Are you ready for a BS 7799 Part 2 Audit

A compliance assessment workbook

BSi
Business Information

“Are you ready for a BS 7799 audit?”

A compliance assessment workbook

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

Contents

1. INTRODUCTION

This document is one of a set of five guides published by DISC to support the use and application of ISO/IEC17799: 2000 and BS 7799 Part 2: 2002. Other guides include:

- 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
- Guide to the implementation and auditing of BS 7799 controls (PD 3004) - Guide to the implementation and auditing of BS 7799 controls
- Guide on the selection of BS 7799 Part 2 controls (PD 3005)

This guide is intended primarily for use by organizations wishing to carry out internal compliance checks of their information security management system (ISMS) against the BS 7799-2:2002 standard. For this purpose it is recommended that the compliance assessments specified in this guide are carried out under the supervision of the person responsible for information security in the organization or by internal audit staff. System developers may also find it a useful reference document when considering the security aspects of new systems. This guide is intended to aid compliance not to define or specify it.

1.1 Scope of this guide

This guide provides a means to help organizations to test the compliance of their ISMS with the requirements of BS 7799-2:2002 using the following check lists:

- ISMS process check workbook to assess the ISMS compliance with the process requirements given in clauses 4 to 7 in BS 7799-2:2002.
- Gap analysis check workbook to assess and record the extent of ISMS compliance with the control requirements laid down in Annex A of BS 7799-2:2002.

The gap analysis check is purely a means to confirm what controls are in place in accordance with the requirements specified in BS 7799-2:2002. Where particular control requirements are not fully satisfied, organizations need to document the reasons why control requirements have not been met. Auditors qualified to carry out assessments to BS 7799 Part 2 will expect, amongst other things, to be able to question such reasons and supporting justification. Please note that this guide is only informative and is not a definitive measure or definition of compliance with BS 7799 Part 2.

Organizations may use the gap analysis to make an informal assessment of their compliance with BS 7799 Part 2 prior, for example, to having an internal ISMS audit or a 2nd party audit carried out by a customer. For accredited certification the gap analysis has no formal status and cannot be taken to form an approved Statement of Applicability (SoA) as it does not meet the SoA requirements defined in BS 7799-2:2002. It does not replace the formal assessment route associated with Part 2 and the PDCA process requirements for establishing, implementing and maintaining an ISMS.

The ISMS process check is a means to confirm that the organization has a set of systems and processes in place to satisfy the requirements specified in BS 7799-2:2002. This check should be applied by organizations preparing for accredited certification, as well as by those preparing for post-certification activities such as surveillance audits and for re-certification. It is a means of being able to check how many activities have been carried out and how many are still to be undertaken. This check does not indicate how well or effective the activities have been, or how correct and effective the implementation of the system of controls is.

1.2 Use of the standards

This guide makes reference to the following standards:

- ISO/IEC 17799:2000 (previously BS 7799-1:1999) - a code of practice that identifies control objectives and controls and provides common practice advice for the implementation of these controls.
- BS 7799-2:2002 - is the specification for an information security management system. This standard is used as the basis for accredited certification.

This guide will be updated following any changes to these standards. Organizations must therefore ensure that the correct version is being used for compliance checks related to pre-certification, certification and post-certification purposes.

1.3 Companion guides

Additional guides are available which provide a more detailed interpretation of the ISO/IEC 17799 and BS 7799 Part 2 standards and practical development advice, i.e. guidance on risk assessment and guidance on the selection of controls.

2. IDENTIFYING THE ISMS SCOPE

It is important both for the organization whose ISMS is being assessed and for the auditors' understanding of the ISMS, that the scope of the ISMS is defined clearly and unambiguously.

Given the complexity of many business applications and processes, as well as the growth of information systems, IT and networking there are many possible ways in which boundaries may be drawn around an ISMS. Similarly the size of organization and its geographical spread will influence the view of what is a suitable scope of the ISMS. It is very rare that business systems and processes work in isolation or are self-contained, as they will have interfaces with other systems. Therefore in defining the scope of the ISMS any interfaces with other systems and processes outside the ISMS boundary need to be taken into consideration.

Guidance on the identification and definition of the ISMS scope is given in the User Guide (PD 3001) which expands on the definition given in BS 7799-2:2002. This describes the ISMS scope in terms of the organization, its location, assets and technology. This should be interpreted to include the information assets, business processes and applications, as well as the technology being used. Although these elements need not be defined in any great detail, it is important that all significant assets are identified.

3. HOW TO USE THIS GUIDE

The aim of the guide is to allow organizations to assess the extent of their ISMS compliance with the requirements specified in BS 7799-2:2002. This section tells you how to prepare for and complete the compliance check. The major component of the compliance check itself is carried out through a questionnaire process. The form and content of the control requirement compliance check questionnaires is described and a sample-completed questionnaire is shown in section 3.3.

The actual compliance check is contained in sections 4 and 5 of this guide:

- **Section 4 ISMS Processes Workbook** - The compliance check of ISMS process requirements. This covers establishing that the prerequisite processes and measures defined Clauses 4 to 7 of BS 7799-2:2002 are in place; and
- **Section 5 Gap Analysis Workbook** - The compliance check of detailed controls from Annex A of BS 7799-2. This covers the identification of what controls are in place and the extent to which they are in place. Additionally, a possibility is given to document the reasons behind any non-implementation of controls, and to explain the rationale for implementing controls, e.g. where this has been done in a non-standard manner.

3.1 ISMS Process Requirements

Introduction

The compliance check on the ISMS processes covers those set of processes defined in BS 7799-2:2002 based on the PDCA model. This set of processes covers an on-going cycle of activities aimed at establishing effective information security management through a programme of continual improvement.

Amongst other things the ISMS processes addresses the assets to be protected, a systematic approach to risk management, the selection of a system of controls and the other processes used to implement and maintain an ISMS according to the PDCA model (see clause 4 of BS 7799-2:2002 for details):

- Plan (processes to establish the ISMS)
- Do (processes to implement and operate the ISMS)
- Check (processes to monitor and review the ISMS)
- Act (processes to maintain and improve the ISMS)

The ISMS system of controls should be implemented effectively and should be monitored and reviewed regularly to ensure their continuous effectiveness; appropriate documentation in support of this should be in place, up to date, accurate and available for inspection and reference; and appropriate records should be maintained to demonstrate continuing compliance with BS 7799: Part 2.

