Guide to the implementation and auditing of BS 7799 controls

BSI
Business
Information

Whilst every care has been taken in developing and compiling this Published Document, BSI accepts no liability for any loss or damage caused, arising directly or indirectly, in connection with reliance on its contents except to the extent that such liability may not be excluded by law.

Information given on the supply of services is provided for the convenience of users of this Published Document and does not constitute an endorsement by BSI of the suppliers named

Guide to the implementation and auditing of BS 7799 controls

Guidance on the implementation of ISMS control requirements to organizations preparing for certification

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

1. Introduction

This document is one of a set of guides published by DISC to support the certification process according to BS 7799 Part 2:2002 Information security management systems, - specification with guidance for use. This document is one of a set of five guides published by DISC to support the use and application of ISO/IEC 17799: 2000 and BS 7799 Part 2: 2002. Other guides are:

- *Preparing for BS 7799 Part 2 certification (PD 3001) - Guidance on implementation of ISMS process requirements to organizations preparing for certification*
- *Guide to BS 7799 Risk Assessment (PD 3002)*
- *Are you ready for a BS 7799 Part 2 Audit? (PD 3003) - A compliance assessment workbook*
- *Guide on the selection of BS 7799 Part 2 controls (PD 3005)*

This guide is intended primarily for use by those within an organization responsible for implementing security, e.g. an information security officer, and those with the task to assess existing implementations of BS 7799 controls, e.g. for compliance checking or internal audit. It will be of use to developers when setting up information security management systems (ISMS) and internal auditors when conducting their assessments.

1.1 Scope of this guide

The scope of this guide is to provide guidance on the implementation of ISMS control requirements and help for auditing existing control implementations to help organizations preparing for certification on accordance with BS 7799-2:2002 - Information security management systems – specification with guidance for use.

The contents of this guide include the ISMS control requirements that should be addressed by organizations considering certification according to BS 7799 Part 2: 2002. To this end, this guide considers in Section 2 each of the controls in BS 7799 Part 2:2002 in two different aspects:

- **Implementation guidance:** describing what needs to be considered to fulfil the control requirements when implementing the controls from BS 7799 Part 2:2002, Annex A. This guidance is aligned with ISO/IEC 17799:2000, which gives advice of the implementation of the BS 7799 Part 2 controls.
- **Auditing guidance:** describing what should be checked when examining the implementation of BS 7799 Part 2 controls to ensure that the implementation covers the essential ISMS control requirements.

It is important to emphasise that this guide does not cover the implementation or auditing of the ISMS process requirements that are covered in PD 3001. This is also discussed in more detail in section 1.3, ‘Meeting BS 7799 Part 2 requirements’ below.

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 should therefore ensure that the correct version is being used for compliance checks related to pre-certification, certification and post-certification purposes.

1.3 Meeting BS 7799 Part 2 requirements

There are two different types of requirements stated in BS 7799-2:2002:

- The requirements contained in the ISMS process, that are described in Sections 4 – 7 of BS 7799-2:2002.
- The ISMS control requirements, contained in Annex A of BS 7799-2:2002.

The ISMS process requirements address how an organization should establish and maintain their ISMS, based on the Plan–Do–Check–Act (PDCA) model. An organization that wants to achieve BS 7799-2 certification needs to comply with all these requirements, exclusions are not acceptable. The guide PD 3001 *Preparing for BS 7799 Certification* provides guidance on the PDCA model and the ISMS process requirements, certification process and preparing for certification. An organization can also check whether they have implemented all of the ISMS process requirements by using the checklists provided by guide PD 3003 *Are you ready for a BS 7799 Part 2 Audit?*

The ISMS control requirements stated in Annex A of BS 7799 Part 2:2002 are applicable for an organization unless the risk assessment and the risk acceptance criteria prove that this is not the case. This is stated in BS 77799 Part 2: "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."

Guide PD 3002 *Guide to BS 7799 Risk Assessment* provides further advice on how to carry out a risk assessment and how to define appropriate risk acceptance criteria. A review of the ISMS control requirements in place could be carried out using the guide PD 3003 *Are you ready for a BS 7799 Part 2 Audit?*

2. Implementing and auditing BS 7799 Part 2 control objectives and controls

In this section each of the control objectives and controls requirements identified in Annex A of BS 7799 Part 2: 2002 as requirements of the certification scheme are discussed from an implementation and assessment viewpoint. This takes into account the implementation advice given in ISO/IEC 17799, the Code of practice for information security management. The complete control objectives from ISO/IEC 17799 are included in this document to clarify the requirements.

2.1 Security Policy (BS 7799-2 cl. A.3)

2.1.1 Information security policy (BS 7799-2 cl. A.3.1)

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

ISO/IEC 17799 extension: Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

2.1.1.1 Information security policy document (BS 7799-2 – cl. A.3.1.1)

A POLICY DOCUMENT SHALL BE APPROVED BY MANAGEMENT, PUBLISHED AND COMMUNICATED, AS APPROPRIATE, TO ALL EMPLOYEES.

Implementation guidance:
Guidance on what an information security policy should contain can be found in ISO/IEC 17799, Clause 3.1.1. Organizational policies should be simple and to the point. In most cases, it might not be appropriate to combine every level of policy into one document. Indeed, the top level policy, the Security Policy Statement, should normally be capable of expression within a single piece of paper. The statement should be distributed to all staff. The appropriate lower level policy should be available to staff as needed and classified accordingly. It may be contained within a Security Policy Manual.

The signed copy of the policy, which should be subject to version control, should be filed for the record. Copies should be sent to all those with major responsibilities for information security (such as holders of the Security Policy Manual) and available to anyone else on request. The full version of the policy may need to be classified.

Where a short version of the policy is considered appropriate, it should be sent, complete with signature, to all staff and those others regularly working on the organization's premises. This version should be unclassified.

Auditing guidance:
This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- a definition of information security,
- reasons why information security is important to the organization, and its goals and principles,
- a brief explanation of the security policies, principles, standards and compliance requirements,

- definition of all relevant information security responsibilities (see also 2.2.1.2 below),
- reference to supporting documentation.

The auditor should ensure that the policy is readily accessible to all employees and that all employees are aware of its existence and understand its contents. The policy may be a stand-alone statement or part of more extensive documentation (e.g. a security policy manual) that defines how the information security policy is implemented in the organization. In general, most if not all employees covered by the ISMS scope will have some responsibilities for information security, and auditors should review any declarations to the contrary with care.
The auditor should also ensure that the policy has an owner who is responsible for its maintenance (see also 2.1.1.2 below) and that it is updated responding to any changes affecting the basis of the original risk assessment.

2.1.1.2 Review and evaluation (BS 7799-2 – cl. A.3.1.2)

THE POLICY SHALL BE REVIEWED REGULARLY, AND IN CASE OF INFLUENCING CHANGE, TO ENSURE IT REMAINS APPROPRIATE.

Implementation guidance:
This control forms an important part of the continuous maintenance and updating of the ISMS that is also addressed in the Plan-Do-Check-Act process described in BS 7799 Part2. This maintenance process should be responsive to all security relevant changes related to the ISMS. Scheduled periodic reviews are essential to keeping the information security policy document current and that it accurately reflects how the organization is managing its risks.

Auditing guidance:
This control is necessary to ensure that the information security policy is current and effective. This policy plays an important role in the establishment and maintenance of an ISMS. Auditors should ensure that the organization has developed procedures to react to any incidents, new vulnerabilities or threats, changes in technology, or anything else that is related to the ISMS, which might make a review of the policy necessary. In addition, there should be scheduled periodic reviews to ensure that the policy remains appropriate and is cost-effective to implement in relation to the protection achieved. The auditor should ensure that the time schedule for such reviews is appropriate for the overall risk situation. Auditors should also check the organization's plans for distributing updated policies and that all employees are made aware of the changes.

2.2 Organizational security (BS 7799-2 - cl. A.4.)

2.2.1 Information security infrastructure (BS 7799-2 - cl. A.4.1)

Objective: To manage information security within the organization.

ISO/IEC 17799 extension: A management framework should be established to initiate and control the implementation of information security within the organization.
Suitable management fora with management leadership should be established to approve the information security policy, assign security roles and co-ordinate the implementation of security across the organization. If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when dealing with

security incidents. A multi-disciplinary approach to information security should be encouraged, e.g. involving the co-operation and collaboration of managers, users, administrators, application designers, auditors and security staff, and specialist skills in areas such as insurance and risk management.

2.2.1.1 Management information security forum and information security co-ordination (BS 7799-2 - cl. A.4.1.1 & A.4.1.2)

A MANAGEMENT FORUM TO ENSURE THAT THERE IS CLEAR DIRECTION AND VISIBLE MANAGEMENT SUPPORT FOR SECURITY INITIATIVES SHALL BE IN PLACE. THE MANAGEMENT FORUM SHALL PROMOTE SECURITY THROUGH APPROPRIATE COMMITMENT AND ADEQUATE RESOURCING.

IN LARGE ORGANIZATIONS, A CROSS-FUNCTIONAL FORUM OF MANAGEMENT REPRESENTATIVES FROM RELEVANT PARTS OF THE ORGANIZATION SHALL BE USED TO CO-ORDINATE THE IMPLEMENTATION OF INFORMATION SECURITY CONTROLS.

Implementation guidance:

A typical management information security forum would consist of key members of the organization management team including the security manager and his direct manager (often the IT manager or director). The chief executive would be chairman. Their duties are outlined in ISO/IEC 17799:2000 Clause 4.1.1.

The number of meetings should be appropriate to the security requirements of the organization. In smaller organizations the subject of the forum could be built into the agenda of a management meeting.

