing business information	C, I, A, L
Unauthorised use of personal information processing facilities in the workplace	C, I, A, L
Unauthorised installation of new software (e.g. containing viruses or Trojan horses)	C, I, A, L
Corruption of business processes	C, I, A, L

4.2.1.5 Specialist information security advice (A.4.1.5)

Security concerns	threatening
Security breaches because of a lack of advice	C, I, A, L
Security breaches because of advice not being co-ordinated within the organization	C, I, A, L
Wrong or ineffective reaction to incidents because of a lack of security advice	C, I, A, L

4.2.1.6 Co-operation between organizations (A.4.1.6)

Security concerns	threatening
Wrong or ineffective reaction to incidents because of a lack of contact to the appropriate organizations	C, I, A, L

Inability to collect evidence	L
Disclosure of confidential information passed between organizations	C

4.2.1.7 Independent review of information security (A.4.1.7)

Security concerns	threatening
Lack of compliance with the security policy	C, I, A, L
Security breaches because of wrongly implemented or not implemented controls	C, I, A, L
Lack of detection of mistakes in the implementation	C, I, A, L

4.2.2 Security of third party access (Clause A.4.2)

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

4.2.2.1 Identification of risks from third party access (A.4.2.1)

Security concerns	threatening
Unauthorised physical access by third parties	C, I, A, L
Unauthorised logical access by third parties	C, I, A, L
Giving the third party more access (physical or logical) than necessary for the work	C, I, A, L
Disclosure of confidential information because of a lack of non-disclosure agreements	C
Security breaches because of wrongly identified security requirements of third party access	C, I, A, L

4.2.2.2 Security requirements in third party contracts (A.4.2.2)

Security concerns	threatening
Breaches of security or legislation by the third party because of no or insufficient contract in place	C, I, A, L
Security breaches by the third party because of misunderstanding of the organization's requirements	C, I, A, L

4.2.3 Outsourcing (Clause A.4.3)

Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

4.2.3.1 Security requirements in outsourcing contracts (A.4.3.1)

Security concerns	threatening
Breaches of security or legislation by the third party because of no or insufficient outsourcing contract in place	C, I, A, L
Security breaches by the third party because of misunderstanding of the organization's requirements	C, I, A, L
Security breaches because of unclear ownership of assets	C, I, A, L

4.3 Asset Classification and Control

4.3.1 Accountability for assets (Clause A.5.1)

Objective: To maintain appropriate protection of organizational assets.

4.3.1.1 Inventory of assets (A.5.1.1)

Security concerns	threatening
Security breaches because of unidentified assets	C, I, A, L
Security breaches because of protection not being appropriate to the value of the asset(s)	C, I, A, L
Breaches of IPR and safeguarding of organizational records	L
Security breaches because of not up to date inventory (e.g. new assets not included)	C, I, A, L
Security breaches because of unclear ownership of assets	C, I, A, L
Lack of compliance with the security policy and co-ordination of security activities	C, I, A, L

4.3.2 Information classification (Clause A.5.2)

Objective: To ensure that information assets receive an appropriate level of protection.

4.3.2.1 Classification guidelines (A.5.2.1)

Security concerns	threatening
Unauthorised access to information	C, I, A, L
Security breaches because of inappropriate or not up to date classification of information	C, I, A, L
Breaches of IPR, safeguarding of organizational records or data protection act	L
Lack of compliance with the security policy and co-ordination of security activities	C, I, A, L
Security breaches because of classification scheme being to complex or being unknown	C, I, A, L

4.3.2.2 Information labelling and handling (A.5.2.2)

Security concerns	threatening
Unauthorised access to information	C, I, A, L
Theft	C, A
Breaches of IPR, safeguarding of organizational records or data protection act	L
Lack of compliance with the security policy and co-ordination of security activities	C, I, A, L
Security breaches because information is not correctly labelled (e.g. outputs from sensitive systems)	C, I, A, L
Security breaches because information is not correctly handled according to its labelling	C, I, A, L
Security breaches because the labelling and/or handling does not correctly reflect the classification scheme (see 5.2.1)	C, I, A, L

4.4 Personnel Security

4.4.1 Security in job definition and resourcing (Clause A.6.1)

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

4.4.1.1 Including security in job responsibilities (A.6.1.1)

Security concerns	threatening
Lack of compliance with the security policy	C, I, A, L
Employees breaching security because of unclear or undefined responsibilities	C, I, A, L

4.4.1.2 Personnel screening and policy (A.6.1.2)

Security concerns	threatening
Fraud, theft or misuse of information processing facilities by an employee who has problems that have not been detected	C, I, A, L
Espionage by an employee or contractor who has problems and can be blackmailed	C
Fraud or theft by agency staff that is not covered by the contract with that agency	C, I, A, L
Any of the above happening because of changes in the personal situation of an employee or contractor	C, I, A, L

4.4.1.3 Confidentiality agreements (A.6.1.3)

Security concerns	threatening
Disclosure of confidential or personal information by an employee or third party staff	C, L
Disclosure of confidential or personal information because of not up to date confidentiality agreements	C, L

4.4.1.4 Terms and conditions of employment (A.6.1.4)

Security concerns	threatening
Breaches of security or legislation because of unclear or undefined responsibilities for security	C, I, A, L
Lack of compliance with security policy or safety standards	C, I, A, L
Unauthorised access to information	C, I, A, L
Disclosure or unauthorised modification of personal employees data	C, I, L

4.4.2 User training (Clause A.6.2)

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

4.4.2.1 Information security education and training (A.6.2.1)

Security concerns	threatening
Security breach because of unawareness of security policy, controls or legal responsibilities	C, I, A, L
Security breach because of unawareness of the consequences and the importance of security to the organization	C, I, A, L

User error and disturbance of business processes because of insufficient training	I, A

4.4.3 Responding to security incidents and malfunctions (Clause A.6.3)

Objective: To minimise the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

4.4.3.1 Reporting security incidents (A.6.3.1)

Security concerns	threatening
Breaches of security or legislation because of inappropriate reaction to incidents	C, I, A, L
Disturbance of business processes and unavailability of information and information processing facilities	I, A
Inability to collect evidence	L
No reporting of incidents because of a lack of a reporting scheme	C, I, A, L
No reporting of incidents because of unawareness of the reporting scheme	C, I, A, L
Recurrence of incidents that were not reported	C, I, A, L

4.4.3.2 Reporting security weaknesses (A.6.3.2)

Security concerns	threatening
Disturbance of business processes and unavailability of information and information processing facilities	I, A
No reporting of security weaknesses because of a lack of a reporting scheme	C, I, A, L
No reporting of security weaknesses because of unawareness of the reporting scheme	C, I, A, L
Security breaches because of security weaknesses that have not been reported	C, I, A, L