The certification audit process will ensure that the organization has a set of processes in place to cover the above objectives and the post certification audits will need to check these are maintained to ensure continuing compliance.

Section 4 of this guide considers these process requirements.

Check Lists

There are two basic questions and these may be addressed to each of the process requirements. The questions are:

Q1 - Is a relevant process in place to satisfy the prescriptive "shall" requirement in clauses 4 to 7 of BS 7799 Part 2? Three answers are possible:

- **Yes** – there is process in place, which completely fulfil the requirement. Some explanation may be required justifying this answer - see "comments" below.

- **Partly** – a process is in place, which address the requirement but not sufficiently to allow an answer of YES.
- **No** - there is no process in place to address the requirement.

Q2 - If the requirement has either not been implemented on only partially implemented, why not? It will be important to understand the reasons and justification for partial or non-implementation.

3.2 Control requirements

Introduction

Annex A of BS 7799-2:2002 contains the detailed control requirements under ten general headings. This guide presents each of the control requirements in question form and allows organizations to indicate:

- Whether the requirement has been implemented;
- Whether the requirement has been partially or not fully implemented and the reason(s) and justification why;
- Whether the requirement has not been implemented at all and the reason(s) and justification why.

It should be understood that reasons for non-implementation may not necessarily be seen as sufficient justification by external auditors whose task is to assess the ISMS to BS 7799: Part 2.

Organizations may wish to further refine the process defined in this guide with more detailed questions per control requirements within each general category. This might be necessary to completely assess all details of a specific control implementation in place in an organization. Due to the number of controls, this might be a work intense task, but will lead to a thorough assessment of the implementation status. In addition, such a questionnaire can be used in several stages of the PDCA process.

Introduction

There are two basic questions and these may be addressed to each control requirement. The questions are:

Q1 - Has this control requirement been implemented? Three answers are possible:

- **Yes** - this means that measures are in place, which completely fulfil the requirement. Some explanation may be required justifying this answer - see "comments" below.
- **Partly** - some measures are in place, which address the requirement but not sufficiently to allow an answer of YES.
- **No** - no measures have been taken to address the requirement. This is also the correct answer where the control is not relevant to the system under review. For example, the control requirement A.10.3.2 "Encryption shall be applied to protect the confidentiality of sensitive or critical information" will not be appropriate to systems, which do not contain sensitive or critical information. In these circumstances the correct answer to question 1 is therefore "No". Question 2 would then be answered by stating that the control is Not Applicable (see below). A "No" response may also be given if a control requirement is relevant but is implemented via another control.

Q2 - If the requirement has either not been implemented on only partially implemented, why not? It will be important to understand the reasons and justification for partial or non-implementation.

The processes surrounding the ISMS PDCA model are based on various risk management processes. Therefore, a certification audit will check the implemented ISMS against the risk management processes that have been used. One important requirement is that any implement system of controls can be traced back to the risk assessment and risk treatment processes. Consequently if this compliance check is carried out just prior to the certification, e.g. as a pre-certification audit, then the absence or non-applicability of controls should be justified on the results of the risk assessment. One example of such a justification is that the implementation of a particular control could not be justified by the levels of risk exposure.

If this compliance check is carried out early in the ISMS process as a gap analysis before embarking on the risk assessment then there may be many other reasons for the absence or non-applicability of controls. For example, (i) financial constraints regarding the existing budget available for security, (ii) environmental factors that may influence the selection of controls such as space availability, climate conditions, surrounding natural and urban geography, (iii) technology reasons as the controls may be infeasible due to (say) the incompatibility of hardware and software, (iv) time constraints as not all control requirements can be implemented immediately due to say the need to carry out upgrades to existing systems and (v) the control requirement may not be applicable to the organization.

COMMENTS - In all such cases some further comment should be given to expand on the particular control implementation, or reasons for partial or non-implementation. Such comments could include:

- Where control requirements are deemed to be in place it may be useful to describe the way in which they have been implemented. This in itself may lead to a recognition that some work still needs to be done in that area, or support the activities described in the 'Check' part of the PDCA model. Alternatively, setting out the implemented controls in this way may indicate that more is being done than necessary and that savings can be made by reducing some controls.
- Where requirements have not or only been partially met, an indication should be given of what steps are to be taken and over what time period to mitigate the (partial) absence of controls in support of the requirement.
- In some cases a decision may have been made to take no further action to implement controls in a given area, in effect, a decision has been taken to accept this as a potential risk. In any case, such a decision should be clearly documented and justified to be fully understood and explained.

A sample completed questionnaire

To help those completing this guideline an example page from the questionnaire section follows.

BS 7799-2:2002 Information security management systems.
A.9 Access control
A.9.7 Monitoring system access and use
Objective: To detect unauthorized activities

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.7.1 Are audit logs of exceptions and other security relevant events produced and kept for an agreed period of time?		✓	
A.9.7.2 Have procedures for monitoring the use of information processing facilities been established and are the results of these monitoring activities reviewed regularly?	✓		
A.9.7.3 Are all computer clocks synchronized for accurate recording?			✓

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason in the following table.

Control	Reasons and justification
A.9.7.1	The operating system provides some audit facilities such as records of log-ons and log-offs, by user and time/date. More detailed accounting records are not available with the system and would need the purchase of an additional accounting package. There is currently insufficient funding for this, especially as a system upgrade is anticipated within the next 18 months. It is expected that a system upgrade will be chosen which offers more detailed accounting down to file and record level and the type of access made e.g. read, write, execute etc.
A.9.7.3	Access to the central processor is via dumb terminals with only one clock being active on the central processor. Synchronisation is not therefore relevant.

4. ISMS PROCESSES WORKBOOK (ASSESSMENT OF ISMS PROCESS REQUIREMENTS)

It is important to lay a firm foundation for the ISMS process within which a system of controls is implemented. BS 7799-2:2002 clauses 4 to 7 define the set of processes for the ISMS. The User Guide PD 3001 in this series expands on the issues involved. By referring to these two documents as necessary you should check and follow the compliance checks addressed in this clause in the following tables.

Guidance on completing the questionnaires will be found at section 3.1.2 of this document.

Please note that the following ISMS process requirements are mandatory and shall be addressed by any organization that aims at accredited BS 7799-2:2002 certification – as stated in BS 7799-2, Section 1.2: *"Excluding any of the requirements specified in clauses 4 to 7 of this standard is not acceptable."*

PD 3003:2002 "Are you ready for a BS 7799 Part 2 Audit?"