Where appropriate to the size of the organization, a cross-functional forum of management representatives from relevant parts of the organization shall be used to co-ordinate the implementation of information security controls. This is necessary to develop all round awareness and co-ordination of security activity across function, divisions and locations, and a cross-functional forum is a useful way to do this.

The cross-functional forum will be particularly valuable in promoting security awareness through their departments and may well get involved with the planning and implementation of an organization wide awareness programme. The typical activities of a forum are described in ISO/IEC 17799:2000 Clause 4.1.2.

All activities of the forum should be documented, including the material presented and the decisions made. The justifications for decisions should also be recorded. Actions should be formally tracked and reported.

Auditing guidance:

This is the required mechanism for ensuring the security needs of the organization are identified, adequately addressed and continuously reviewed. It would be expected that this is the body, which establishes and manages the ISMS, as described in Section 3.1 above. The forum should have the appropriate degree of authority, so auditors should check that it is chaired or at least attended by the person responsible for information security (which might be the ‘information security manager’, see also 2.2.1.2 below). Minutes of meetings should be formally recorded; similarly any actions raised should be tracked by a defined process. A pragmatic approach to forum activities needs to be taken; a small organization may be able to justify combining the information security forum with other activities, but if this is the case it should be assured that information security is always adequately addressed and that the minutes clearly identify security related issues.

Large organizations and those with high information security requirements should establish a separate security forum. The auditor will need to determine that the frequency of meetings and other activities such as reviews are appropriate. The size and the attendants of the forum should be appropriate for the organization. In a small organization, for example, it could be the managing director and security manager only, for larger concerns a committee covering each department and including senior managers and security staff would be more appropriate. The auditor should judge each situation as to the needs of the organization and declared ISMS scope. Given the rate of technological advances, an organization using information processing facilities is likely to need to review security operations at least six monthly.

2.2.1.2 Allocation of information security responsibilities (BS 7799-2- cl. A.4.1.3)

RESPONSIBILITIES FOR THE PROTECTION OF INDIVIDUAL ASSETS AND FOR CARRYING OUT SPECIFIC SECURITY PROCESSES SHALL BE CLEARLY DEFINED.

Implementation guidance:
Responsibility for the protection of individual assets and for carrying out specific security processes should be clearly defined and documented. This is not a trivial task and can encompass, to some extent, every employee. It is fundamental that management and staff should be told what is expected of them and especially where information security is not generally likely to be their first interest. In general all staff should have a basic responsibility for security noted in their job description. Where more specific activities form part of the job these may be separately specified.

Auditing guidance:
Auditors should ensure that responsibilities at all levels are defined and this should be backed up by some evidence that the personnel concerned have acknowledged and accepted these responsibilities. The security policy and or the risk treatment plan is normally used to define the higher level responsibilities and reporting structure but the explicit detail of information security responsibilities would normally be contained in job descriptions or some other format based on the individual. It should be possible to identify an owner for any asset who has responsibility for its security. Auditors should check that somebody with overall responsibility for information security has been appointed (e.g. an information security manager), and that all owners are aware of their information security responsibilities. Auditors should also ensure that all documentation of this nature is current and properly controlled.

2.2.1.3 Authorization process for information processing facilities (BS 7799-2- cl. A.4.1.4)

A MANAGEMENT AUTHORIZATION PROCESS FOR NEW INFORMATION PROCESSING FACILITIES SHALL BE ESTABLISHED.

Implementation guidance:
Equipment needs to be chosen carefully to ensure that it will meet security and control requirements. The organization is vulnerable to loss of security where unsuitable equipment is selected, or the security facilities provided by the supplier fail to meet requirements.
Technical approval is important to ensure that new equipment is of an approved device type. Business unit approval should be obtained to ensure that the facility is being obtained to satisfy a business need. The security manager's approval is required as confirmation that the facility fits into the security environment and complies with security policies and controls. Approvals and authorization should be documented.

Auditing guidance:
It is essential that the integrity of security controls is maintained and hence additions or changes to information processing facilities should be properly controlled with the necessary management approval and authorisation. Procedures for this should be defined and implemented, and supporting documentation should be available. Auditors should ensure new installations, upgrades, re-configurations or any similar work being done on the security infrastructure is approved at the appropriate level, is technically validated, configuration managed and otherwise fully documented. The introduction of any new facilities by personnel and its use for business purposes should be explicitly authorised.

2.2.1.4 Specialist information security advice (BS 7799-2- cl. A.4.1.5)

SPECIALIST ADVICE ON INFORMATION SECURITY SHALL BE SOUGHT FROM EITHER INTERNAL OR EXTERNAL ADVISORS AND COORDINATED THROUGHOUT THE ORGANIZATION.

Implementation guidance:
Some aspects of security can be complex and difficult for the layman and the expert alike. The subject has become very broad and has developed sub-specialities of many kinds in areas such as communications, viruses, operating systems and databases. Security managers should understand the need to ask for specialist advice and learn to recognize where they need it. Selection of external advisors for specific aspects of security should be part of project action and expenditure plans and be appropriately approved. Internally, advice may well be available from technical specialist who also understands the security aspects of their equipment. External advice is available from many sources including books, specialist publications (periodicals), IT organizations and consultancies, suppliers of security products.

Auditing guidance:
It is up to the organization to determine whether and what advice is to be sought – it might be appropriate to establish an in-house point of contact of information security knowledge, or to use consistent and qualified external bodies such as consultants or recognised experts - in some cases a combination of several sources might be appropriate. In all cases there should be a clear link to the activities of the security forum. The auditor should determine what advice is provided, is it appropriate, is it qualified and are there any areas where advice is clearly required and has not been sought. Again, necessary levels of authorisation - for access to security controls - needs to be applied, together with vendor control, if appropriate. It is advisable to look at the reporting of security incidents: have the appointed specialists been involved in evaluating the causes, have the recommended corrective actions been taken? In a small organization the designated information security manager (or equivalent) may be the sole source of security expertise. Auditors should ensure that this is sufficient for the security requirements in place that notice of security and technological changes is made and that external advice is taken when necessary.

2.2.1.5 Co-operation between organizations (BS 7799-2 - cl. A.4.1.6)

APPROPRIATE CONTACTS WITH LAW ENFORCEMENT AUTHORITIES, REGULATORY BODIES, INFORMATION SERVICE PROVIDERS AND TELECOMMUNICATIONS OPERATORS SHALL BE MAINTAINED.

Implementation guidance:
The organization should identify and establish all appropriate liaisons to be in place with external regulatory bodies, service providers and any other organization important for information security.

In addition, good ideas can be acquired from a meeting of security managers, many of whom have long and valuable experience in the subject, as well as joining specialist groups, standards committees etc. While some involve a membership fee they will usually give you a taste of what they have to offer before you make up your mind. Other bodies don't have members as such but are useful sources of information. The Internet is an increasingly useful source of security information. Try a search on a key word or organization using one of the many search tools available.

Exchanges of security information should be controlled to ensure that confidential information is not passed to unauthorized persons. Some bodies operate on a strict non-disclosure basis to enable confidential discussion.

Auditing guidance:

This control requires appropriate liaisons to be in place with external regulatory bodies, service providers and others who may have a crucial role in either preventing security incidents or in mitigating their effects. The auditor should therefore look for the existence of the necessary contacts in contingency planning and infrastructure support. The auditor should look for evidence that legal and industry operational and technical requirements are being monitored for compliance as appropriate. The auditor should ensure that the organization knows and has documented all applicable legal requirements, and that all contacts necessary to comply with these requirements are in place.

In addition, it might be helpful for an organization to participate in best practice and knowledge of common threats being promulgated across the industry. A large organization may be involved in security specialist groups, standards committees or similar activities outside their own environment. Smaller organizations are unlikely to be able to support extensive involvement but attendance at appropriate conferences and seminars would partly address this.

2.2.1.6 Independent review of information security (BS 7799-2 - cl. A.4.1.7)

THE IMPLEMENTATION OF THE INFORMATION SECURITY POLICY SHALL BE REVIEWED INDEPENDENTLY.

Implementation guidance:

As with all business activities, security practice should be reviewed from time to time, preferably by an independent body, to provide assurance to the senior management that the organization's security practices are, indeed, adequate - hopefully those that their policy led them to expect.

'Independent' does not exclude an internal review provided that the reviewer has appropriate independence from the management and staff being reviewed. An internal audit department would be appropriate. However, a small organization may find it necessary to look for someone from outside. A certification audit, undertaken by a certified reviewer, under the scheme would also satisfy the requirements of this control.

Auditing guidance:

It is important for the auditor to check that such reviews are taking place, and that it is carried out by an independent party. Without such an independent review objectivity cannot really be achieved. A third party audit satisfies the requirement. In cases where third party audits are not being performed this requirement can be satisfied by review via internal auditors, management or other bodies external to the security practitioners. The results of other reviews, such as those described in Section 2.10.2, Reviews of security policy and technical compliance, should be taken into account.

2.2.2 Security of third party access (BS 7799 : Part 2 - cl. A.4.2)

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

ISO/IEC 17799 extension: Access to the organization's information processing facilities by third parties should be controlled. Where there is a business need for such third party access, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in a contract with the third party.
Third party access may also involve other participants. Contracts conferring third party access should include allowance for designation of other eligible participants and conditions for their access. ISO/IEC 17799 could be used as a basis for such contracts and when considering the outsourcing of information processing.

2.2.2.1 Identification of risks from third party access (BS 7799-2 - cl. A.4.2.1)

THE RISKS ASSOCIATED WITH ACCESS TO ORGANIZATIONAL INFORMATION PROCESSING FACILITIES BY THIRD PARTIES SHALL BE ASSESSED AND APPROPRIATE SECURITY CONTROLS IMPLEMENTED.