4.4.3.3 Reporting software malfunctions (A.6.3.3)

Security concerns	threatening
No reporting of software malfunctions because of a lack of a reporting scheme	C, I, A, L
No reporting of software malfunctions because of unawareness of the reporting scheme	C, I, A, L
Security breaches because of software malfunctions that have not been reported	C, I, A, L
Disturbance of business processes and unavailability of information and information processing facilities	I, A
Security breaches because of incorrect handling of software malfunctions (e.g. by the user)	C, I, A, L

4.4.3.4 Learning from incidents (A.6.3.4)

Security concerns	threatening
Recurrence of incidents	C, I, A, L
Incorrect or inefficient procedures to handle incidents	C, I, A, L
Disturbance of business processes and unavailability of information and information processing facilities	I, A
Security breaches because of not reducing occurrence, frequency or damage of incidents	C, I, A, L

4.4.3.5 Disciplinary process (A.6.3.5)

Security concerns	threatening
Deliberate breaches of security or legislation because of a lack of a disciplinary process	C, I, A, L
Accidental breaches of security or legislation because of a 'couldn't care less' attitude	C, I, A, L
Security breaches by disgruntled employees who have been treated incorrectly under the suspect of security breaches	C, I, A, L

4.5 Physical and Environmental Security

4.5.1 Secure areas (Clause A.7.1)

Objective: To prevent unauthorised access, damage and interference to business premises and information.

4.5.1.1 Physical security perimeter (A.7.1.1)

Security concerns	threatening
Unauthorised physical access because of a lack of or an inappropriately protecting perimeter (e.g. resulting in theft or destruction)	C, I, A, L
Environmental contamination (fire, flood, disaster)	I, A

4.5.1.2 Physical entry controls (A.7.1.2)

Security concerns	threatening
Unauthorised physical access because of a lack of entry controls (e.g. resulting in theft or destruction)	C, I, A, L
Access because of not up to date access rights	C, I, A, L

4.5.1.3 Securing offices, rooms and facilities (A.7.1.3)

Security concerns	threatening
Unauthorised physical access to offices, rooms and facilities (e.g. resulting in theft or destruction)	C, I, A, L
Non-compliance with safety standards	L
Environmental contamination (fire, flood, disaster)	I, A

4.5.1.4 Working in secure areas (A.7.1.4)

Security concerns	threatening
Unauthorised access to information and information processing facilities	C, I, A, L
Unauthorised physical access by third parties (e.g. resulting in theft or destruction)	C, I, A, L

4.5.1.5 Isolated delivery and loading areas (A.7.1.5)

Security concerns	threatening
Unauthorised physical access (e.g. resulting in theft or destruction)	C, I, A, L
Unauthorised access to information and information processing facilities via an unprotected delivery and loading area	C, I, A, L

4.5.2 Equipment security (Clause A.7.2)

Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

4.5.2.1 Equipment siting and protection (A.7.2.1)

Security concerns	threatening
Unauthorised physical access to equipment because of a lack of or an inappropriately protecting perimeter	C, I, A, L
Theft	C, A, L
Unavailability of information and/or information processing facilities	A
Lack of equipment security	C, I, A, L
Environmental contamination (fire, water, explosives, smoke, dust, vibration, chemical effects, electrical supply interference, electromagnetic radiation) to equipment	I, A
Lack of compliance with safety standards	L
Overlooking because of wrong siting of equipment	C

4.5.2.2 Power supplies (A.7.2.2)

Security concerns	threatening
Power supply failure	I, A
Air conditioning failure	I, A
Unavailability of information and/or information processing facilities	A
Electrical anomalies	I, A
Lightning	I, A
Lack of compliance with safety standards	L

4.5.2.3 Cabling security (A.7.2.3)

Security concerns	threatening
Damage to cables	I, A
Unavailability of information and/or information processing facilities	A
Lack of compliance with safety standards	L
Interception	C
Interference	I, A

4.5.2.4 Equipment maintenance (A.7.2.4)

Security concerns	threatening
Lack of equipment security	C, I, A, L
Unavailability of information and/or information processing facilities	A
Hardware failure	I, A
Disclosure of confidential information during the maintenance process	C

4.5.2.5 Security of equipment off-premises (A.7.2.5)

Security concerns	threatening
Theft	C, I A
Damage to equipment (wilful damage, lack of maintenance, electromagnetic radiation, etc.)	I, A
Unauthorised removal of equipment	C, I, A, L
Unauthorised access to information stored and/or processed on the equipment	C, I, A, L
Inadequate insurance for the equipment	
Eavesdropping	C

4.5.2.6 Secure disposal or re-use of equipment (A.7.2.6)

Security concerns	threatening
Lack of equipment security	C, I, A, L
Disclosure of confidential information	C
Unauthorised copying of proprietary information or software	L

4.5.3 General controls (Clause A.7.3)

Objective: To prevent compromise or theft of information and information processing facilities.

4.5.3.1 Clear desk and clear screen policy (A.7.3.1)

Security concerns	threatening
Unauthorised access to information and information processing facilities	C, I, A, L
Theft	C, A, L
Destruction of information because of a environmental contamination or disaster	A

4.5.3.2 Removal of property (A.7.3.2)

Security concerns	threatening
Unauthorised access to information	C, I, A, L
Unauthorised removal of property	C, I, A, L

4.6 Communications and Operations Management

4.6.1 Operational procedures and responsibilities (Clause A.8.1)

Objective: To ensure the correct and secure operation of information processing facilities.

4.6.1.1 Documented operating procedures (A.8.1.1)

Security concerns	threatening
Non-compliance with security policy	C, I, A, L
Misuse of information processing facilities	C, I, A, L
Lack of co-ordinated security activities	C, I, A, L
Unavailability of information or information processing facilities	A
Security breaches because of undefined operating procedures (e.g. handling of outputs and mail, maintenance, etc.)	C, I, A, L

4.6.1.2 Operational change control (A.8.1.2)

Security concerns	threatening
System failure and disruption to business processes because of unauthorised changes or wrong estimation of impact	C, I, A, L
Security breach because of unauthorised changes that compromise the controls in place	C, I, A, L
Security breach because of unawareness of changes	C, I, A, L

4.6.1.3 Incident management procedures (A.8.1.3)

Security concerns	threatening
Breaches of security or legislation because of inappropriate reaction to incidents (by employees or third party contractors)	C, I, A, L
No reporting of incidents because of a unclear responsibilities or lack of procedures	C, I, A, L
Unavailability of information or information processing facilities, loss of services	A
Recurrence of incidents that were not reported	C, I, A, L
Lack of evidence when tracing an incident	C, I, A, L
Ineffective recovery from incidents because of incomplete or inaccurate reporting	C, I, A, L

4.6.1.4 Segregation of duties (A.8.1.4)

Security concerns	threatening
Fraud	I, L
Forgery	I, L
System misuse	C, I, A, L
Unauthorised access to information (e.g. personal information)	C, I, A, L
Lack of co-ordinated security activities	C, I, A, L

4.6.1.5 Separation of development and operational facilities (A.8.1.5)

Security concerns	threatening
Unauthorised modification of files or system environment	I, A

System failure	C, I, A, L
Introduction of unauthorised and untested code or malicious code	C, I, A, L
Unauthorised alteration of operational data, e.g. to commit fraud	I, L
Disruption to business processes	I, A
Unavailability of information or information processing facilities	A

4.6.1.6 External facilities management (A.8.1.6)

Security concerns	threatening
Disclosure of confidential information at the contractor's site	C
Damage to or loss of information at the contractor's site	I, A
Breach of IPR and software copyright legislation	L
Insufficient identification of risks and lack of appropriate controls in the contract	C, I, A

4.6.2 System planning and acceptance (Clause A.8.2)

Objective: To minimise the risk of systems failures.