Compliance assessment workbook

Internal project reference number:

Date of audit:

Scope of this compliance workbook:

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

a) Define the scope of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology.

.**Q1.** Consider the following aspects relating to the ISMS scope. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.1.a.1 Is there a document, which describes unambiguously the scope of the ISMS?			
4.2.1.a.2 Are significant exclusions from the scope identified and the reasons for their exclusion explained clearly?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.a.1		
4.2.1.a.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

b) Define an ISMS policy in terms of the characteristics of the business, the organisation, its location, assets and technology.

Q1. Consider the following aspects relating to ISMS policy. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.1.b.1 Is there an Information Security Policy in place, which covers the defined scope?			
4.2.1.b.2 Does the policy provide a framework for setting objectives and for establishing direction and principles for action regarding information security?			
4.2.1.b.3 Does the policy take account of business and legal or regulatory requirements and contractual security obligations?			
4.2.1.b.4 Does the policy establish the strategic, organisational and risk management context in which the establishment and maintenance of the ISMS takes place?			
4.2.1.b.5 Does the policy establish criteria against which risk will be evaluated and the structure of the risk assessment is defined?			
4.2.1.b.6 Has the policy been approved by the management?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.b.1		
4.2.1.b.2		
4.2.1.b.3		
4.2.1.b.4		
4.2.1.b.5		
4.2.1.b.6		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

c) Define a systematic approach to risk assessment

Q1. Consider the following aspects relating to the risk assessment approach. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.1.c.1 Has a method of risk assessment been defined that is suited to the ISMS and the identified business information security, legal and regulatory requirements?			
4.2.1.c.2 Have policy and objectives for the ISMS to reduce risks to acceptable levels been set?			
4.2.1.c.3 Have criteria for accepting the risks been determined?			
4.2.1.c.4 Have the levels for acceptable risk been determined based on the criteria in 4.2.1.c.3?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.c.1		
4.2.1.c.2		
4.2.1.c.3		
4.2.1.c.4		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

d) Identify the risks

Q1. Consider the following aspects relating to risk identification. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.1.d.1 Is there a process in place and being used for the identification of risks?			
4.2.1.d.2 Does this process identify the assets within the scope of the ISMS, the threats to these assets, the vulnerabilities that might be exploited by the threats and the impacts that losses of confidentiality, integrity and availability may have on the assets?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.d.1		
4.2.1.d.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

e) Assess the risks

Q1. Consider the following aspects relating to the assessment of risks. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.1.e.1 Is there a process in place and being used for assessing the risks?			
4.2.1.e.2 Does this process assess the business harm that might result from a security failure taking account the potential loss of confidentiality, integrity and availability of the ISMS assets?			
4.2.1.e.3 Does this process assess the realistic likelihood of such a security failure occurring in the light of prevailing threats and vulnerabilities and impacts on the ISMS assets?			
4.2.1.e.4 Does this process estimate the levels of risk?			
4.2.1.e.5 Does this process determines whether the risk is acceptable or requires the treatment using the criteria using the criteria in 4.2.1 c)?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.e.1		
4.2.1.e.2		
4.2.1.e.3		
4.2.1.e.4		
4.2.1.e.5		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

f) Identify and evaluate options for the treatment of risks.

Q1. Consider the following aspect relating to the process of risk treatment. Tick one box.

Aspect	Yes	Partly	No
4.2.1.f.1 Is there a process in place and being used to identify and evaluate options for the treatment of risks?			
4.2.1.f.2 Does this process take account the following possible actions: (i) apply controls to treat the risks, (ii) knowingly and objectively accept the risks providing they clearly satisfy the organization's policy and criteria for risk acceptance (see 4.2.1 c), (iii) taking action to avoid the risks, or (iv) transferring the risks to other parties such as insurers, suppliers?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.f.1		
4.2.1.f.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

g) Select control objectives and controls for the treatment of risks

Q1. Consider the following aspect relating to the process of selecting controls. Tick one box.

Aspect	Yes	Partly	No
4.2.1.g.1 Is there a process in place and being used for selecting the control objectives and controls from Annex A of BS 7799 Part 2:2002?			
4.2.1.g.2 Does this process ensure that the selection of controls is justified on the basis of the risk assessment and risk treatment?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.g.1		
4.2.1.g.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

h) Prepare a Statement of Applicability

Q1. Consider the following aspect relating to the process of preparing a statement of applicability. Tick one box.

Aspect	Yes	Partly	No
4.2.h.1 Is there a process in place and being used for the preparing a Statement of Applicability (SoA)?			
4.2.h.2 Has a Statement of Applicability (SoA) been prepared which justifies the decision taken for or against each control objectives and controls selected in 4.2.1 g)?			
4.2.h.3 Does the Statement of Applicability (SoA) record the exclusion of any control objectives and controls listed in Annex A of BS 7799-2:2002?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.h.1		
4.2.1.h.2		
4.2.1.h.3		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use

4.2.1 Establish the ISMS

i) Obtain management approval of the proposed residual risks and authorisation to implement and operate the ISMS.

Q1. Consider the following aspect relating to the process approving proposed residual risks and ISMS authorisation. Tick one box.

Aspect	Yes	Partly	No
4.2.1.i.1 Is there a process in place and being used for obtaining management approval of residual risks?			
4.2.1.i.2 Is there a process in place and being used for obtaining management authorization for the implementation and operation of the ISMS?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.1.i.1		
4.2.1.i.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.2.2 Implement and operate the ISMS

Q1. Consider the following aspects relating to the processes and procedures an organisation needs to have in place and being used for the implementation and operation of the ISMS. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.2.a Is there a process in place and being used for formulating a risk treatment plan that identifies the appropriate management action, responsibilities and priorities for managing information security risks ?			
4.2.2.b Is there a process in place and being used for implementing the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities?			
4.2.2.c Is there a process in place and being used for implementing the controls selected in 4.2.1 (g) to meet the control objectives?			
4.2.2.d Is there a process in place and being used for implementing necessary training and awareness programmes (in accordance with clause 5.2.2)?			
4.2.2.e Is there a process in place and being used for managing the operations associated with the ISMS implementation?			
4.2.2.f Is there a process in place and being used for managing the resources need for the ISMS implementation?			
4.2.2.g Are there procedures and other controls being implemented capable of enabling prompt detection of and response to security incidents?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.2.a		
4.2.2.b		
4.2.2.c		
4.2.2.d		
4.2.2.e		
4.2.2.f		
4.2.2.g		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.2.3 Monitor and review the ISMS