Implementation guidance:
There are several ways of how third party access can cause risks to the information security within an organization. This might be via physical access as well via logical access, e.g. using online connections. For any case of third party access, a risk assessment should be in place to determine these risks. It is important that the risks accruing through each connection are thoroughly and realistically assessed. In the same way, the risks through access by contractors etc. should be assessed. Non-technical controls such as good contract terms and regular monitoring are important ways of reducing the risk further.
Third party access to organization facilities should not be provided until a contract has been signed defining the terms for physical access and the connection and its control requirements, and the appropriate safeguards have been implemented.

Auditing guidance:
The auditor should first of all check the risk assessment the organization has made to identify the risks from third party access. Risks might result from remote access to mainframe or server software, Internet connection, and Intranets may not be as isolated as they at first appear, particularly where multiple sites are involved. Remember that the link may well be in a part of the organization declared outside of the ISMS scope. In the same way, any risks of physical third party access should be assessed. It should be considered what is being done to evaluate the security integrity of the third party, whether the controls are giving adequate protection, and how often is the risk reassessed.

2.2.2.2 Security requirements in third party contracts (BS 7799-2 - cl. A.4.2.2)

ARRANGEMENTS INVOLVING THIRD PARTY ACCESS TO ORGANIZATIONAL INFORMATION PROCESSING FACILITIES SHALL BE BASED ON A FORMAL CONTRACT CONTAINING ALL NECESSARY SECURITY REQUIREMENTS.

Implementation guidance:

The same level of security as for your own staff should be provided for third party staff, including user IDs, passwords, data access controls, and so on. However, the significant difference is that you are not in charge of their management, personnel controls, IT and security policies and practices. The other organization may also have a quite different set of ethics and business culture from those of your own organization. These differences should be identified and assessed, perhaps before deciding to do business with the other party.

The key safeguard is the contract. This should spell out in appropriate detail the controls to be exercised. It should also provide extensive details on the IT facilities that each party will make available to the other and the security controls to be put in place.

Clause 4.2.2 of ISO/IEC 17799:2002 provides an extensive list of suggested contract items that should be put in place as required by the results of the risk assessment (see 2.2.2.1 above). The contract clauses could also require compliance with BS 7799, or even certification, again depending on the requirements. Ensure that contract signatories on both sides are properly identified and authorized.

The security documentation set should include copies of all relevant contracts and, possibly several, additional documents describing specific elements of the relationship. Any deviation from these requirements should be justified and documented.

Auditing guidance:

The auditor needs to check that all security requirements for third party arrangements are identified, and addressed in a formal contract or service level agreement between the two organizations. ISO/IEC 17799, Clause 4.2.2 provides a list of issues that should be considered for inclusion in such agreements.

2.2.3 Outsourcing (BS 7799-2 - cl. A.4.3)

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

ISO/IEC 17799 extension: Outsourcing arrangements should address the risks, security controls and procedures for information systems, networks and/or desk top environments in the contract between the parties.

2.2.3.1 Security requirements in outsourcing contracts (BS 7799-2 - cl. A.4.3.1)

THE SECURITY REQUIREMENTS OF AN ORGANIZATION OUTSOURCING THE MANAGEMENT AND CONTROL OF ALL OR SOME OF ITS INFORMATION SYSTEMS, NETWORKS AND/OR DESK TOP ENVIRONMENTS SHALL BE ADDRESSED IN A CONTRACT AGREED BETWEEN THE PARTIES.

Implementation guidance:

The contract between the parties involved in the outsourcing arrangements is a key element of establishing an appropriate level of control of the organization information processing assets. The proper implementation and management of these controls is also important to support this contract. The list of suggested contract items given in Clause 4.2.2 and 4.3.1 in ISO/IEC 17799:2000 should be considered as a basis for this contract.

Depending on the business processes and operational needs of the organization requiring outsourcing these contracts may need to deal with a number of complex security questions. The various controls given in ISO/IEC 17799:2000 provide a good basis for securing outsourcing arrangements. Careful consideration should be given to such arrangements when establishing an organization's ISMS.

Auditing guidance:
Outsourcing information processing activities involves a degree of security risk since the organization loses direct control and influence of these processing activities. One way to protect against the risks of outsourcing is to have a contract in place that clearly defines the security requirements, controls and responsibilities of both parties. Auditors should ensure that a contract is in place that covers all security requirements of the organization. The exact content of such a contract should be determined with help of a risk assessment. ISO/IEC 17799 Clauses 4.2.2 and 4.3.1 contain a list of potential topics that should be considered when drafting such a contract.

2.3 Assets classification and control (BS 7799-2 - cl. A.5)

2.3.1 Accountability for assets (BS 7799-2 - cl. A.5.1)

Objective: To maintain appropriate protection of organizational assets.

ISO/IEC 17799 extension: All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

2.3.1.1 Inventory of assets (BS 7799: Part 2 - cl. A.5.1.1)

AN INVENTORY OF ALL IMPORTANT ASSETS ASSOCIATED WITH EACH INFORMATION SYSTEM SHALL BE DRAWN UP AND MAINTAINED.

Implementation guidance:
An asset inventory is a requirement of accounting standards, so for this reason as well as for security reasons all organizations should have such an inventory. Appropriate protection can only be properly applied to equipment and information if you know that the organization has them - only then can their security requirements be assessed.
The inventory of physical assets should contain full details of equipment identity including maker, model, generic type (printer, PC), serial number, date of acquisition, tag number, the name of the keeper. You should also keep a record of disposals - when and how/who to. Organizational inventory tags (logo, inventory number) should be fixed to all items that appear in the inventory. Information assets should be listed by application, perhaps as a list of database or file names. Include documentation, procedures and business recovery plans. Indicate the owner and those with operational responsibility.
List all software products, where they are used and where the original media are kept. Adequate procedures should be in place to maintain accuracy in the inventory and a stock check should be carried out at least annually.

Auditing guidance:
Organizations should maintain an accurate asset inventory. This is to include all major information, software, physical, services and processes to be protected. The assessment will

need first to determine that assets have been properly identified and classified - see also Section 2.3.2 below. The auditor needs to evaluate the inventory's adequacy; is it complete and accurate; does it contain all necessary detail, when and how is it updated? Are disposals recorded, when and to whom?

It should be checked that somebody has been given the responsibility for the asset inventory. It should also be checked how is the inventory protected. If the inventory is computer based, what about access control and back-up; if paper based, where is it kept, how is it protected against loss; and what happens when the record is replaced, are old copies kept, how long, where? The asset inventory should identify:

- the item, where applicable uniquely by serial number, date etc.,
- security classification,
- owner,
- location,
- media (if information),
- date of entry and/or audit check.

2.3.2 Information classification (BS 7799-2 - cl. A.5.2)

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

ISO/IEC 17799 extension: Information should be classified to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification system should be used to define an appropriate set of protection levels, and communicate the need for special handling measures.

2.3.2.1 Classification guidelines (BS 7799-2 - cl. A.5.2.1)

CLASSIFICATIONS AND ASSOCIATED PROTECTIVE CONTROLS FOR INFORMATION SHALL TAKE ACCOUNT OF BUSINESS NEEDS FOR SHARING OR RESTRICTING INFORMATION, AND THE BUSINESS IMPACTS ASSOCIATED WITH SUCH NEEDS.

Implementation guidance:

Information of different levels of sensitivity will require differing levels of protection and handling procedures. A method of labelling called classification should be used to identify the protection level of each item of information. The classification scheme should be in writing and available to all those with authority to apply it - all those who originate documents and data.

Each class of information requires a clear definition that will unambiguously indicate to staff when it should be used. Too many classes may lead to drift - staff forget the clear definitions and take a guess. Too few and staff will find they might need to over or under classify.

There is no standard for the classification of information. Most large organizations have a formal scheme and they vary considerably. Similar labels are used (confidential, personnel, etc.) but their meaning can be very different - often because their business needs are different. Care should be taken in interpreting classification labels on documents from other organizations, because different organizations may have different definitions for the same (or a similar sounding) label. Equally, ensure that your classifications will be properly respected when sent to other organizations.

Procedures are required specifying the handling, storage and disposal requirements of each classification. Allow also for the need to reduce the level of classification once the sensitivity has passed. Provide for change and expiry dates in these circumstances.

Auditing guidance:
Auditors should confirm that the organization has given due consideration to develop and implement adequate classification guidelines. For assets to be properly protected there should be some form of grading or classification giving due consideration to the key measures of confidentiality, integrity and availability. The classification scheme should be applied to all assets considered in the scope of the ISMS. Without a clear classification, assets may not be properly protected.

The scheme should not be too complex and should be supported by arrangements with other organizations to ensure that the possibly different classification schemes are understood. Do the procedures account for how the correct classification checked? Does a procedure to downgrade the classification level exist? Ensure that the classification scheme is readily accessible, understood by all staff and regularly reviewed. The owner of an assets should be responsible for its classification.

2.3.2.2 Information labelling and handling (BS 7799-2 - cl. A.5.2.2)

A SET OF PROCEDURES SHALL BE DEFINED FOR INFORMATION LABELLING AND HANDLING IN ACCORDANCE WITH THE CLASSIFICATION SCHEME ADOPTED BY THE ORGANIZATION.

Implementation guidance:
There is a risk of unauthorised disclosure of classified material. All information items should be prominently labelled to ensure that they are given the necessary protection in use, storage and transport. All printed items should contain the appropriate classification label (unless unclassified); unbound documents should carry it on every page.