4.6.2.1 Capacity planning (A.8.2.1)

Security concerns	threatening
Availability of information and information processing facilities	A
System failure	I, A
Insufficient system resources	I, A

4.6.2.2 System acceptance (A.8.2.2)

Security concerns	threatening
Availability of information and information processing facilities	A
System failure	I, A
Insufficient system resources	I, A
Insufficient security controls in place	C, I, A, L
User error because of a lack of training	C, I, A, L

4.6.3 Protection from malicious software (Clause A.8.3)

Objective: To protect the integrity of software and information.

4.6.3.1 Controls against malicious software (A.8.3.1)

Security concerns	threatening
Unauthorised access to information and information processing facilities (disclosure, modification and/or destruction and breaches of legislation)	C, I, A, L
Inability to provide evidence	L
Disruption of business processes	I, A
Viruses	I, A
Logic bombs	C, I, A
Worms	I, A
Trojan horses	C, I, A
Hoaxes	A

4.6.4 Housekeeping (Clause A.8.4)

Objective: To maintain the integrity and availability of information processing and communication services.

4.6.4.1 Information back-up (A.8.4.1)

Security concerns	threatening
Loss of or damage to information (by third parties, viruses, theft, disaster, environmental contamination, fire, flood, etc.)	I, A
Unauthorised modification of information	I, A, L
Inability to provide evidence	L
System failure	I, A
Hardware failure	I, A
Inability to restore back-up information	I, A
Insufficient protection of back-up information	I, A

4.6.4.2 Operator logs (A.8.4.2)

Security concerns	threatening
Non-compliance with security policy	C, I, A, L
Inability to provide evidence	L
Lack of monitoring	C, I, A, L

4.6.4.3 Fault Logging (A.8.4.3)

Security concerns	threatening
Inability to provide evidence	L
Non-compliance with security policy	C, I, A, L
Compromise of controls	C, I, A, L
Insufficient corrective action after a fault has taken place	C, I, A, L

4.6.5 Network management (Clause A.8.5)

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

4.6.5.1 Network controls (A.8.5.1)

Security concerns	threatening
Unauthorised access to connected services	C, I, A
Unauthorised access to information (e.g. organizational records, personal information, confidential information) and information processing facilities	C, I, A, L
Disclosure, modification or loss of information stored or processed in networks	C, I, A
Loss of availability of the network services and computers connected	A
Denial of service	I, A

4.6.6 Media handling (Clause A.8.6)

Objective: To prevent damage to assets and interruptions to business activities.

4.6.6.1 Management of removable computer media (A.8.6.1)

Security concerns	threatening
Unauthorised removal of computer media	C, I, A, L
Disclosure, modification or loss of information (including organizational records and personal information)	C, I, A, L
Damage to removable computer media	A

4.6.6.2 Disposal of media (A.8.6.2)

Security concerns	threatening
Disclosure of confidential information (including personal information)	C
Security breaches by a contractor handling disposal of media, equipment, etc.	C, I, A, L
Lack of evidence	L

4.6.6.3 Information handling procedures (A.8.6.3)

Security concerns	threatening
Disclosure, modification or loss of information (including organizational records and personal information)	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L
Inaccurate input of information	I, A
Inaccurate output of information	I, A

4.6.6.4 Security of system documentation (A.8.6.4)

Security concerns	threatening
Unavailability of information and information processing facilities	A
Unauthorised access to system documentation	C, I, A

4.6.7 Exchanges of information and software (Clause A.8.7)

Objective: To prevent loss, modification or misuse of information exchanged between organizations.

4.6.7.1 Information and software exchange agreements (A.8.7.1)

Security concerns	threatening
Lack of exchange agreements	C, I, A, L
Unauthorised access to information exchanged between organizations	C, I, A
Misuse of information exchanged between organizations	I, L
Security breaches by the third party contractor	C, I, A, L
Breach of legislation	L

4.6.7.2 Security of media in transit (A.8.7.2)

Security concerns	threatening
Unauthorised access to information on media in transit	C, I, A
Misuse of information on media in transit	I, L
Interception and eavesdropping	C, I

Breach of legislation	L
Corruption of media in transit	I, A

4.6.7.3 Electronic commerce security (A.8.7.3)

Security concerns	threatening
Unauthorised access to electronic commerce information.	C, I, A
Fraud	I, L
Contract dispute, repudiation	I, L
Breach of legislation	L
Interception and eavesdropping	C, I
Miss-routing and re-routing of messages	C, I, A
Denial of service	A
Lack of authentication between trading partners	C, I, A, L

4.6.7.4 Security of electronic mail (A.8.7.4)

Security concerns	threatening
Unauthorised access to information	C, I, A
Denial of service	A
Malicious software in downloads or mails	C, I, A
Breach of legislation	L
Miss-routing and re-routing of messages	C, I, A
Repudiation	I, L
Interception and eavesdropping'	C, I
Compromise of the organization (e.g. by sending defamatory mail)	

4.6.7.5 Security of electronic office systems (A.8.7.5)

Security concerns	threatening
Disclosure of confidential information	C
Breach of legislation	L
Unauthorised recording of phone calls	C
Unauthorised access to or distribution of mail	C, I, A
Interception and eavesdropping	C, I
Miss-routing and re-routing of messages	C, I, A
Denial of service	A
Repudiation	I, L

4.6.7.6 Publicly available systems (A.8.7.6)

Security concerns	threatening
Unauthorised modification or destruction of publicly available information	I, A
Non-compliance with legislation	L
Interception and eavesdropping	C, I
Repudiation	I, L
Denial of service	A
Unauthorised access to the connected network	C, I, A, L

4.6.7.7 Other forms of information exchange (A.8.7.7)

Security concerns	threatening
Disclosure of confidential information	C
Interception	C
Eavesdropping	C
Breach of legislation	L

Denial of service	A
Miss-dialling (phone or fax)	C, A

4.7 Access Control

4.7.1 Business requirements for access control (Clause A.9.1)

Objective: To control access to information.