Q1. Consider the following aspects relating to the processes and procedures an organisation needs to have in place and use for monitoring and reviewing the ISMS. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.3.a Are monitoring procedures and other controls being executed to: a) Detect errors in the results of processing promptly; b) Identify failed and successful security breaches and incidents promptly; c) Enable management to determine whether the security activities delegated to people or implement by information technology are performing as expected; d) Determine the actions to be taken to resolve a breach of security reflecting business priorities?			
4.2.3.b Is there a process in place and being used for the regular review of the effectiveness of the ISMS (including meeting security policy objectives and review of security controls) taking into account results of security audits, incidents, suggestions and feedback from all interested parties?			
4.2.3.c Is there a process in place and being used for reviewing the level of residual risk and acceptable risk taking into account changes to: a) The organisation; b) Technology; c) Business objectives and processes; d) Identified threats; e) External events, such as changes to the legal or regulatory environment and changes in social climate?			
4.2.3.d Are internal ISMS audits conducted at planned intervals?			
4.2.3.e Is there a process in place and being used for a regular management review of the ISMS (at least once a year) to ensure that the scope remains adequate and for identifying improvements in the ISMS process?			
4.2.3.f Is there a process in place and being used to record actions and events that could have an impact on the effectiveness or performance of the ISMS?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.3.a		
4.2.3.b		
4.2.3.c		

4.2.3.d		
4.2.3.e		
4.2.3.f		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.2.4 Maintain and improve the ISMS

Q1. Consider the following aspects relating to the processes and procedures an organisation needs to have in place and use for maintaining and improving the ISMS. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.2.4.a Is there a process in place and being used to implement the identified improvements in the ISMS?			
4.2.4.b Is there a process in place and being used to take appropriate corrective and preventive actions in accordance with 7.2 and 7.3, and to apply the lessons learnt from the security experiences of other organizations and those of the organization itself?			
4.2.4.c Is there a process in place and being used to communicate the results and actions and agree with all interested parties?			
4.2.4.d Is there a process in place and being used to ensure that the improvements achieve their intended objectives?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.2.4.a		
4.2.4.b		
4.2.4.c		
4.2.4.d		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.3 Documentation requirements
4.3.1 General

Q1. Consider the following aspects relating to the general requirements related to documentation. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.3.1.a Are documented statements of security policy and control objectives readily available?			
4.3.1.b Is there a document, which describes the scope of the ISMS and the procedures and controls in support of the ISMS readily available?			
4.3.1.c Is the risk assessment report readily available?			
4.3.1.d Is the risk treatment plan readily available?			
4.3.1.e Are documented procedures readily available which ensure the effective planning, operation and control of the information security processes?			
4.3.1.f Are records readily available that provide evidence of conformity to requirements and the effective operation of the ISMS?			
4.3.1.g Is a copy of the statement of applicability readily available for inspection?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.3.1.a		
4.3.1.b		
4.3.1.c		
4.3.1.d		
4.3.1.e		
4.3.1.f		
4.3.1.g		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them. See section 3.3 for details. Use additional sheets if necessary.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.3 Documentation requirements
4.3.2 Control of documents

Q1. Consider the following aspects relating to the control of documentation. Tick one box for each aspect.

Aspect	Yes	Partly	No
4.3.2.a Is there a process in place and being used to protect and control the documents required by the ISMS?			
4.3.2.b Is there a documented procedure in place and being used that supports this process which defines the management actions to:			
a) Approve documents for adequacy prior to issue;			
b) Review and update documents as necessary and re-approve documents;			
c) Ensure that changes and the current revision status of documents are identified;			
d) Ensure that the most recent versions of relevant documents are available at points of use;			
e) Ensure that documents remain legible and readily identifiable;			
f) Ensure that documents of external origin are identified;			
g) Ensure that the distribution of documents is controlled;			
h) Prevent the unintended use of obsolete documents;			
i) Apply suitable identification to them if they are retained for any purpose?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.3.2.a		
4.3.2.b		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
4.3 Documentation requirements
4.3.3 Control of records

Q1. Consider the following aspect relating to the control of records. Tick one box.

Aspect	Yes	Partly	No
4.3.3.a Is there a process in place and being used to establish, maintain and control records?			
4.3.3.b Does this process take into account relevant legal requirements?			
4.3.3.c Does this process ensure the records remain legible, readily identifiable and retrievable?			
4.3.3.d Are the controls needed to identify, store, protect, retrieve, retain and dispose of records in place and document?			
4.3.3.e Are records kept of the performance of the processes defined in 4.2.1 to 4.2.4 and of all occurrences of security incidents related to the ISMS?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
4.3.3.a		
4.3.3.b		
4.3.3.c		
4.3.3.d		
4.3.3.e		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
5 Management responsibility
5.1 Management commitment

Q1. Consider the following aspect relating to ensuring management commitment. Tick one box.

Aspect	Yes	Partly	No
5.1 Is there a process in place and being used to ensure that management provides evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:			
a) Establishing an information security policy;			
b) Ensuring that information security objectives and plans are established;			
c) Establishing roles and responsibilities for information security;			
d) Communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;			
e) Providing sufficient resources to develop, implement, operate and maintain the ISMS (see 5.2.1);			
f) Deciding the acceptable level of risk;			
g) Conducting management reviews of the ISMS (in accordance with clause 6 of BS 7799 Part 2:2002).?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
5.1		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
5 Management responsibility
5.2 Resource management

Q1. Consider the following aspect relating to the management of resources. Tick one box.

Aspect	Yes	Partly	No
5.2.1 Is there a process in place which the organisation uses to determine and provide the resources needed to: a) Establish, implement, operate and maintain an ISMS; b) Ensure that information security procedures support the business requirements; c) Identify and address legal and regulatory requirements and contractual security obligations; d) Maintain adequate security by correct application of all implemented controls; e) Carry out reviews when necessary, and to react appropriately to the results of these reviews; f) Where required, improve the effectiveness of the ISMS?			
5.2.2.a Is there a process in place and being used to ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by: a) Determining the necessary competencies for personnel performing work effecting the ISMS; b) Providing competent training and, if necessary, employing competent personnel to satisfy these needs; c) Evaluating the effectiveness of the training provided and actions taken; d) Maintaining records of education, training, skills, experience and qualifications (see 4.3.3)?			
5.2.2.b Is there a process in place and being used to ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
5.2.1		
5.2.2.a		
5.2.2.b		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
6 Management review of the ISMS
6.1 General

Q1. Consider the following aspect relating to the general requirements regarding the review of the ISMS. Tick one box.