Computer data should also be classified although it is sometimes difficult to label it. However, its classification should be maintained in the system or application documentation. This should be reflected in the system in terms of access levels and the range of users who can access it and at what level (read only, write, delete). Some security systems include a security labelling facility.

Transmitted information also requires classification. Low sensitivity information might be sent in an open email message but higher sensitivities may require encryption. The classification should be indicated in the text of the message.

Information may cease to be sensitive after a certain period of time, for example, when it has been made public. In such cases, provide an expiry date to avoid unnecessary protection expense.

Auditing guidance:
Organizations should have procedures for the labelling and handling of classified information, compatible with the classification scheme. Auditors should also ensure that the marking correctly represents the most sensitive item in the entity (e.g. an information processing system or a database).

Labelling physical items such as documents, tapes, hardware etc. is straightforward but what about information and correspondence electronically transferred? The solutions the organization have chosen for labelling electronic formats should be checked for adequacy: is this clear and understandable, does it convey the correct label to the receiver of the information and does this subsequently lead to sufficiently secure use or storage of that information? Are the labels of physical assets appropriate? Labels may be hard to find where they should be prominent; stick on labels may become detached and leave the item unmarked and unprotected.

2.4 Personnel security (BS 7799-2 - cl. A.6)

2.4.1 Security in job definition and resourcing (BS 7799-2 - cl. A.6.1)

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

ISO/IEC 17799 extension: Security responsibilities should be addressed at the recruitment stage, included in contracts, and monitored during an individual's employment. Potential recruits should be adequately screened (see 2.4.1.2), especially for sensitive jobs. All employees and third party users of information processing facilities should sign a confidentiality (non-disclosure) agreement.

2.4.1.1 Including security in job responsibilities (BS 7799-2 - cl. A.6.1.1)

SECURITY ROLES AND RESPONSIBILITIES AS LAID DOWN IN THE ORGANIZATION'S INFORMATION SECURITY POLICY SHALL BE DOCUMENTED IN JOB DEFINITIONS.

Implementation guidance:

The organization will be vulnerable to widespread insecurity if staff is not aware of security policy and expectations. Staff should have a job description that describes their normal duties and their responsibilities under the organization's security policies.

Every staff member should have a reference to security in their job description even if only to the need to uphold the policy and report suspected incidents and observed weaknesses. Those staff with substantial and complex security responsibilities should have these detailed in the job description. Job descriptions should be signed by staff, and their manager, to indicate acceptance and understanding. Staff should be given a personal copy.

Ensure that temporary and contract staff is also provided with job descriptions. There may be contract terms specifying the details of the responsibilities to be undertaken - in which case, ensure that the individual has a copy of these responsibilities.

Auditing guidance:

All employees having specific responsibilities for information security should have a job description or equivalent, which defines security roles and responsibilities. Auditors should check that this is available, signed by both the employee and appropriate manager to signify understanding and acceptance; is dated and contains correct and consistent information details relating to security functions. A check of the security responsibilities defined in policy statements and individual procedures should provide full consistency with the individual job descriptions.

Organizations might vary in where these job descriptions are held; some will be with the individual, others with personnel departments. In the latter case it should be checked that the individual has access to this information - they should have their own copy, as a person is unlikely to comply with a document last seen perhaps up to a year ago. Where individuals have jobs with specific security requirements, such as a network administrator, ensure that the job description fully reflects this, statements covering all employees are not acceptable in such cases. Similarly, out of date descriptions, e.g. if a different job is now being performed, should not be accepted.

It is particularly important that new personnel in jobs fully understand their responsibilities and the paperwork must be completed at the time of appointment, not at the next convenient

review. Auditors should pay particular attention to temporary employees and contract staff; as they might not have official job descriptions. This is not acceptable, there should be job descriptions including security for everyone working in the scope of the ISMS.
At the very minimum ensure that everybody have signed a confidentiality agreement - see below - and that contractual terms exist specifying their function. Security in job descriptions should be carefully investigated, as this can be a potential weak link in many situations.

2.4.1.2 Personnel screening and policy (BS 7799-2 - cl. A.6.1.2)

VERIFICATION CHECKS ON PERMANENT STAFF, CONTRACTORS, AND TEMPORARY STAFF SHALL BE CARRIED OUT AT THE TIME OF JOB APPLICATIONS.

Implementation guidance:
Application screening is the essential control that can prevent taking on the wrong person. Legal restraint may put a limit on the checks that one may consider. Great store has to be put into an identification check, the CV review and the character references. Where the proposed position provides access to sensitive information it is essential to get to the details of the applicant's responsibilities in previous positions and get them confirmed by previous employers. While one should beware of very cursory references remember that some organizations will not, as a matter of policy, offer any detail or opinion other than confirmation of the period employed and the last position held. Gaps in employment should be questioned. Check higher education records and professional qualifications where these are relevant.
All exchanges and interviews should be fully documented and retained on file throughout employment and for a reasonable period after it ceases, or after rejection of an application pending any possible challenge.

Auditing guidance:
The procedures for personnel recruitment (including contractors and temporary staff) should include procedures for appropriate verification checks. ISO/IEC 17799, Clause 4.1.2 lists items to be covered; in particular organizations should not rely solely on employee supplied CV's without suitable verification of the claims made. Any follow up actions, such as conversations with referees, should be documented. It should be checked that managers are aware of their responsibilities for evaluating and reviewing the work carried out in their area of responsibility, including all related security responsibilities. It should also be ensured that all information related to personnel verification checks is handled in accordance with all relevant legislation (e.g. data protection).

2.4.1.3 Confidentiality agreements (BS 7799-2 - cl. A.6.1.3)

EMPLOYEES SHALL SIGN A CONFIDENTIALITY AGREEMENT AS PART OF THEIR INITIAL TERMS AND CONDITIONS OF EMPLOYMENT.

Implementation guidance:
There is always a risk that staff may release confidential information, both during and after employment. Their responsibility to the organization should be reinforced by signing a confidentiality undertaking. Staff should always be given a copy of the agreement for their own record. This control might not stop those who remove information for payment but a signed form will provide the organization with valuable support in any court case.
While staff would normally sign such an undertaking as part of their initial conditions of employment, there may be value in some situations in repeating the exercise every few years, and prior to termination of employment, to remind staff of their commitment. Where new staff do not sign any contract until after a period of probationary employment, they

should at least sign a confidentiality undertaking before starting work. Agency staff and third party users should also be subject to this control.

Auditing guidance:
Auditors should check that all employees within the scope of the ISMS having access to any confidential assets have signed a confidentiality agreement. Whether or not it is necessary for visitors to sign such a statement (see below regarding entry controls) depends on what they will see and do. Temporary or contract staff should do the same if access to any confidential assets is granted.

As a minimum look for contractual statements of confidentiality between the organizations employing and supplying the staff, check that these individuals are aware of their obligations in this respect. Overall control of confidentiality statements needs to be handled by the personnel department so check that they have a process for this, that records are up to date, in particular that staff who have left or are about to leave have signed the necessary documentation.

2.4.1.4 Terms and conditions of employment (BS 7799-2 - cl. A.6.1.4)

THE TERMS AND CONDITIONS OF EMPLOYMENT SHALL STATE THE EMPLOYEE'S RESPONSIBILITY FOR INFORMATION SECURITY.

Implementation guidance:
It is important that employees are aware of their security and legal responsibilities regarding the handling of information and the use of information processing facilities and the consequences of not complying with security or legal requirements. This also extends to any contractual obligations that the organization has entered into and that might relate to the employee's scope of work. Any such responsibilities should be included in any terms and conditions of employment.

It is also important that employees understand that such responsibilities may extend beyond their normal working environment and working hours, as well as home working, working on customer's sites and any other form of remote working.

Auditing guidance:
Auditors should check whether the terms and conditions of employment accurately describe the employee's responsibilities for security. These descriptions should cover all security relevant aspects of the employee's job, including responsibilities applicable to legal requirements, working outside the organization or outside normal working hours, and those responsibilities that might extend beyond the employee's contract. The terms and conditions should also describe the action taken if employees do not fulfil their security responsibilities. Procedures should be in place to ensure that the terms and conditions of employment are updated if the employee's security responsibilities change in any way, e.g. taking on new roles or using new or different information processing facilities.

2.4.2 User training (BS 7799-2 - cl. A.6.2)

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

ISO/IEC 17799 extension: Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.

2.4.2.1 Information security education and training (BS 7799-2 - cl. A.6.2.1)

ALL EMPLOYEES OF THE ORGANIZATION AND, WHERE RELEVANT, THIRD PARTY USERS, SHALL RECEIVE APPROPRIATE TRAINING AND REGULAR UPDATES IN ORGANIZATIONAL POLICIES AND PROCEDURES.

Implementation guidance:

The organization is vulnerable to the activities of untrained staff. There is a risk of them producing incorrect and corrupted information or loosing it completely. Untrained staff can take wrong actions and make mistakes through ignorance.

All staff should be trained in the relevant policies and procedures, including security requirements and other business controls. They should also be trained to use all the IT products and packages required of their position as well as the relevant security procedures. Training may be required at one or two levels:

a) *security awareness*: Every member of staff should be given the basic level of security awareness training. A course should convey to them the organization's security policy, objectives and framework within which they are expected to work. Essential procedures should be provided and described. Awareness should be refreshed as necessary and through ongoing action.

b) *technical training*: Those staff with special responsibilities for security (not only security officers) should be provided with the necessary skills in formal training. A training plan should be developed for each individual according to the specific knowledge and skill required for the position held. The general development of security knowledge can benefit from attending suitable conferences.