4.7.1.1 Access control policy (A.9.1.1)

Security concerns	threatening
Unauthorised access to information or information processing facilities (by employees or third party staff)	C, I, A, L
Inadequate access control policy (too restrictive or not restrictive enough)	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L
Non-compliance with security policy	C, I, A, L
Non-compliance with legislation	L

4.7.2 User access management (Clause A.9.2)

Objective: To prevent unauthorised access to information systems.

4.7.2.1 User registration (A.9.2.1)

Security concerns	threatening
Unauthorised user access to information	C, I, A, L
No unique user identification and authentication	C, I, A, L
Inability to collect evidence	L
Out of date or no adequate access rights	C, I, A, L
No compliance with security policy	C, I, A, L

4.7.2.2 Privilege management (A.9.2.2)

Security concerns	threatening
Unauthorised access because of misuse of privileges	C, I, A, L
Wrong allocation of privileges	C, I, A, L
No withdrawal of unnecessary privileges	C, I, A, L
No separation between user and privileged role	C, I, A, L

4.7.2.3 User password management (A.9.2.3)

Security concerns	threatening
Unauthorised access because of lack of password management	C, I, A, L
Insecure password handling	C, I, A, L
Inability to collect evidence	L
No management process for the allocation of passwords	C, I, A, L
Insecure storage of passwords	C, I, A, L

4.7.2.4 Review of user access rights (A.9.2.4)

Security concerns	threatening
No formal review process for access rights	C, I, A, L
No formal review process for privileges	C, I, A, L
No process to check the validity of privileges allocated	C, I, A, L

4.7.3 User responsibilities (Clause A.9.3)

Objective: To prevent unauthorised user access.

4.7.3.1 Password use (A.9.3.1)

Security concerns	threatening
Unauthorised user access	C, I, A, L
Guessing or cracking of passwords	C, I, A, L
Selection of bad passwords	C, I, A, L
Insecure handling of passwords	C, I, A, L
Inability to collect evidence	L

4.7.3.2 Unattended user equipment (A.9.3.2)

Security concerns	threatening
Unauthorised access to unattended equipment	C, I, A, L
Lack of protection of unattended equipment	C, I, A, L

4.7.4 Network access control (Clause A.9.4)

Objective: Protection of networked services.

4.7.4.1 Policy on use of network services (A.9.4.1)

Security concerns	threatening
Unauthorised access to networks	C, I, A, L
Inadequate access control policy (too restrictive or not restrictive enough)	C, I, A, L
Lack of authorisation procedures	C, I, A, L

4.7.4.2 Enforced path (A.9.4.2)

Security concerns	threatening
Unauthorised access to information, business applications and networks	C, I, A, L
Unauthorised use of information processing facilities	C, I, A, L
Wrong configuration of gateways or firewalls	C, I, A, L

4.7.4.3 User authentication for external connections (A.9.4.3)

Security concerns	threatening
Unauthorised access to information and networks	C, I, A, L
Lack of or too weak user authentication	C, I, A, L
Inability to collect evidence	L

4.7.4.4 Node authentication (A.9.4.4)

Security concerns	threatening
Unauthorised access to information and networks	C, I, A, L

Lack of or too weak node authentication	C, I, A, L
Inability to collect evidence	L

4.7.4.5 Remote diagnostic port protection (A.9.4.5)

Security concerns	threatening
Unauthorised access to information and information processing facilities in networks	C, I, A, L
Lack of protection for diagnostic ports	

4.7.4.6 Segregation in networks (A.9.4.6)

Security concerns	threatening
Unauthorised access to information and information processing facilities in networks	C, I, A, L
No segregation between sensitive and less sensitive parts of the network	C, I, A, L
Wrong configuration of gateways or firewalls	C, I, A, L
Non-compliance with access control policy	C, I, A, L

4.7.4.7 Network connection control (A.9.4.7)

Security concerns	threatening
Unauthorised connections	C, I, A, L
No or wrong filter rules	C, I, A, L

4.7.4.8 Network routing control (A.9.4.8)

Security concerns	threatening
Non-compliance with access control policy	C, I, A, L
Unauthorised access to information and information processing facilities in networks	C, I, A, L
Unauthorised connections	C, I, A, L
Unauthorised information exchange	C, I, A, L

4.7.4.9 Security of network services (A.9.4.9)

Security concerns	threatening
Unauthorised access to networks and services	C, I, A, L
No clear description of the security attributes of services used	C, I, A, L

4.7.5 Operating system access control (Clause A.9.5)

Objective: To prevent unauthorised computer access.

4.7.5.1 Automatic terminal identification (A.9.5.1)

Security concerns	threatening
Unauthorised access to computers	C, I, A, L
Lack of or too weak automatic terminal identification and authentication	C, I, A, L

4.7.5.2 Terminal logon procedures (A.9.5.2)

Security concerns	threatening
Unauthorised access to computers, networks and services	C, I, A, L
Inability to collect evidence	L
Insecure logon procedures	C, I, A, L

4.7.5.3 User identification and authentication (A.9.5.3)

Security concerns	threatening
No unique user identification	C, I, A, L
No or too weak user authentication	C, I, A, L
Unauthorised access to information, applications, services and information processing facilities	C, I, A, L
Lack of evidence in case of an incident	L

4.7.5.4 Password management system (A.9.5.4)

Security concerns	threatening
Unauthorised user access to information, applications, services and information processing facilities	C, I, A, L
Insecure password handling and management	C, I, A, L
Inability to collect evidence	L
Selection of bad passwords	C, I, A, L
Insecure storage of passwords	C, I, A, L

4.7.5.5 Use of system utilities (A.9.5.5)

Security concerns	threatening
Misuse of system utilities, e.g. to override system and application controls	C, I, A, L
Lack of segregation of applications from system utilities	C, I, A, L
Unauthorised access	C, I, A, L
Lack of authentication prior to the use of system utilities	C, I, A, L
Lack of authorisation prior to the use of system utilities	C, I, A, L

4.7.5.6 Duress alarm to safeguard users (A.9.5.6)

Security concerns	threatening
Unauthorised access	C, I, A, L
Coercion of users	C, I, A, L
Lack of procedures to respond to a duress alarm	C, I, A, L

4.7.5.7 Terminal time-out (A.9.5.7)

Security concerns	threatening
Unauthorised access	C, I, A, L
Inappropriate time delay before time out	C, I, A, L

4.7.5.8 Limitation of connection time (A.9.5.8)

Security concerns	threatening
Unauthorised access	C, I, A, L

4.7.6 Application access control (Clause A.9.6)

Objective: To prevent unauthorised access to information held in information systems.

4.7.6.1 Information access restriction (A.9.6.1)

Security concerns	threatening
Unauthorised access to information and applications	C, I, A, L
Non-compliance with access control policy	C, I, A, L

4.7.6.2 Sensitive system isolation (A.9.6.2)

Security concerns	threatening
Unauthorised access to sensitive systems, information and applications	C, I, A, L

4.7.7 Monitoring system access and use (Clause A.9.7)

Objective: To detect unauthorised activities.