Aspect	Yes	Partly	No
6.1.1 Is there a process in place and being used to ensure that management reviews the organization's ISMS at planned intervals to check the continuing suitability, adequacy and effectiveness of the ISMS?			
6.1.2 Do these reviews include the assessment of opportunities for improvement and the need for changes to the ISMS, including the security policy and security objectives?			
6.1.3 Are the results of these reviews documented, and are records maintained in accordance with 4.3.3?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
6.1.1		
6.1.2		
6.1.3		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
6 Management review of the ISMS
6.2 Review input

Q1. Consider the following aspect relating to the input provide to the management review. Tick one box.

Aspect	Yes	Partly	No
6.2 Is there a process in place and being used to ensure that the input to the management review includes information on:			
a) Results of audits;			
b) Feedback from interested parties;			
c) Techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;			
d) Status of preventive and corrective actions;			
e) Vulnerabilities or threats not adequately addressed in the previous risk assessment;			
f) Follow-up actions from previous management reviews;			
g) Any changes that could affect the ISMS;			
h) Recommendations for improvement?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
6.2		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
6 Management review of the ISMS
6.3 Review output

Q1. Consider the following aspect relating to the decisions and actions taken resulting from the management review. Tick one box.

Aspect	Yes	Partly	No
6.3 Is there a process in place and being used to ensure that the output from the management review includes any decisions and actions related to: a) Improvement of the effectiveness of the ISMS; b) Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to: i. Business requirements; ii. Security requirements; iii. Business processes effecting the existing business requirements; iv. Regulatory or legal environment; v. Levels of risk and/or levels of risk acceptance. c) Resource needs?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
6.3		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
6 Management review of the ISMS
6.4 Internal ISMS audit

Q1. Consider the following aspect relating to an internal ISMS audit function. Tick one box.

Aspect	Yes	Partly	No
6.4.a Is there a process in place and being used to ensure that the organization conducts internal ISMS audits at planned intervals to determine whether control objectives, controls, processes and procedures of its ISMS: a) Conform to the requirements of this standard and relevant legislation or regulations; b) Conform to the identified information security requirements; c) Are effectively implemented and maintained; d) Perform as expected?			
6.4.b Is there an audit programme in place, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits.?			
6.4.c Is audit criteria, scope, frequency and methods defined and documented?			
6.4.d Is there a process in place and being used for the selection of auditors that ensures objectivity and impartiality of the audit process and that auditors shall not audit their own work?			
6.4.e Is there a documented procedure in place and being used that defines the responsibilities and requirements for planning and conducting of audits and for reporting results and maintaining records?			
6.4.f Is there a process in place and being used to ensure that management responsible for the area being audited carry out actions to eliminate nonconformities and their causes without undue delay?			
6.4.g Is there a process in place and being used to ensure that improvement activities include the verification of the actions taken and the reporting of verification results?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
6.4.a		
6.4.b		
6.4.c		
6.4.d		
6.4.e		
6.4.f		

6.4.g		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
7 ISMS improvement
7.1 Continual improvement

Q1. Consider the following aspect relating to the continual improvement of the ISMS. Tick one box.

Aspect	Yes	Partly	No
7.1 Is there a process in place and being used to ensure that the organization continually improves the effectiveness of the ISMS through the use of the information security policy, security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
7.1		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
7 ISMS improvement
7.2 Corrective action

Q1. Consider the following aspect relating to taking corrective action to eliminate nonconformities. Tick one box.

Aspect	Yes	Partly	No
7.2.a Is there a process in place and being used to ensure that action is taken to eliminate the causes nonconformities associated with the implementation and operation of the ISMS in order to prevent recurrence?			
7.2.b Is there a documented procedure for corrective actions in place and being used which covers the following requirements: a) Identification of nonconformities of the implementation and/or operation of the ISMS; b) Determination of the causes of nonconformities; c) Evaluation of the need for actions to ensure that nonconformities do not recur; d) Determination and implementing the corrective action needed; e) Recording the results of action taken (see clause 4.3.3); f) Review of corrective action taken?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
7.2.a		
7.2.b		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
7 ISMS improvement
7.3 Preventive action

Q1. Consider the following aspect relating to taking preventive action to guard against future nonconformities. Tick one box.

Aspect	Yes	Partly	No
7.3.a Is there a process in place and being used to ensure that action is taken to guard against future nonconformities in order to prevent occurrence?			
7.3.b Does this process ensure that any preventive actions taken are appropriate to the impact of the potential problems?			
7.3.c Is there a documented procedure in place and being used for preventive actions which covers the following requirements:			
a) Identification of potential nonconformities and their causes;			
b) Determination and implementation of the preventive action to be taken;			
c) Recording the results of the preventive action taken (see clause 4.3.3);			
d) Review of preventive action taken;			
e) Identification of the changed risks and ensuring that attention is focussed on the significantly changed risks?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Aspect	Reasons and justification	Action to be taken
7.3.a		
7.3.b		
7.3.c		

COMMENTS: Enter a wider explanation of the reason(s) indicated above. Where aspects are already addressed it may be helpful to detail them.

5. GAP ANALYSIS WORKBOOK (ASSESSMENT OF DETAILED CONTROLS)

The following questionnaires should be addressed to determine the extent to which appropriate control requirements have been implemented within the identified system or systems. Guidance on completing the questionnaires will be found at section 3.2 of this document.