All training, and relevant conference attendance, should be recorded in the individual's training record. Training should be available to employees, agency staff and third party users as appropriate. Ensure that training suppliers use appropriately qualified staff and that the syllabus is clear and consistent with the organization's requirements.

Auditing guidance:

This control is applicable to all employees, including users of information processing facilities such as system administrators, managers and application users, as well as senior management and those processing any form of information (e.g. paper based, telephone etc.).

The first point to note is the appropriateness of the training; this must be consistent with the job and the related security responsibilities. How is it provided, internally or externally? If internal, is it a formal course or general "on the job" type training? Who has provided the training, are they suitably qualified? If the training is informal, is there some definition of what has been covered? If the training is external, who has approved the supplier? What records exist and do they reflect the nature and depth of training given?

As a minimum organizations should have some form of induction training which is given to all employees. This will cover the general principles of security, the policy, areas of applicability etc. This should be formally recorded in individual records. In addition, it should be ensured that sufficient training for those with more complex security responsibilities is in place, and that all training material is up to date, and that the training is provided in time for the job to be carried out.

There will be situations, particularly with technical aspects, where experience or previously acquired qualifications are claimed in lieu of formal training. Auditors need to take a pragmatic approach on this and view the sum total of formal training, qualifications and experience when looking at the skills of individuals and how they fit with their roles. If previously acquired experience is claimed, make sure it is current and relevant - in what environment was it gained, has it been verified in any way. Many organizations rely too heavily at what individuals claim in CV's - an inadequately trained or experienced individual in a key position can cause major damage to vital assets, ensure the organization treat this seriously. This relates to the checks that should be made on recruitment (see 2.4.1.2 above).

2.4.3 Responding to security incidents and malfunctions (BS 7799-2 - cl. A.6.3)

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

ISO/IEC 17799 extension: Incidents affecting security should be reported through appropriate management channels as quickly as possible.
All employees and contractors should be made aware of the procedures for reporting the different types of incident (security breach, threat, weakness or malfunction) that might have an impact on the security of organizational assets. They should be required to report any observed or suspected incidents as quickly as possible to the designated point of contact. The organization should establish a formal disciplinary process for dealing with employees who commit security breaches. To be able to address incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 12.1.7).

2.4.3.1 Reporting security incidents (BS 7799-2- cl. A.6.3.1)

SECURITY INCIDENTS SHALL BE REPORTED THROUGH APPROPRIATE MANAGEMENT CHANNELS AS QUICKLY AS POSSIBLE.

Implementation guidance:
If incidents occur without being reported and responded to, they might cause more damage than necessary and it is a lost opportunity to prevent it occurring again. Failure to report also gives a false sense of security and may compromise risk assessment. Without a reporting procedure even a major incident might not find its way to those responsible for investigation and recovery until serious losses have been experienced. Minor incidents might be cleared up locally without weakness in control being recognized and corrected.
The definition of an incident is often a difficulty in practice and attention is required to ensure that all staff can recognize one when they see it. In plain terms a security incident is any event that could result in loss or damage to assets, or an action that would be in breach of the organization's security procedures. In reality one may have to specify specific incidents as reportable, e.g. virus detected on a PC or media, suspicion of misuse of a system (possible hacking), theft, password exposure, unexpected results from system monitoring, non-compliance with procedures, etc.
Any staff might be the first to notice a security problem; early notification of a problem to experienced technical staff can reduce the potential cost of an incident by having it investigated quickly. In the event of system abuse the avoidance of loss can be very significant. Build a culture of 'no blame' fault reporting - where staff is blamed for their mistakes they will be tempted to cover up the problems.
A number of incidents may already be reportable under the procedures of other departments. Failures of computer and telecommunications equipment, for instance, will be reported to engineers for repair. However, they should also be reported and recorded as security incidents (loss of information and service availability). Ensure that there are procedures covering the reporting and investigation of incident, and that progress in resulting action is monitored.

Auditing guidance:
All organizations should have appropriate procedures and management channels for reporting security incidents. Auditors should ensure that the procedures deal with all possible incidents and provide sufficient response. If an organization claims to have had no incidents to report and thus the process cannot be demonstrated, it is most likely the case that incidents took place – just nobody noticed. Therefore, incident reporting procedures should be in place independent of the incidents that have taken place in the past.

Ensure that the definition of what is and isn't a security incident is clearly described and that staff in responsible positions understand this. It could be useful to ask example questions such as "would you consider finding an unattended security safe open a security incident?", "if somebody reported receiving somebody else's salary slip, would that be considered a security incident?". Obviously such questions need to be applicable in the environment concerned, but answers from staff can be quite revealing and indicate the general approach to such matters. Where reports are present, check how the reaction to this incident was – has it been settled, have the reasons been investigated, and has the person providing the original report been informed about the outcome (if this is not confidential)?

2.4.3.2 Reporting security weaknesses (BS 7799-2- cl. A.6.3.2)

USERS OF INFORMATION SERVICES SHALL BE REQUIRED TO NOTE AND REPORT ANY OBSERVED OR SUSPECTED SECURITY WEAKNESSES IN, OR THREATS TO, SYSTEMS OR SERVICES.

Implementation guidance:
Any organization will always be vulnerable to the exploitation of unrecognised security weaknesses. No system can be 100% secure. Because of their knowledge of how the security controls, systems and software work, many IT staff are in a very good position to recognize weaknesses in security. They should be encouraged to report their suspicions to allow proper investigation and correction if necessary.

Procedures should require users to note and report any observed or suspected security weaknesses in, or threats to, security controls, systems or services. Users should report these matters either to their line management or directly to their service provider, as quickly as possible where they should be recorded and investigated. They should be aware that they should not try to exploit the identified weakness(es) in any way.

Auditing guidance:
Similar reporting procedures, as those for incidents should be in place for suspected or real security weaknesses. It is important that all employees are aware of the importance or reporting security weaknesses, and that this includes any weaknesses, not just those related to information processing facilities – an open window might also be a security weakness. The procedures for reporting should also include regulations for the employees to not use security weaknesses, e.g. to gain unauthorised access – even if the original intent is just to prove the weakness, this might cause serious damage.

2.4.3.3 Reporting software malfunctions (BS 7799-2- cl.A.6.3.3)

PROCEDURES SHALL BE ESTABLISHED FOR REPORTING SOFTWARE MALFUNCTIONS.

Implementation guidance:
The organization is always vulnerable to the effects of malfunctioning and malicious software. The most common malicious problem of this type is malicious software. Catching malicious software early can avoid huge recovery costs and prevent server systems from going out of service for, possibly, hours.

Faults in perfectly genuine software can also cause serious malfunctions that may require skilled support to recover from. Especially integrity and availability of files may be damaged by such faults and a recovery from back up may result in the loss of recent work. Users will normally be the first to recognize that something is wrong and they should follow formal reporting procedures so that timely investigative and corrective action can be taken.

Auditing guidance:

This may be covered under similar processes as incidents and potential weaknesses described above, but it should be ensured that the reporting format prompts the user to state the symptoms of the problem and any screen messages to help investigation. The reporting procedures (like those for incidents and malfunctions) should ensure that the malfunctions are reported, as minor irritants for some users could be major security issues for others.

Timeliness of this reporting is vital, for example, the early reporting of a potential software virus may prevent untold damage being done. Auditors should look carefully at the corrective actions, maybe the software can be corrected, other times a correction will have to await a new release and a workaround may be needed - is this effective, do other procedures need to be modified to account for this, how is the situation promulgated to those who need to be aware? Are temporary changes of this type properly authorised? If an external body needs to be involved, for example the supplier of the software, how is this information conveyed, ensure that this in itself causes no security breaches.

Reporting of security incident, weakness and malfunctions are reported to a point of contact in the organization: check that this is the most appropriate contact point, and that sufficient knowledge and availability is ensured. Is the necessary attention and priority given, are escalation procedures apparent, and do the persons reporting get feedback?

2.4.3.4 Learning from incidents (BS 7799-2 - cl. A.6.3.4)

MECHANISMS SHALL BE IN PLACE TO ENABLE THE TYPES, VOLUMES AND COSTS OF INCIDENTS AND MALFUNCTIONS TO BE QUANTIFIED AND MONITORED.

Implementation guidance:

In addition to detecting and taking action to resolve incidents, it is important that the organization (and the relevant people within the organization) learns from the incident to avoid future problems or if they do occur again they can be dealt with more effectively.

Learning from incidents will also provide useful information about actions that need to be taken to enhance security and can be used in training and awareness programs.

Auditing guidance:

Auditors should review any examples of how the organization has reacted to incidents and software and system malfunctions in the past. They should review how the organization quantifies and measures incidents, and whether the incident handling procedures are appropriate for the incidents that have occurred or are likely to occur in the future.

If the organization claims that an insufficient number of incidents have occurred or insufficient information or evidence is available to be learnt from, then this should be reacted to with some caution, as this might be a sign that the incident reporting procedures are not used. The auditor should enquire, question and discuss with the organization's such a situation.

Plans and procedures to react to incidents and malfunctions should be in place. This should include the implementation of additional controls or procedures to avoid re-occurrences, to limit the damage, collect evidence, or to allow a quicker and more efficient reaction in the future. Learning from incidents also includes that use of incidents in training and awareness programmes to give real life examples.

2.4.3.5 Disciplinary process (BS 7799-2 - cl. A.6.3.5)

THE VIOLATION OF ORGANIZATIONAL SECURITY POLICIES AND PROCEDURES BY EMPLOYEES SHALL BE DEALT WITH THROUGH A FORMAL DISCIPLINARY PROCESS.