4.7.7.1 Event logging (A.9.7.1)

Security concerns	threatening
Lack of evidence in case of an event	L
Non-compliance with access control policy	C, I, A, L
No checks of event logs	C, I, A, L

4.7.7.2 Monitoring system use (A.9.7.2)

Security concerns	threatening
Non-compliance with access control policy	C, I, A, L
Unauthorised access	C, I, A, L
Lack of evidence	L
System failures	I, A
Lack or insufficient frequency of reviews	C, I, A, L
Unauthorised modification of log files	C, I, A, L

4.7.7.3 Clock synchronization (A.9.7.3)

Security concerns	threatening
Lack of evidence	L
Non-compliance with access control policy	C, I, A, L

4.7.8 Mobile computing and teleworking (Clause A.9.8)

Objective: To ensure information security when using mobile computing and teleworking facilities.

4.7.8.1 Mobile computing (A.9.8.1)

Security concerns	threatening
Unauthorised access to information and equipment	C, I, A, L
Breaches of legislation (e.g. software copyright, personal data, misuse of facilities, cryptographic controls)	L
Theft	C, I, A, L
Destruction	A
Loss if information	A
Malicious software	C, I, A, L
Lack of identification and authentication	C, I, A, L
Unintended disclosure of information (e.g. by overlooking)	C

4.7.8.2 Teleworking (A.9.8.2)

Security concerns	threatening
Theft of equipment and information	C, I, A, L
Unauthorised access to information at the teleworking site	C, I, A, L

Unauthorised remote access to the organization's information processing facilities	C, I, A, L
Breaches of legislation (e.g. software copyright, personal data, cryptographic controls)	L
Misuse of information processing facilities	C, I, A, L
Unauthorised teleworking	C, I, A, L
Unsuitable teleworking equipment or protection	C, I, A, L

4.8 System Development and Maintenance

4.8.1 Security requirements of systems (Clause A.10.1)

Objective: To ensure that security is built into information systems.

4.8.1.1 Security requirements analysis and specification (A.10.1.1)

Security concerns	threatening
Security breaches because of insufficient security built into the system	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L
Wrong assessment of security requirements	C, I, A, L

4.8.2 Security in application systems (Clause A.10.2)

Objective: To prevent loss, modification or misuse of user data in application systems.

4.8.2.1 Input data validation (A.10.2.1)

Security concerns	threatening
Incorrect input data	I, A
Incorrect business processes	I, A
Unauthorised changes to input data	I, A
System failures	I, A

4.8.2.2 Control of internal processing (A.10.2.2)

Security concerns	threatening
Processing errors	I, A
Unauthorised changes and corruption to messages	I, A
No or wrong procedures to recover from failures	I, A

4.8.2.3 Message authentication (A.10.2.3)

Security concerns	threatening
Unauthorised changes to messages	I, L
Corruption of messages	I, A

4.8.2.4 Output data validation (A.10.2.4)

Security concerns	threatening
Incorrect output data	C, I, A
Incorrect business processes	I, A

4.8.3 Cryptographic controls (Clause A.10.3)

Objective: To protect the confidentiality, authenticity or integrity of information.

4.8.3.1 Policy on the use of cryptographic controls (A.10.3.1)

Security concerns	threatening
Loss of confidentiality of information	C
Loss of integrity of information	I, L
Loss of authenticity	I, L
Non-compliance with legislation	L
Non-compliance with the security policy	C, I, A, L
Lack of unique identification and authentication (cryptography based)	C, I, A, L
Inappropriate or inaccurate use of cryptographic techniques	C, I, A, L
Wrong level of protection	C, I, A, L
Lack of or inappropriate key management	C, I, A, L

4.8.3.2 Encryption (A.10.3.2)

Security concerns	threatening
Loss of confidentiality of information or the secret key	C
Interception and eavesdropping	C
Wrong level of protection	C
Wrong selection of algorithm	C
Lack of or inappropriate key management	C, I, A, L
Non-compliance with legislation	L

4.8.3.3 Digital signatures (A.10.3.3)

Security concerns	threatening
Loss of integrity of information or the public key	I, L
Loss of authenticity	I, L
Loss of confidentiality of the private key	C
Lack of unique identification and authentication (cryptography based)	C, I, A, L
Wrong level of protection	I, L
Wrong selection of algorithm	I, L
Lack of or inappropriate key management	C, I, A, L
Non-compliance with legislation	L

4.8.3.4 Non-repudiation services (A.10.3.4)

Security concerns	threatening
Repudiation of actions or events	I, A, L
Lack of or inappropriate key management	C, I, A, L
Inability of resolving disputes	I, A, L

4.8.3.5 Key management (A.10.3.5)

Security concerns	threatening
Disclosure of keys	C, I, L
Loss of keys	A, L
Modification of keys	C, I, A, L
Lack of or inappropriate key management	C, I, A, L
Lack of recovery possibilities	A, L
Too long key lifetime	C, I, L

Non- compliance with legislation	L

4.8.4 Security of system files (Clause A.10.4)

Objective: To ensure that IT projects and support activities are conducted in a secure manner.

4.8.4.1 Control of operational software (A.10.4.1)

Security concerns	threatening
Corruption of operational systems	C, I, A, L
Unavailability of information and information processing facilities	A
System failure	I, A
Updates and changes to the operational system without authorisation	C, I, A, L
No back-ups of previous versions	C, I, A, L

4.8.4.2 Protection of system test data (A.10.4.2)

Security concerns	threatening
Use of operational data for tests	I, A, L
No segregation of development, test and operational environment	C, I, A, L
Unauthorised access to test data	I, A

4.8.4.3 Access control to program source library (A.10.4.3)

Security concerns	threatening
Corruption of computer programs	C, I, A, L
System failure	I, A
Unavailability of information and information processing facilities	A
Unauthorised access to program source libraries	C, I, A, L

4.8.5 Security in development and support processes (Clause A.10.5)

Objective: To maintain the security of application system software and information.