Please note that exclusions to the following control requirements can only be made if these exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable regulatory requirements. Any exclusions of controls found to be necessary to satisfy the risk acceptance criteria need to be justified and evidence need to be provided that the associated risks have been properly accepted by accountable people.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.3 Security policy
A.3.1 Information security policy
Objective: To provide management direction and support for information security.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.3.1.1 Is a published policy document, approved by management, published and communicated, as appropriate, to all employees?			
A.3.1.2 Is the published policy reviewed regularly, and in case of influencing changes?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.3.1.1	
A.3.1.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.4 Organizational security
A.4.1 Information security infrastructure
Objective: To manage information security within the organization.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.4.1.1(a) Is a management forum in place to ensure that there is clear direction and visible management support for security initiatives?			
A.4.1.1(b) Does the management forum promote security through appropriate commitment and adequate resourcing?			
A.4.1.2 Where appropriate to the size of the organization, is the implementation of information security controls co-ordinated through a cross-functional forum of management representatives from relevant parts of the organization?			
A.4.1.3 Are responsibilities for the protection of individual assets and for carrying out specific security processes clearly defined?			
A.4.1.4 Is there a management authorization process in place for new information processing facilities?			
A.4.1.5 Is specialist advice on information security sought from either internal or external advisors and co-ordinated throughout the organization?			
A.4.1.6 Does your organization maintain appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators?			
A.4.2.1.7 Is the implementation of the information security policy in your organization independently reviewed?			

Continued on next page.

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.4 Organizational security
A.41.1 Information security infrastructure (Continued from previous page)

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.4.1.1	
A.4.1.2	
A.4.1.3	
A.4.1.4	
A.4.1.5	
A.4.1.6	
A.4.1.7	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.4 Organizational security
A.4.2 Security of third party access
Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.4.2.1 Have the risks associated with access to organizational information processing facilities by third parties been assessed and appropriate security controls implemented?			
A.4.2.2 Do contracts with third parties involving access to organizational information processing facilities specify all necessary security requirements and conditions?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.4.2.1	
A.4.2.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.4 Security organization
A.4.3 Outsourcing
Objective: To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.4.3.1 Are the security requirements of the organization outsourcing the management and control of all or some of its information systems, networks and/or desk top environments clearly defined and agreed between all parties, and addressed in the outsourcing contract(s)?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.4.3.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.5 Asset classification and control
A.5.1 Accountability for assets
Objective: To maintain appropriate protection of organizational assets.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.5.1.1 Is there an inventory of all important assets associated with each information system drawn up and maintained?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.5.1.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.5 Asset classification and control
A.5.2 Information classification
Objective: To ensure that information assets receive an appropriate level of protection.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.5.2.1 Are classifications and associated protective controls suited to business needs for sharing or restricting information, and the business impacts associated with such needs?			
A.5.2.2 Are procedures in place for information labelling and handling in accordance with a classification scheme adopted by your organization?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.5.2.1	
A.5.2.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.6 Personnel security
A.6.1 Security in job definition and resourcing
Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.6.1.1 Do job definitions include security roles and responsibilities as defined in the organization's information security policy?			
A.6.1.2 Are verification checks on permanent staff, contractors and temporary staff carried out at the time of job applications?			
A.6.1.3 Do employees sign a confidentiality agreement as part of their initial terms and conditions of employment?			
A.6.1.4 Are the employee's responsibilities for information security stated in terms and conditions of employment?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.6.1.1	
A.6.1.2	
A.6.1.3	
A.6.1.4	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.6 Personnel security
A.6.2 User training
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.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.6.2.1 Are employees of the organization and, where relevant, third party users, given appropriate training and regular updates in organizational policies and procedures?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.6.2.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.6 Personnel security
A.6.3 Responding to security incidents and malfunctions
Objective: To minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.6.3.1 Are security incidents reported through appropriate management channels as soon after an incident as possible?			
A.6.3.2 Are users required to note and report any observed or suspected security weaknesses in, or threats to, systems or services?			
A.6.3.3 Are there procedures for reporting software malfunctions, and are they followed?			
A.6.3.4 Are mechanisms in place to enable the type, volume and cost of incidents and malfunctions to be quantified and monitored?			
A.6.3.5 Are violations of organizational security policies and procedures by employees dealt with through a formal disciplinary process?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.6.3.1	
A.6.3.2	
A.6.3.3	
A.6.3.4	
A.6.3.5	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.7 Physical and environmental security
A.7.1 Secure areas
Objective: To prevent unauthorized access, damage and interference to business premises and information.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.7.1.1 Have security perimeters been used to protect areas that contain information processing facilities?			
A.7.1.2 Are the secure areas protected by appropriate entry controls to ensure that only authorized personnel have access?			
A.7.1.3 Have secure areas been created to protect offices, rooms and facilities with special security requirements?			
A.7.1.4 Are there additional controls and guidelines for working in secure areas to enhance the security provided by physical controls?			
A.7.1.5 Are delivery and loading areas controlled and, if possible, isolated from information processing facilities to avoid unauthorised access?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.7.1.1	
A.7.1.2	
A.7.1.3	
A.7.1.4	
A.7.1.5	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.7 Physical and environmental security
A.7.2 Equipment security
Objective: To prevent loss, damage or compromise of assets and interruption to business activities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.7.2.1 Is equipment sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access?			
A.7.2.2 Is equipment protected from power failures and other electrical anomalies?			
A.7.2.3 Is power and telecommunications cabling carrying data or supporting information services protected from interception or damage?			
A.7.2.4 Is equipment correctly maintained to enable its continued availability and integrity?			
A.7.2.5 Is there a management authorization process in place regarding the use of equipment for information processing outside the organization's premises?			
A.7.2.6 Is information erased from equipment prior to disposal or re-use?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.7.2.1	
A.7.2.2	
A.7.2.3	
A.7.2.4	
A.7.2.5	
A.7.2.6	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.7 Physical and environmental security
A.7.3 General controls
Objective: To prevent compromise or theft of information and information processing facilities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.7.3.1 Does the organization operate a clear desk and clear screen policy to protect information from unauthorized access, loss or damage?			
A.7.3.2 Does the removal of equipment, information or software belonging to the organization require the authorization of management?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.7.3.1	
A.7.3.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.1 Operational procedures and responsibilities
Objective: To ensure the correct and secure operation of information processing facilities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.8.1.1 Are operating procedures identified in the security policy documented and maintained?			
A.8.1.2 Are changes to information processing facilities and systems controlled?			
A.8.1.3 Have incident management responsibilities and procedures been established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trials and logs?			
A.8.1.4 Are duties and areas of responsibilities segregated in order to reduce the opportunities for unauthorized modification or misuse of information or services?			
A.8.1.5 Are development and testing facilities separated from operational systems and are there rules for the migration of software from development to operation status defined and documented?			
A.8.1.6 Prior to using external facilities management services, have the risks been identified and appropriate security controls agreed with the contractor, and incorporated into the contract?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.1.1	
A.8.1.2	
A.8.1.3	
A.8.1.4	
A.8.1.5	
A.8.1.6	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.2 System planning and acceptance
Objective: To minimize the risk of systems failure.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.8.2.1 Are capacity demands monitored and projections of future capacity requirements made to enable adequate for processing power and storage to be made available?			
A.8.2.2 Are acceptance criteria established for new information systems, upgrades and new versions and suitable tests carried out prior to acceptance?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.2.1	
A.8.2.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.3 Protection against malicious software
Objective: To protect the integrity of software and information from damage by malicious software.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.8.3.1 Are detection and prevention controls to protect against malicious software and appropriate user awareness procedures implemented?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.3.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.4 Housekeeping
Objective: To maintain the integrity and availability of information processing and communication services.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.8.4.1 Are back-up copies of essential business information and software taken and tested regularly?			
A.8.4.2 Do operational staff maintain a log of their activities and are these logs subject to regular, independent checks?			
A.8.4.3 Are faults reported and is corrective action taken?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.4.1	
A.8.4.2	
A.8.4.3	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.5 Network management
Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.8.5.1 Are a range of controls implemented to achieve and maintain security in networks?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.5.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.6 Media handling and security
Objective: To prevent damage to assets and interruptions to business activities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.8.6.1 Is the management of removable computer media such as tapes, disks, cassettes and printed reports controlled?			
A.8.6.2 Have procedures been established for the secure and safe disposal of media?			
A.8.6.3 Are procedures established for the handling and storage of information to protect from unauthorized disclosure or misuse?			
A.8.6.4 Is system documentation protected from unauthorized access?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.6.1	
A.8.6.2	
A.8.6.3	
A.8.6.4	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.8 Communications and operations management
A.8.7 Exchanges of information and software
Objective: To prevent loss, modification or misuse of information exchanged between organizations.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.8.7.1 Have agreements been established for the electronic and manual exchange of information and software between organizations?			
A.8.7.2 Is media in transit protected from unauthorized access, misuse or corruption?			
A.8.7.3 Is electronic commerce protected against fraudulent activity, contract dispute and disclosure or modification of information?			
A.8.7.4 Has a policy been developed for the use of electronic mail and have controls been implemented to control the security risks created by electronic mail?			
A.8.7.5 Have policies and guidelines been prepared and implemented to control the business and security risks associated with electronic office systems?			
A.8.7.6 Is there a formal authorization process applied before information is made publicly available and is the integrity of such information protected to prevent unauthorized modification?			
A.8.7.7 Have policies, procedures and controls been implemented to protect the exchange of information through the use of voice, facsimile and video communications facilities?			