Implementation guidance:
Any non-compliance with the security policy or controls by staff needs to be properly dealt with or there will be a decline in standards and an increase in insecurity. The disciplinary process will be influenced by the organization's culture and personnel management practices but it should be documented and staff should be aware of the details.

Auditing guidance:
This might be a sensitive issue in organizations, but it is important that such a process is in place to be able to properly react to any security breaches. Employees should be made aware of the disciplinary process, and that it provides fair treatment to all involved. If the disciplinary process is not implemented correctly the organization might be liable to potential claims for unfair dismissal or other personal infringements. A disciplinary process should be defined and without it's deterrent, management effectiveness may well be compromised. Auditors should check with recorded security incidents, look at the criteria for disciplinary action and verify that such procedures are being effectively employed.

2.5 Physical and environmental security (BS 7799-2 - cl. A.7)

2.5.1 Secure areas (BS 7799-2 - cl. A.7.1)

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

ISO/IEC 17799 extension: Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference. The protection provided should be commensurate with the identified risks. A clear desk and clear screen policy is recommended to reduce the risk of unauthorized access or damage to papers, media and information processing facilities.

2.5.1.1 Physical security perimeter (BS 7799-2 – cl. A.7.1.1)

ORGANIZATIONS SHALL USE SECURITY PERIMETERS TO PROTECT AREAS WHICH CONTAIN INFORMATION PROCESSING FACILITIES.

Implementation guidance:
Premises that contain business processes, information, services, IT and other assets are vulnerable to the undesirable activities of people. Some of those people may also work for the organization, so internal protection is required as well as external.

Small premises may be a single domain with an obvious perimeter. Larger premises may need to use several perimeters to be divided into several domains. It is important to properly define the perimeter of each domain.

The objective is to be able to control entry into (and possible exit from) every domain, and additionally to record entry and exit from sensitive areas. A security model can be prepared showing, perhaps schematically, the various domains and the access points between them. A risk assessment should be used to define appropriate perimeters and to select controls to give adequate protection.

Procedures should be provided regarding the management of physical security, access control and it's monitoring. Give due consideration to out of hours working and any necessary authorization, supervision and monitoring. Clause 7.1.1 in ISO/IEC 17799 contains a list of guidelines and controls.

Auditing guidance:

All organizations should be able to demonstrate physical protection of their assets. Where major installations are involved, security procedures should describe what measures are taken, how this is monitored and who has access. The assess the physical protection in place, auditors will need to look for potential breaches: open fire escapes, unattended reception areas, sharing of security passes, unlocked cabinets are all potential security threats and should be noted.

A part of the physical protection in place is the use of physical perimeters, so the organization should be able to explain what perimeters are in place, and what protection is achieved with them (this should be supported by a risk assessment). Auditors should also check how the access into the building is controlled and monitored, and whether the controls in place are sufficient for the needs of the organization, or whether there are possibilities to circumvent the protection.

2.5.1.2 Physical entry controls (BS 7799-2 - cl A.7.1.2)

SECURE AREAS SHALL BE PROTECTED BY APPROPRIATE ENTRY CONTROLS TO ENSURE THAT ONLY AUTHORIZED PERSONNEL ARE ALLOWED ACCESS.

Implementation guidance:

A secure area in this context is any area that the organization identifies, by use of a risk assessment, to require access control. Such areas may include the entire premises but certainly computer rooms, telecommunications rooms and closets, and plant rooms (power, air conditioning). A clerical area handling sensitive data such as tele-sales, customer service or banking, may also fall into this category. Different areas will possibly need different levels of security and access control.

The threats include breaches of confidentiality, unauthorized tampering with or theft of equipment (loss of integrity or availability).

Appropriate entry controls may extend from a check of organization ID cards to an electronic check of personal identity including the entry of a password or PIN (Personal Identity Number). It should be ensured that all people accessing secure areas are appropriately checked and that badges are used to identify authorised people. Specific controls are listed in ISO/IEC 17799, Clause 7.1.2

Auditing guidance:

Auditors should check the entry controls in place and ensure that these are sufficient to restrict physical access to authorised people only. Do employees wear badges and is this mandatory? What about visitors, are badges issued, is their entry and exit logged, what restrictions are placed on their movements? Are persons not wearing badges challenged? Auditors, invariably being visitors to the organization, can determine this from their own treatment.

Auditors should also check the audit trails of the access that has taken place in the past, and ensure that procedures for the review and update of the physical access rights are in place. Authorisation in terms of access rights and restrictions may be in a variety of forms: they could be described in job descriptions, they could be written into procedures or they could be listed at the point where the restrictions apply, such as a label affixed to a door for example. Auditors should take a view on the appropriateness of each approach.

2.5.1.3 Securing offices, rooms and facilities (BS 7799-2 - cl. A.7.1.3)

SECURE AREAS SHALL BE CREATED IN ORDER TO PROTECT OFFICES, ROOMS AND FACILITIES WITH SPECIAL SECURITY REQUIREMENTS.

Implementation guidance:

Areas supporting critical business activities such as data centres (the whole premises), computer suites and telecommunications rooms, should be identified by risk assessment. These areas should be accessed only by authorized persons. Entry and exit should be recorded and entry authority should be confirmed at each entry by use of an access control system.

The risk of loss of confidentiality, integrity and availability all increase as more of the organization's key data, are located in one place. This very soon marks out the premises as critical to the organization. Especially strong security is required, outside and inside, to ensure that losses are not experienced.

The selection and design of the site should take account of the possibility of damage from fire, flooding, explosions, civil unrest, and other forms of natural or man-made disaster. Consideration should be given also to any threats presented by neighbouring accommodation.

A long list of important controls to consider are listed in ISO/IEC 17799, Clause 7.1.3. The selection of all these controls should be documented as previously described and the necessary training should be recorded in staff training records.

Auditing guidance:

The level of protection provided for a secure area needs to be compatible with the most sensitive information held in this area, in line with the procedures for the handling of classified information. There is a clear link here to risk assessment and auditors should verify that the information security requirements have been identified and that the protection in place is adequate for this.

A list of security controls that might be applicable to protect secure areas is given in ISO/IEC 17799, Clause 7.1.3. As well as access control, auditors should investigate other security and availability aspects such as power supplies, emergency support, environmental protection - is there a fire hazard, could the installation be flooded - what is there to prevent or mitigate these dangers? See also sections 2.5.2.1 Equipment siting and protection and 2.5.2.2 Power supplies below.

2.5.1.4 Working in secure areas (BS 7799-2 - cl.A.7.1.4)

ADDITIONAL CONTROLS AND GUIDELINES FOR WORKING IN SECURE AREAS SHALL BE USED TO ENHANCE THE SECURITY OF SECURE AREAS.

Implementation guidance:

In addition to enhancing the security of the physical perimeter using entry controls and securing offices, rooms and facilities for day to day operations, the specific security requirements of areas involving sensitive work need to be considered.

For example, an organization could be working on a new product the design of which has high commercial value and is ahead of its competitors. Another example might involve similar circumstances where an organization has a project or process that is sensitive and needs to be protected from damage, loss, modification or disclosure.

Therefore, the work in secure areas should be protected and supervised as described in ISO/IEC 17799, Clause 7.1.4.

Auditing guidance:
Personnel working in secure areas should be subject to specific controls that ensure sufficient security is implemented for the sensitive and critical information that is processed in such areas. Auditors should review:

- the entry controls in place to ensure that only authorized personnel has access to such areas;
- to what extent the work going on in such areas is generally known and whether this exceeds any rules on 'need to know';
- how easy or difficult it is to take information (e.g. in form of paper or discs) in or out of such areas;
- whether it is possible to take photographic, video, audio or any other recording equipment inside such areas and to use or leave such equipment there to record;
- whether the work in such areas is sufficiently supervised and that mechanisms are in place to ensure that dual controls are is applied where appropriate.

2.5.1.5 Isolated delivery and loading areas (BS 7799-2 - cl. A.7.1.5)

DELIVERY AND LOADING AREAS SHALL BE CONTROLLED, AND WHERE POSSIBLE, ISOLATED FROM INFORMATION PROCESSING FACILITIES TO AVOID UNAUTHORIZED ACCESS.

Implementation guidance:
Breaches of confidentiality, integrity and availability can all be suffered through uncontrolled delivery and despatch. There are threats from unauthorised access, malicious delivery (e.g. letter bomb), and unauthorized despatch, which frequently involve theft.

A busy organization will experience a lot of deliveries and collections. No one will be surprised to see packages being delivered or collected by strangers (delivery staff). It is therefore essential to control this activity to ensure that deliveries are expected items and collections are of only properly authorized despatches, and that delivery staff are properly controlled with respect to access.

In order to control these problems, a segregated area is recommended, which isolates delivery and loading from the most secure areas. Internal procedures should be used to ensure that the transfer of goods between loading bay and secure area is controlled. Full records of all deliveries and despatches should be kept. The names of all delivery drivers and vehicle numbers should be recorded.

Auditing guidance:
This control is to help prevent security incidents by delivery and loading operations. Deliveries may involve outside personnel on the premises and their movements need to be restricted. Products received could cause a hazard if not properly inspected, tested or stored as appropriate. Items leaving the premises could inadvertently contain sensitive information.

All these risk areas, where applicable, should be identified by the risk assessment and security procedures and adequate measures taken to both prevent and mitigate the potential security breaches. For example, how are goods received: by the person requiring the goods, a stores employee, and a general receptionist? What happens to the goods after receipt: are they sent directly into the secure area, are they held in some store, are they left on someone’s desk?