4.8.5.1 Change control procedures (A.10.5.1)

Security concerns	threatening
Corruption of information processing facilities	C, I, A, L
System failure	I, A
Unauthorised access to information processing facilities	C, I, A, L
Unauthorised changes to software	C, I, A, L
Unavailability of information and information processing facilities	A
No segregation of development, test and operational environment	C, I, A, L

4.8.5.2 Technical review of operating system changes (A.10.5.2)

Security concerns	threatening
Security breaches because of changes to the operating system	C, I, A, L
Unauthorised changes to software	C, I, A, L
Unavailability of information and information processing facilities	A
Lack of security review of changes	C, I, A, L

4.8.5.3 Restrictions on changes to software packages (A.10.5.3)

Security concerns	threatening
Unauthorised modification of software packages	C, I, A, L
Unavailability of information and information processing facilities	A
Compromise of in-built security controls	C, I, A, L
No back-up copies of the original software	I, A

4.8.5.4 Covert channels and Trojan code (A.10.5.4)

Security concerns	threatening
Disclosure of information	C
Unauthorised modification to information or software	I, A, L
Unavailability of information and information processing facilities	A
Malicious code	C, I, A, L

4.8.5.5 Outsourced software development (A.10.5.5)

Security concerns	threatening
Security breaches by the contractor	C, I, A, L
No or insufficient possibilities to test the software for functionality and security	C, I, A, L
Loss of licensing, code ownership or IPR	L

4.9 Business Continuity Management

4.9.1 Aspects of business continuity planning (Clause A.11)

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

4.9.1.1 Business continuity management process (A.11.1.1)

Security concerns	threatening
Interruptions to business activities	C, I, A, L
Disasters	C, I, A, L
Security failures	C, I, A, L
Unavailability of information and services (including organizational records)	A
Lack of co-ordination of security activities	C, I, A, L
Non-compliance with health and safety standards	L

4.9.1.2 Business continuity and impact analysis (A.11.1.2)

Security concerns	threatening
Wrong assessment of risks and impacts	C, I, A, L
Non-compliance with health and safety standards	L
Lack of plans and strategies	C, I, A, L

4.9.1.3 Writing and implementing continuity plans (A.11.1.3)

Security concerns	threatening
Lack of emergency procedures	C, I, A, L
No clearly identified responsibilities	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L

Non-compliance with health and safety standards	L
No implementation of the continuity planes	C, I, A, L
No education and testing (see also 11.1.5)	C, I, A, L

4.9.1.4 Business continuity planning framework (A.11.1.4)

Security concerns	threatening
Inconsistency of continuity plans	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L
Non-compliance with health and safety standards	L
Lack of knowledge of when to activate the plan and what the procedures are like	C, I, A, L
No clearly identified responsibilities	C, I, A, L
No education and testing (see also 11.1.5)	C, I, A, L

4.9.1.5 Testing, maintaining and re-assessing business continuity plans (A.11.1.5)

Security concerns	threatening
No education and testing of the continuity plans	C, I, A, L
Ineffective plans	C, I, A, L
Lack of co-ordination of security activities	C, I, A, L
Non-compliance with health and safety standards	L
Unawareness of plans	C, I, A, L
Lack of maintenance of the plans	C, I, A, L
Lack of reviewing and updating the plans	C, I, A, L
Lack of change control	C, I, A, L

4.10 Compliance

4.10.1 Compliance with legal requirements (Clause A.12.1)

Objective: To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations, and of any security requirements.

4.10.1.1 Identification of applicable legislation (A.12.1.1)

Security concerns	threatening
Non-compliance with applicable legislation, rules and regulations (of employees or third party contractors)	L
Non-compliance with security policy	C, I, A, L

4.10.1.2 Intellectual property rights (IPR) (A.12.1.2)

Security concerns	threatening
Breaches of intellectual property rights (of employees or third party contractors)	L
Lack of rules and regulations for copying	L
Breaches of software copyright (of employees or third party contractors)	L
Lack of rules and regulations for software copying	L

4.10.1.3 Safeguarding of organizational records (A.12.1.3)

Security concerns	threatening
Loss of important organizational records	L

Destruction of important organizational records	L
Falsification of important organizational records	L
Inability to provide evidence	L
Lack of guidelines how to identify, handle and protect important organizational records	L

4.10.1.4 Data protection and privacy of personal information (A.12.1.4)

Security concerns	threatening
Unauthorised modification of personal data	I, A, L
Disclosure of confidential personal data	C, L
Non-compliance with data protection act (of employees or third party contractors)	L
No clearly identified responsibilities	C, I, A, L

4.10.1.5 Prevention of misuse of information processing facilities (A.12.1.5)

Security concerns	threatening
Misuse or unauthorised use of information processing facilities (of employees or third party contractors)	C, I, A, L
Lack of procedures to authorise users	C, I, A, L
Lack of disciplinary actions	C, I, A, L

4.10.1.6 Regulation of cryptographic controls (A.12.1.6)

Security concerns	threatening
Non-compliance with laws, rules and regulations regarding cryptographic controls (of employees or third party contractors)	L

4.10.1.7 Collection of evidence (A.12.1.7)

Security concerns	threatening
Inability to provide legally admissible evidence (insufficient quality and/or completeness)	L

4.10.2 Review of security policy and technical compliance (Clause A.12.2)

Objective: To ensure compliance of systems with organizational security policies and standards.

4.10.2.1 Compliance with security policy (A.12.2.1)

Security concerns	threatening
Non-compliance with the security policy	C, I, A, L
Non-compliance with security controls and/or procedures	C, I, A, L

4.10.2.2 Technical compliance checking (A.12.2.2)

Security concerns	threatening
Incorrect implementation of controls	C, I, A, L
Incorrect business processes	I, A
Unavailability of information or information processing facilities	A
Ineffective controls	C, I, A, L
Penetration testing	C, I, A, L
Technical compliance checking by incompetent or unauthorised persons	C, I, A, L

4.10.3 System audit considerations (Clause A.12.3)

Objective: To maximise the effectiveness, and to minimise interference to/from the system audit process.

4.10.3.1 System audit controls (A.12.3.1)

Security concerns	threatening
Interference by the audit process	I, A
Unauthorised access to information during the audit process	C, I, A, L
Incorrect business processes	I, A
Unavailability of information or information processing facilities	A
Non-compliance with security policy	C, I, A, L
Inability to collect evidence	L

4.10.3.2 Protection of system audit tools (A.12.3.2)

Security concerns	threatening
Lack of integrity of the audit tool	I, A, L
Misuse of audit tools	C, I, A, L
Incorrect business processes	I, A
Inability to collect evidence	L

5 Selection Factors and Constraints

5.1 Selection Factors

5.1.1 Costs

There are a number of cost related issues that need to be considered during the selection of BS 7799 Part 2 control objectives and controls.

Following Section 3, the controls should have been selected on the basis of balanced security, i.e. of complementary technical and non-technical controls, commensurate legal and other obligations, business requirements, and with the risks resulting from risk assessments. But there may still be some opportunity for identifying where additional, cheaper, e.g. non-technical controls could be used to reduce some of the control requirements (and thus reduce the overall cost). Opportunities to fulfil two or more control objectives or security requirements with one control should also be used.

There may be a range of products to fulfil particular technical requirements. To aid the selection, a checklist can be produced that includes identification of the minimum security assurance needed, cost and usability as well as security factors. This can then be used throughout the selection process to ensure that appropriate product(s) are acquired that provide the requisite security and also the best value for money.