Continued on next page

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.8.7.1	
A.8.7.2	
A.8.7.3	
A.8.7.4	
A.8.7.5	
A.8.7.6	
A.8.7.7	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.1 Business requirement for access control
Objective: To control access to information.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.9.1.1 Are business requirements for access control defined and documented, and is access restricted to what is defined in the access control policy?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.1.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.2 User access management
Objective: To ensure that access rights to information systems are appropriately authorized, allocated and maintained.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.2.1 Are procedures in place for the formal registration and de-registration of users for granting access to all multi-user information systems and services?			
A.9.2.2 Is the allocation and use of privileges restricted and controlled?			
A.9.2.3 Is the allocation of passwords controlled through a formal management process?			
A.9.2.4 Are user access rights reviewed by management at regular intervals using a formal process?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.2.1	
A.9.2.2	
A.9.2.3	
A.9.2.4	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.3 User responsibilities
Objective: To prevent unauthorized user access.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.3.1 Are users required to follow good security practices in the selection and use of passwords?			
A.9.3.2 Are users required to ensure that unattended equipment has appropriate protection?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.3.1	
A.9.3.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.4 Network access control
Objective: Protection of networked services.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.4.1 Are users only permitted direct access to the services that they are specifically authorized to use?			
A.9.4.2 Is the path from the user terminal to the computer service controlled?			
A.9.4.3 Is access by remote users subject to an authentication check?			
A.9.4.4 Are connections to remote computer systems authenticated?			
A.9.4.5 Is access to diagnostic ports securely controlled?			
A.9.4.6 Are controls in place in networks to segregate groups of information services, users and information systems?			
A.9.4.7 Is the connection capability of users in shared networks restricted in line with the access control policy?			
A.9.4.8 Do shared networks have routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications?			
A.9.4.9 Has a clear description been obtained and documented of the security attributes of all network services been provided?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.4.1	
A.9.4.2	
A.9.4.3	
A.9.4.4	
A.9.4.5	
A.9.4.6	
A.9.4.7	
A.9.4.8	
A.9.4.9	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.5 Operating system access control
Objective: To prevent unauthorized computer access.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.5.1 Are terminals automatically identified to authenticate connections to specific locations and to portable equipment?			
A.9.5.2 Is access to information services via a secure logon process?			
A.9.5.3 Are users provided with a unique identifier (user ID) for their personal and sole use so that activities are traceable to individuals and has a suitable authentication technique been chosen to substantiate the claimed identity of a user?			
A.9.5.4 Are password management systems in place that provide an effective, interactive facility for the provision of quality passwords?			
A.9.5.5 Is the use of system utility programs restricted and tightly controlled?			
A.9.5.6 Are duress alarms provided for users who might be the target of coercion?			
A.9.5.7 Are there procedures and mechanisms in place to ensure that inactive terminals in high-risk locations or serving high-risk systems will shut down after a defined period of inactivity to prevent access by unauthorized persons?			
A.9.5.8 Are there restrictions on the connection times to high-risk applications to provide additional security?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.5.1	
A.9.5.2	
A.9.5.3	
A.9.5.4	
A.9.5.5	
A.9.5.6	
A.9.5.7	
A.9.5.8	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.6 Application access control
Objective: To prevent unauthorized access to information held in information systems.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.6.1 Is access to information and application system functions restricted in accordance with the access control policy?			
A.9.6.2 Do sensitive systems have a dedicated (isolated) computing environment?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.6.1	
A.9.6.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.7 Monitoring system access and use
Objective: To detect unauthorized activities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.7.1 Are audit logs produced to record exceptions and other security-relevant events and are these retained for an agreed period to assist in future investigations and access control monitoring?			
A.9.7.2 Are there procedures established for monitoring the use of information processing facilities and are the results of the monitoring activities reviewed regularly?			
A.9.7.3 Are all computer clocks synchronized for accurate recording?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.7.1	
A.9.7.2	
A.9.7.3	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.9 Access control
A.9.8 Mobile computing and teleworking
Objective: To ensure information security when using mobile computing and teleworking facilities.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.9.8.1 Is there a formal policy in place and have appropriate controls been adopted to protect against the risks of working with mobile computing facilities, especially in unprotected environments?			
A.9.8.2 Are there policies, procedures and standards in place to authorize and control teleworking activities?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.9.8.1	
A.9.8.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.10 Systems development and maintenance
A.10.1 Security requirements of systems
Objective: To ensure that security is built into information systems.