2.5.2 Equipment security (BS 7799-2 - cl. A.7.2)

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

ISO/IEC 17799 extension: Equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

2.5.2.1 Equipment siting and protection (BS 7799-2 - cl. A.7.2.1)

EQUIPMENT SHALL BE SITED OR PROTECTED TO REDUCE THE RISKS FROM ENVIRONMENTAL THREATS AND HAZARDS, AND OPPORTUNITIES FOR UNAUTHORIZED ACCESS.

Implementation guidance:

Equipment at the work point can be vulnerable to damage and interference with a resultant loss of integrity and availability. Accessibility can lead to unauthorized use and breach of confidentiality of the information displayed.

Physical damage can arise from poor environmental conditions particularly in industrial situations where moisture, dust and chemicals can all take their toll. Electrical and electromagnetic interference can be significant in some environments and need to be tested for. It is relatively easy to protect equipment such as communications devices and connection panels - simply lock them in an appropriate small room or equipment cupboard. Equipment required by operating staff needs to be available in their workspace and rugged versions should be considered. Ensure that the risk assessment covers this kind of situation.

Where networked equipment is considered, remember that remote equipment probably requires more security attention than in house equipment. Clearly establish the bounds of the organization's network responsibilities and apply appropriate protection at the boundaries. Ensure that remote equipment is accounted for in inventories, security scope and risk assessments.

Auditing guidance:

Organizations need to demonstrate how their equipment is protected. Equipment should be sited away from potential risk areas such as windows that could be easily broken during a burglary without setting off an alarm. Consider also that terminal screens may be viewed from outside the protected area.

In some environments it may be appropriate to secure computer equipment to desks. As well as malicious damage, equipment needs to be protected from accidental damage from a very untidy or poorly managed environment, unrestricted access, unstable racks, spilt coffee etc., and from environmental hazards such as water, chemicals and fire. Check that such measures have been considered and that adequate protection is implemented.

Look beyond the immediate computer area, does a fire or water hazard exist in adjacent areas? A large organization will probably have a site layout plan, look for this, and see how it was developed.

2.5.2.2 Power supplies (BS 7799-2 - cl. A.7.2.2)

EQUIPMENT SHALL BE PROTECTED FROM POWER FAILURES AND OTHER ELECTRICAL ANOMALIES.

Implementation guidance:
Electricity supply is an essential prerequisite to ensure business continuity and to the use of any computing and communications equipment. While we tend to take a reliable public supply for granted, we are always at risk of a break resulting from 'high winds over the Pennines' or the activities of someone with a digger. No electricity, no availability.

The risk assessment should highlight those facilities that require electrical back up - especially for computer services supporting critical business operations. The selected back-up, such as an uninterruptible power supply (UPS) or generator, should be capable of sustaining sufficient power for the maximum potential period of power cut, or at least for the time identified in the business continuity plans.

Some equipment requires a very clean power supply, free of peaks and troughs (spikes). If not smoothed, this problem can lead to a loss of availability through damage or failure.

Auditing guidance:
The necessary level of protection provided from power failure or disturbances depends on the security requirements and the criticality of the equipment and the information held on the system (e.g. high availability requirements should yield strong controls to ensure sufficient power supplies). Auditors should check in any case that at least minimal protection in the form of power line surge suppression is provided.

For higher requirements, check that sufficient back-up facilities such as standby generators, UPS units, redundant disk (RAID) units, etc. are in place. If this is the case, look closer at the power supply support – does it have sufficient capacity - what is the extended operating period - does it match the contractual obligations – is it maintained and tested in accordance with manufacturer's recommendations? The auditor should also check that emergency lighting is provided in case of a power failure.

2.5.2.3 Cabling security (BS 7799-2 - cl. A.7.2.3)

POWER AND TELECOMMUNICATIONS CABLING CARRYING DATA OR SUPPORTING INFORMATION SERVICES SHALL BE PROTECTED FROM INTERCEPTION OR DAMAGE.

Implementation guidance:
Unless properly installed, it can be very easy to damage the cables and especially their connectors, leading to a loss of availability and a sometimes difficult to find fault. Cables left on floors and hanging loose around walls are a safety hazard and will suffer excessive ware or pulling leading to damage.

In sensitive businesses the communications cables may be at risk of interception and loss of confidentiality in which case they need to be protected by conduits with all connections made in locked equipment rooms or boxes. While physical protection will be the principle safeguard to consider, there are also data transmission controls such as encryption that can be employed in the most sensitive places. The risk assessment should highlight these cases.

Public access to roadside telecommunications junction boxes may also pose a risk in some places, both from physical damage and tampering. Discuss this with your network service provider with a view, perhaps, to relocating the box underground beneath a secure lid.

Auditing guidance:
The general condition of interconnecting plugs and cables should be checked: are they correctly fitted and properly routed, or are they badly put together and placed where they

could be damaged or cause an accident? ISO/IEC 17799 clause 7.3.2 provides a list of controls that should be applied for power and telecommunication cables.
Routing of communications links could be critical for some users. Auditors should establish what the communication risks are and look for potential weak points - network cabling routed between departments or buildings, telephone cabling accessible to interruption or eavesdropping.

2.5.2.4 Equipment maintenance (BS 7799-2- cl. A.7.2.4)

EQUIPMENT SHALL BE CORRECTLY MAINTAINED TO ENABLE ITS CONTINUED AVAILABILITY AND INTEGRITY.

Implementation guidance:
The reliability of computing and communication equipment can lead us into a false sense of security. The sudden failure of equipment that has worked faultlessly for years can have a profound effect on the integrity and availability of business processes and services - especially if the equipment cannot readily be replaced.
Most equipment is supplied with maintenance instructions and these need to be built into operating procedures. Ensure that maintainers are qualified, and that they are accompanied when carrying out their maintenance work. Keep records of faults and maintenance - monitoring these will help judge when equipment should be replaced and so avoid the sudden failure.

Auditing guidance:
Auditors should ensure that the organization has controls in place to ensure equipment maintenance in accordance with suppliers recommended service intervals and specifications. In addition, simple operations such as regular cleaning of air filters, tape drive mechanisms and printers can save considerable disruption. Even mundane activities such as regular disk defragmenting on computers can affect efficiency.
Look to see what maintenance activities are identified in the procedures, determine whether they are sufficient and check the records to ensure that maintenance activities in the past have taken pace as lined out in the procedures. There needs to be a formal fault reporting mechanism, check for this and logs of defects and their rectification. It should be checked that only authorised personnel can carry out maintenance activities, and that outside personnel doing maintenance is accompanied.

2.5.2.5 Security of equipment off-premises (BS 7799-2 - cl. A.7.2.5)

ANY USE OF EQUIPMENT FOR INFORMATION PROCESSING OUTSIDE AN ORGANIZATION'S PREMISES SHALL REQUIRE AUTHORIZATION BY MANAGEMENT.

Implementation guidance:
The security of equipment off-site should be subject to a risk assessment and appropriate controls should be used to ensure that it remains in place, in operation and does not provide an uncontrolled risk, e.g. through its links to central networks. The risk assessment should ensure that the security provided off site is equivalent to the security arrangements on site.
Be especially careful to identify all the risks inherent in portable equipment. They are particularly vulnerable to theft when in public places and that leads to breaches of confidentiality as well as the non-availability of the device. More about the security of mobile equipment is discussed in Section 2.7.8.1, Mobile computing.

Auditing guidance:

This control addresses the security of any equipment used away from the premises. For some organizations this will not be an issue, depending on the business carried out, but for most organizations this could be a significant area of concern. Additional protection mechanisms are also described in Section 2.7.8, where 2.7.8.1 addresses mobile computing and 2.7.8.2 the security issues related to home workers and their environment.
Use of equipment outside the secure environment of the organization yields lots of security problems and added threats. Therefore, the auditor should check that the controls provided for the physical protection of equipment outside premises give adequate security, comparable with what is achieved on-site. Procedures and guidelines should be in place to ensure that equipment off premises is not left unattended, and that, where relevant, sufficient insurance is taken.

2.5.2.6 Secure disposal or re-use of equipment (BS 7799-2 - cl. A.7.2.6)

INFORMATION SHALL BE ERASED FROM EQUIPMENT PRIOR TO DISPOSAL OR RE-USE.

Implementation guidance:
Serious breaches of confidentiality can occur when disposed of disk drives are accessed by unauthorised persons, e.g. sold on the second hand market, or when being re-used. The files may well have been deleted from the directory but the data image is still on the disk, accessible to anyone with the right tools. Copies can also be made from your registered and identifiable software, laying the organization open to charges of illegal copying and distribution of copyright material.
Therefore, the organization should use controls to ensure that any re-used or disposed of equipment does no longer contain information of any sensitivity – it is best, if this equipment is completely empty. Plenty of storage devices are relatively cheap and the organization should consider complete destruction as a method of disposal for unwanted storage devices.

Auditing guidance:
Organizations should have an effective process for ensure data is removed on equipment, which is disposed of or otherwise taken outside of their control. Auditors should check that users understand the potential dangers here and that the organization has effective means of ensure that no sensitive information is contained in equipment, which is disposed of. Erasing files from magnetic media is not secure: the information is often still accessible. Disks may need to be formatted and overwritten several times before all the original data is obliterated.
For very sensitive systems, specialist equipment may be needed to remove the magnetic signature from disks and tapes. The policy may need to extend to all media - labelling of items holding sensitive data could be removed before disposal making positive identification difficult.
Depending on the risks involved, physical destruction of diskettes and tapes may be the best option, and this should also to extend to hard disks inside computers. Some organizations may consider this a drastic step but magnetic storage is relatively cheap, much cheaper than the loss or compromising of sensitive data. Consider also items sent for repair; are there any checks to ensure that sensitive information cannot be accessed or interfered with?