It would be inappropriate to recommend controls that are more expensive to implement and manage than the value of the assets they are designed to protect, i.e. the losses, impacts or damages if security incidents occur.

It may also be inappropriate to recommend controls that are more expensive than the budget for security the organization has assigned. However, in this situation great care must be taken because often what the organization is doing in practice is accepting a level of risk by not implementing the controls. In these circumstances, the organization must be clear on the risks it is accepting and not be ignorant of them.

5.1.2 Availability

In considering the controls selected, it may be found that some controls will be difficult or impossible to be implemented for technical reasons, and/or difficult to maintain, e.g. because of some aspect of an existing environment. Further, some controls may not be the most usable from an operational/user acceptability viewpoint. Where such situations are identified, alternative controls will almost certainly have to be identified. These may be non-technical controls – physical, personnel, procedural, etc., to compensate for the lack of a technical control, or alternative technical controls.

If a product is not available to fulfil an identified technical role, there may be others that nearly meet the requirement but need some other accompanying control to meet the requirement, e.g. procedural controls. It may be that the required product is not currently available and there is no acceptable alternative. In this case, management will need to consider other options for risk treatment, such as risk transfer or risk avoidance.

Many situations can be identified, even avoided, by producing and documenting a technical security architecture design as soon as the list of controls identified following Section 3 is known. For obvious reasons, this security architecture should be constructed in line with the overall

organization's technical architecture to ensure compliance. Once the technical security architecture design is agreed it should be possible to identify anomalies, or impossibilities, and cover the requirements in an alternative way.

5.1.3 Implementation and maintenance

When selecting controls, other related factors to be considered are the ease, time and cost of implementation, as ell as the effort necessary for maintenance. If there will be major difficulties, technical or otherwise, with implementation or maintenance of a particular control, or the effort or cost involved is disproportionate to the security benefits to be gained, then consideration should be given to alternative controls. For example, if a technical control will be very difficult to implement because of the existing technical environment, then there may be another similar technical control, or compensating procedural controls, that could be implemented instead. Another example could be where it would be difficult to implement remote maintenance securely, in which case maintenance might have to be accomplished through site visits.

5.2 Constraints

5.2.1 Existing controls

The BS 7799 Part 2 control objectives and controls selected following the process in Section 3 should be additional to any existing and planned controls. In order to achieve that, first the existing and planned controls should be identified and it should be checked which of the following cases is true.

- The existing controls provide sufficient security. In this case, no additional controls should have been selected in Section 3 – if, nevertheless, controls have been selected they should only be implemented if they provide additional security that is necessary, e.g. because of future demands.

- The existing controls do not provide sufficient security. In this case, a decision has to be made to either remove these controls, or to add to them to achieve sufficient security. This decision is dependent on the costs involved (see also 5.1.1), whether an 'upgrade' is possible at all, and the security needed.

An example for the latter case is an organization that controls access to computers with help of passwords, but has no password management system or rules for selecting and handling passwords in place and is not satisfied with the security provided at the moment. There are several possibilities for this organization:

- they can implement a password management system and other rules and controls related to passwords (see also BS 7799 Part 2 Annex A, controls A.9.2.3, A.9.3.1 and A.9.5.4) to improve the security provided by the passwords; or

- they can use other means of user authentication (see also BS 7799 Part 2, Annex A, controls A.9.2.3, A.9.4.3 and A.9.5.3) such as methods based on cryptography or bio-metric techniques if that proves to be more adequate.

In addition, it should be checked whether the controls selected following Section 3 are compatible with other existing and planned controls. For example, physical access controls can be used to support the access control achieved by logical access control mechanisms, and an awareness training for all employees can ensure that these controls are understood and used in day to day business operations.

5.2.2 Have all control objectives and security requirements been addressed?

Before finally deciding on the controls to be implemented, it should be ensured that the control objectives and controls selected fulfil all security requirements that have been addressed.

It should be noted that there always will be a residual risk – it is not possible to achieve total security. So the question should be raised whether these residual risks are acceptable to the organization or not.

First of all, it should be assessed how much the selected controls reduce the identified risks[7], for all the risks that have been identified resulting from threats and vulnerabilities, as well as risks resulting from security breaches and legislative, contractual or business requirements. The organization should decide which risks are considered to be acceptable, and which are not acceptable to the organization. This decision should be made for the whole organization (or at least the ISMS considered) to ensure a consistent level of security. If one or more of the risks are not reduced to an acceptable level by the controls selected, a decision needs to be made on how to progress further.

In many cases, it is most advisable to select additional or different controls using the information given in Sections 3 and 4 to finally reduce the risks to an acceptable level. But it might be the case that this leads to unacceptable costs (see also 5.1.1), or that a reduction to an acceptable level is simply not possible. For example, an organization might want to apply electronic commerce and there is a risk of compromise or modification of financial information involved. The risk is unacceptable to the organization, and the only control that would allow sufficient reduction of the risk would be the use of cryptography. If one business partner of this organization resides in a country where the use of cryptographic means is not allowed, the protection cannot be applied, and the corresponding risk is unacceptable. In such cases, the organization should decide on the most suitable risk treatment option (see also Sections 1.2.3 – 1.2.6). This decision should be a management decision and should be documented. Additional plans to recover from such risks can also be made to reduce the impact if they really occur.

5.2.3 Implementing and maintaining controls

Once the options for risk treatment have been selected, the set of controls is agreed, and suitable products identified, this should be documented in the risk treatment plan for implementation and agreed with the appropriate management. The implementation should take place as soon as possible to avoid security breaches, but has to take account of other major initiatives, such as the installation of new programmes. Where possible, implementation should be effected with minimal or no effect on users and normal business operations, if necessary 'out of hours'.

Once the implementation and the other parts of the "Do" activity in the PDCA model have been completed, and the ISMS has been in operation for a while (and – where applicable – has been certified), the "Check" part pf the PDCA model should start. One important element of the checking activity is the evaluation of the security controls in place, e.g. through a security audit/compliance check review (see also Guide PD 3003 for more details on that). This review will ascertain that the requisite controls are implemented are used and are working correctly, and are providing effective security that is adequate to the requirements. The security concerns listed in Section 4 can support this process.

Checking of the security arrangements should take place on a regular basis, e.g. through such an audit trail content review and analysis, security change management and incident/breach handling.

[7] *The guide PD 3002 'Guide to BS 7799 Risk Assessment' describes the process of how to decide whether a residual risk is acceptable.*

One aspect of implementation and maintenance that should not be overlooked, a control in its own right, is security awareness and training. Even with the best solutions, technical and otherwise, without users being aware of why and how security should be maintained, the required levels of security will not be preserved and security incidents and breaches will surely follow. The same is true if those conducting implementation and maintenance activities, and those with security responsibilities are not sufficiently aware and trained.

Annex A Risk Assessment

This section gives a brief overview of the risk assessment process. A more detailed description is given in PD 3002.