Q1. Implementation status. Tick one box.

Control requirement	Yes	Partly	No
A.10.1.1 Do business requirements for new systems or enhancements to existing systems specify the requirements for controls?			

Q2. If you have ticked either of the boxes marked **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.10.1.1	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.10 Systems development and maintenance
A.10.2 Security in application systems
Objective: To prevent loss, modification or misuse of user data in application systems.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.10.2.1 Is data input to application systems validated to ensure that it is correct and appropriate?			
A.10.2.2 Are there validation checks incorporated into systems to detect corruption of the data processed?			
A.10.2.3 Has a message authentication system been implemented where there is a security requirement to protect the integrity of the message content?			
A.10.2.4 Is data output from application system validated to ensure that the processing of stored information is correct and appropriate to the circumstances?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.10.2.1	
A.10.2.2	
A.10.2.3	
A.10.2.4	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.10 Systems development and maintenance
A.10.3 Cryptographic controls
Objective: To protect the confidentiality, authenticity or integrity of information.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.10.3.1 Is there a policy on the use of cryptographic controls for the protection of information?			
A.10.3.2 Is encryption applied to protect the confidentiality of sensitive or critical information?			
A.10.3.3 Are digital signatures applied to protect the authenticity and integrity of electronic information?			
A.10.3.4 Are non-repudiation services used to resolve disputes about occurrence or non-occurrence of events or actions?			
A.10.3.5 Is a key management system used to support the use of cryptographic techniques, based on an agreed set of standards, procedures and methods?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.10.3.1	
A.10.3.2	
A.10.3.3	
A.10.3.4	
A.10.3.5	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.10 Systems development and maintenance
A.10.4 Security of system files
Objective: To ensure that IT projects and support activities are conducted in a secure manner.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.10.4.1 Are procedures in place to control the implementation of software on operational systems?			
A.10.4.2 Is test data protected and controlled?			
A.10.4.3 Is strict control maintained over access to program source libraries?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.10.4.1	
A.10.4.2	
A.10.4.3	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.10 Systems development and maintenance
A.10.5 Security in development and support processes
Objective: To maintain the security of application system software and information.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.10.5.1 Are there strict formal change control procedures for the implementation of changes?			
A.10.5.2 Are the application systems reviewed and tested when changes occur?			
A.10.5.3 Are modifications to software packages discouraged and any essential changes strictly controlled?			
A.10.5.4 Are purchase, use and modification of software controlled and checked to protect against possible covert channels and Trojan code?			
A.10.5.5 Are controls applied to secure outsourced software development?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.10.5.1	
A.10.5.2	
A.10.5.3	
A.10.5.4	
A.10.5.5	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.11 Business continuity management
A.11.1 Aspects of business continuity management
Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures or disasters.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.11.1.1 Is there a managed process in place for developing and maintaining business continuity across the organization?			
A.11.1.2 Is there a strategy plan in place, based on risk assessment, detailing the overall approach to business continuity?			
A.11.1.3 Are plans developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes?			
A.11.1.4 Is a single framework of business continuity plans maintained to ensure that all plans are consistent and to identify priorities for testing and maintenance?			
A.11.1.5 Are business continuity plans tested regularly and maintained by regular reviews to ensure they are up to date and effective?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.11.1.1	
A.11.1.2	
A.11.1.3	
A.11.1.4	
A.11.1.5	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.12 Compliance
A.12.1 Compliance with legal requirements
Objective: To avoid breaches of any criminal and civil law, and statutory, regulatory or contractual obligations and, of any security requirements.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.12.1.1 Are all relevant statutory, regulatory and contractual requirements explicitly defined and documented for each information system?			
A.12.1.2 Are appropriate procedures implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of propriety software products?			
A.12.1.3 Are important records of the organization protected from loss, destruction and falsification?			
A.12.1.4 Are there controls applied to protect personal information in accordance with relevant legislation?			
A.12.1.5 Is there management authorization for the use of information processing facilities and are controls applied to prevent the misuse of such facilities?			
A.12.1.6 Are controls in place to ensure compliance with national agreements, laws, regulations or other instruments to control the access to or use of cryptographic controls?			
A.12.1.7 Where actions against a person or organization involves the law, either civil or criminal, does collection of evidence conform to the rules for evidence laid down by the relevant law, rules of a specific court, published standard or code of practice for the production of admissible evidence?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.12.1.1	
A.12.1.2	
A.12.1.3	
A.12.1.4	
A.12.1.5	
A.12.1.6	
A.12.1.7	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.12 Compliance
A.12.2 Review of security policy and technical compliance
Objective: To ensure compliance of systems with organizational security policies and standards.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.12.2.1 Do managers take action to ensure that all security procedures within their area of responsibility are carried out correctly? In addition, are all areas within the organization subject to regular review to ensure compliance with security policies and standards?			
A.12.2.2 Are information systems regularly checked for compliance with security implementation standards?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.12.2.1	
A.12.2.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)

BS 7799-2:2002 Information security management systems – Specification with guidance for use
A.12 Compliance
A.12.3 System audit consideration
Objective: To maximize the effectiveness, and to minimize interference to/from the system audit process.

Q1. Implementation status. Tick one box for each control requirement.

Control requirement	Yes	Partly	No
A.12.3.1 Are all audits of operational systems carefully planned and agreed to minimize the risk of disruptions to business processes?			
A.12.3.2 Is access to system audit tools protected to prevent possible misuse or compromise?			

Q2. If you have ticked any of the boxes marked either **Partly** or **No** you should indicate the reason by ticking one or more of the following boxes.

Control	Reasons and justification
A.12.3.1	
A.12.3.2	

COMMENTS: (Enter a wider explanation of the reason(s) indicated above. Where control measures are in place it may be helpful to detail them. See section 3.2 for details. Use additional sheets if necessary.)