Assessing Risks

Risk assessment methods and techniques are used to identify the risks information processing facilities, or individual system components, are facing. A risk assessment involves the systematic consideration of the following:

- 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;
- the realistic likelihood of such a breach occurring in the light of prevailing threats, vulnerabilities and controls.

Risk Assessment Components

The risk assessment process includes the following components:

Assets

An asset is something that has value to the organization, its business operations and their continuity. Therefore, assets need protection to ensure correct business operations and business continuity. This includes assets such as information and information processing facilities (see also examples below) as well as assets that are essential to the financial strength to the organization (e.g. cash, cash equivalents and tangible items that depreciate). It also includes the resources at the disposal of the business (i.e. non-cash assets in the business portfolio including people, product and process-knowledge and capabilities, and strength of company brands).

Examples of assets include:

information and information processes (including paper documents)	business databases and data files, system documentation, user manuals, operational or support procedures, continuity plans, processing results and process-knowledge, contracts, guidelines, company documentation, documents containing important business results
software	application software, system software, development tools and utilities
physical items	computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units)
human	personnel, customers, subscribers, specialists
brands and image	strength of a company image and reputation, its trade marks and company brands

services	computing and communications services, other services

Security Requirements

Security requirements are from the three main sources listed below and should be documented in an ISMS and considered in the risk assessment:

- 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 organisation's information systems.

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 the information being handled by the information processing facility or service, e.g. its unauthorised destruction, disclosure, modification, corruption, and unavailability or loss. Examples of threats are:

	Threat Types
unauthorised activities	unauthorised access to information, information processing facilities, networks and services, disclosure of information, unauthorised modification of information, theft, unauthorised copying of software
software problems	software malfunctions, malicious code, processing errors
personnel problems	user error, misuse of information processing facilities, fraud
communications problems	mis-or re-routing of messages, denial of service
acts of god	fire, flood, natural disaster

Vulnerabilities

Vulnerabilities are weaknesses associated with an information processing facility and its 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 alone does not cause harm, it is merely a condition or set of conditions that may allow a threat to affect an asset. Examples of vulnerabilities include:

- lack of or inappropriate physical protection;
- wrong selection and management of passwords;
- unprotected or unauthorised connections to the Internet ;
- insecure key management for cryptographic keys;

- security breaches because of a lack of awareness.

Legal 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 identified and 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.

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 identified and 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.

Risks

The objective of the risk assessment is to identify and assess the risks, following the risk assessment process explained below. The risks are calculated from the combination of asset values and assessed levels of related security requirements.

Risk Assessment Process

Assessment of risk involves the following activities[8]:

- identification and valuation of assets;
- the identification of all security requirements, i.e. threats and vulnerabilities, legal and business requirements;
- the assessment of the likelihood of the threats and vulnerabilities to occur, and the importance of legal and business requirements;
- the calculation of risk resulting from these factors;
- the selection of the appropriate risk treatment option; and
- the selection of controls to reduce the risks to an acceptable level.

Asset Identification and Valuation

All assets within the scope of the ISMS should be identified. After fulfilling the objective of asset identification by listing all assets within the scope of the ISMS, values should be assigned to these assets. These values represent the importance of the assets to the business of the organization.

[8] *The risk assessment process is described in full detail in PD 3002 'Guide to BS 7799 Risk Assessment and Risk Management'.*

With some assets such as cash, cash equivalents or tangible items that depreciate this valuation process is reasonably straightforward. With other assets, such as non-cash and intangible assets, current accounting standards and approaches do not generally help in this valuation. However, it is important to assign a value to these types of asset to defend investments, to report to shareholders and of course to decide what protection is needed to safeguard this asset. The process of asset valuation is explained in more detail in PD 3002.

Asset values represent the importance of the assets to the business of the organization. This can be expressed in terms of the impacts from the disclosure, modification, non-availability and/or destruction of information, and other system assets. It should also include impacts from denial of commitment to order, purchase or deliver something, to a price or a liability, or of delivery confirmation. Asset identification and valuation, based on the business needs of an organization, is a major factor in the identification of risks and in selection of controls. Identification and Assessment of Security Requirements

Threats and Vulnerabilities

All threats and vulnerabilities related to the assets within the scope of the ISMS should be identified. After identifying the threats and vulnerabilities, it should be assessed how likely it is that a combination of threats and vulnerabilities occur.

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

- for deliberate threats: the motivation, the capabilities perceived and necessary, resources available to possible attackers, and the perception of attractiveness;
- for 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.

Legal and Business Requirements

Like for the threats and vulnerabilities, all relevant legal and business requirements need to be identified for each of the assets in the scope of the ISMS. This should be followed by a valuation for the legal and business requirements. 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.

Risk Assessment

The objective is to identify and assess the risks to which the information processing facility and its assets are exposed, in order to identify and select appropriate and justified security controls. 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 PD 3002.

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.

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.

For the identified and assessed risks, there are four possible actions an organization might want to take (see also the more detailed description in Section 1.2.3 – 1.2.6 of these options):

- 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).

Selection of Controls

For all those risks where the option 'risk reduction' has been identified as the best possible option to treat the risks, control objectives and controls should be selected to reduce the risks to the acceptable level.

The risk assessment process provides important information about what causes the risks and how the risks can be reduced by the appropriate selection of controls. Therefore, it enables an organization to identify the necessary control objectives and controls from BS 7799 Part 2 to be implemented.

The information obtained during a risk assessment influences the selection of control objectives and controls in many ways (see also Sections 3 and 4):

- the value of an asset shows how much resources (time, money, etc.) should be spent to protect it;
- the requirements for confidentiality, integrity or availability of an asset help to identify applicable controls, e.g. information with a need for availability can be protected by the use of back-up copies, information with a need for integrity can be protected by using any mechanisms detecting unauthorised changes, and information with a confidentiality need may require to be protected by encryption. As these examples show, the controls applicable in one situation are not necessarily relevant to others;
- information on the assessed security requirements can also be basis for the selection of controls; for example, the likelihood of a threat can be reduced, e.g. by making it more difficult for a possible attacker to get (unauthorised) access to the system. Another possibility is the reduction of the damage that an occurrence of a threat would create, e.g. the introduction of an uninterruptable power supply to avoid damage in the case of power fluctuations;
- details of existing controls can have a strong influence on the selection of further controls, since all controls should be compatible and supporting each other, e.g. an already existing control to have unique user IDs is enhanced by the implementation of audit trails and related analysis and monitoring facilities to provide evidence in the case of a security incident;
- the assessed measures of risks can be used to prioritise the risks in order to decide which should be dealt with first, and how to allocate limited resources.

All information obtained from the conduct of a risk assessment should be considered when selecting controls, and in addition other selection criteria like those discussed in Section 5 should be taken into account.

It should be noted that a risk assessment might identify exceptional business risks requiring 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.