2.5.3 General controls (BS 7799-2 - cl. A.7.3)

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

ISO/IEC 17799 extension: Information and information processing facilities should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage. Handling and storage procedures are considered in 8.6.3.

2.5.3.1 Clear desk and clear screen policy (BS 7799-2 - cl. A.7.3.1)

ORGANIZATIONS SHALL HAVE A CLEAR DESK AND A CLEAR SCREEN POLICY AIMED AT REDUCING THE RISKS OF UNAUTHORIZED ACCESS, LOSS OF, AND DAMAGE TO INFORMATION.

Implementation guidance:
Offices generally provide easy opportunity for other people to browse around and read documents or information on screens that were not for their eyes. Such people may be other staff or outsiders e.g. visitors, cleaners. The availability of technology means that it is a simple and quick operation to thieve a paper or copy it, returning the original without being noticed. If the access to computers is not protected, this might lead to unauthorised persons browsing through possibly sensitive information. Confidentiality is easily compromised. Theft leads to non-availability.

A disorderly desk may lead to the loss of documents due to mis-filing, or even putting them in the waste bin by mistake. The more sensitive the information the higher the risk of experiencing such losses. Information left out on desks is likely to be lost to the wind, damaged or destroyed in a disaster such as a fire, flood or explosion.

Organizations should adopt a clear desk policy for papers and computer media and a clear screen policy for information processing facilities in order to reduce these risks. Staff usually see this as an onerous control so training should emphasize the benefits of working in an organized and tidy environment, and that screen savers with passwords are used, or equipment is switched off when leaving the office. Compliance should be monitored and persistent offenders noted and disciplined.

Auditing guidance:
The objective of this control is to both ensure that sensitive information in any form (processed electronically, on paper or media, etc.) is not left unattended and also that information is not lost - and hence compromised, modified or unavailable. This needs to apply to both working and non-working hours. It also needs to apply to the appropriate classification of information, see also Section 2.3.2, Information classification.

The danger of sensitive information being accessed by outside staff, e.g. cleaning staff, should be protected against. It should also be checked what happens when desks, filing cabinets and safes are left unattended during the day - is this a problem, is security being compromised? Consider also the access to computers while staff are absent, independent of the duration of this absence; password protected screen savers, switching the computer off, or any other form of clear screen control should be applied.

Where necessary, additional logical access control as described in 2.7 Access control, should also be in place. If the whole area is covered by the appropriate level of security and all staff is appropriately cleared then additional measures may not be needed. Check that the overall policy is clear, that staff are aware of and follow the appropriate procedures.

2.5.3.2 Removal of property (BS 7799-2 - cl. A.7.3.2)

EQUIPMENT, INFORMATION OR SOFTWARE BELONGING TO THE ORGANIZATION SHALL NOT BE REMOVED WITHOUT AUTHORIZATION OF THE MANAGEMENT.

Implementation guidance:
Property removed without authorization may be in process of being stolen. This can lead to non-availability and loss of confidentiality where items contain information or software. In a

technology rich environment the risk of loss can be very high, especially among items that can be useful in the home. Consider the possibility of the unauthorized removal of information via the Internet for later retrieval at home.

Equipment, data, software and the organization's business papers, should not be taken (or transmitted) off-site without formal authorisation. It is essential that the organization should know where its assets are and who has control over them. All items of equipment should, where possible, be marked to indicate their ownership.

Those carrying items, such as portable PCs and sensitive business information (on the PC or on paper), in and out on a regular basis should be provided with authority to carry with them and to be produced on demand at any of the organization's premises.

Where items are on long term loan, for instance, to home workers, the individual should be required to endorse the inventory annually to the effect that the items are in their possession, in good condition and still necessary for their work. Procedures should be implemented to ensure that those leaving employment return all company property before departure.

The visiting staff of other organizations bringing property in should be required to log the property on entry so that they can remove it on departure without difficulty. Appropriate documentation should be kept regarding procedures, authorizations, off site inventory and returns.

Auditing guidance:

In many organizations staff may regularly be required to take equipment, data and documents away from the premises. This may be to work at home or to attend meetings at other premises. For some organizations controlling this might cause a problem. The auditor needs first to ensure the organization have identified both the problem and how to effectively control it. There are a number of options:

- Removal of any sensitive information is prohibited. On the face of it this is the simplest approach but difficult to implement for the majority of organizations. Highly restricted environments might need to use this approach.
- Removal of sensitive information is permitted under appropriate controls. The organization needs to be very clear what information is involved and what controls are needed.
- Removal of sensitive information is permitted without control. This can be very dangerous, and should not be chosen if not accompanied with additional controls regulating the handling of sensitive information outside the organization's premises.

The auditor needs to verify which policy approach is taken and then look at the documented procedures for control. Is a booking in/out system in use, what authorisation is needed and recorded; is this for all items or only a restricted range? How does management monitor compliance? A regime that is too restrictive is liable to lead to avoidance, too lax will lead to obvious breaches. Does the confidentiality agreement (see 2.4.1.3 above and ISO/IEC 17799, clause 6.1.3) cover responsibility for information held while off premises? Many employees now use notebook computers: what controls exist for these or any sensitive data held? Information held on notebook computers or diskettes could be disguised by changing the file names, are search tools needed to combat this, if so when are they employed?

Ease of communications now means that information removal off-site no longer has to use physical media, auditors should also investigate what transfer control mechanisms exist when accessing, for example, the Internet.

2.6 Communications and operations management (BS 7799-2 - cl. A.8)

2.6.1 Operational procedures and responsibilities (BS 7799-2 - cl. A.8.1)

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

ISO/IEC 17799 extension: Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures. Segregation of duties (see 8.1.4) should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

2.6.1.1 Documented operating procedures (BS 7799-2 - cl. A.8.1.1)

THE OPERATING PROCEDURES IDENTIFIED IN THE SECURITY POLICY SPECIFIED IN THE SECURITY POLICY SHALL BE DOCUMENTED AND MAINTAINED.

Implementation guidance:

As with all the controls in this section, the scale of implementation should be appropriate for the size and complexity of the particular organization. A large organization with many staff involved may require more comprehensive and detailed procedures than a small organization where a few thoroughly experienced staff covers the whole operation.

Inadequate or incorrectly documented procedures can result in system or application failures, causing loss of availability, failure of data integrity and breaches of confidentiality. Complicated or infrequently used procedures provide opportunities for mistakes and require particular care in their drafting. Operating procedures should be treated as formal documents, changes to which may only be approved by authorized persons.

Many organizations outsource the operation and management of their computers and communications to a specialist facilities management organization. One way of ensuring that appropriate security is in place is to use sufficiently detailed contracts and to check whether the other organization is BS 7799-2 compliant.

Auditing guidance:

Auditors should examine and inspect the organization's operating procedures, that these are appropriately documented and that they are being applied throughout the relevant parts of the organization. In order to be able to check these procedures for completeness, auditors need to have a general understanding of the various operational processes and workings of the organization.

In addition, the handling and management of, and compliance with, these procedures should be checked. A check should be made to ensure that it is not possible to modify the procedures without appropriate authorization, and that it is not possible to circumvent these procedures or any associated controls.

Responsibility for network services operation and administration is often a separate department or even a separate organization. The auditor therefore needs to understand the arrangement and ensure that the necessary levels of service and procedures are properly documented. In some areas detailed work instructions will be needed. There is likely to be considerable use made of suppliers documentation, so this should also be checked for relevance and availability.

2.6.1.2 Operational change control (BS 7799-2 - cl. A.8.1.2)

CHANGES TO INFORMATION PROCESSING FACILITIES AND SYSTEMS SHALL BE CONTROLLED.

Implementation guidance:
Uncontrolled changes to operational information processing facilities and systems can cause major interruptions to business processes. Changes that might cause problems include the installation of new software, changes to a business process or operational environment or introducing new connections between information processing facilities and systems.

In order to avoid interruption to business activities any changes to operational systems should only take place after formal approval has been given. The procedures for such an approval should take into account the possible effects of the changes and define what action is needed to recover from unsuccessful changes.

Care should also be taken to control the changes to applications (see also 2.8.5.1) since these changes are likely to have an impact on the operational systems in which these applications are running.

Auditing guidance:
The auditor should check that management responsibility and formal procedures are in place to control changes to operational information processing facilities. All such changes should be monitored and logs should exist describing exactly which changes have been made. It should be ensured that no changes could take place without assessing the possible damage such changes can cause and obtaining appropriate approval for the proposed change.

Procedures should be in place describing how to react if something goes wrong, and it should be ensured that no change could start without appropriate fallback procedures in place allowing going back to the original state. Auditors should ensure that the procedures also cover informing all relevant personnel if a change has taken place. If operational changes also yield changes to the applications, the changes should be integrated (see also Section 2.8.5.1, Change control procedures).

2.6.1.3 Incident management procedures (BS 7799-2 - cl. A.8.1.3)

INCIDENT MANAGEMENT RESPONSIBILITIES AND PROCEDURES SHALL BE ESTABLISHED TO ENSURE A QUICK, EFFECTIVE AND ORDERLY RESPONSE TO SECURITY INCIDENTS AND TO COLLECT INCIDENT RELATED DATA SUCH AS AUDIT TRAILS AND LOGS.

Implementation guidance:
Incidents can make us vulnerable to breaches of confidentiality, failure of integrity of equipment and data, and, most commonly, loss of availability. They are usually preventable and provide a valuable opportunity to improve our procedures and processes to prevent them occurring again. Examples include fire or flood, electrical failure, hardware breakdown, failed software, virus infection, unauthorised access (actual or attempted) to controlled premises or to computer systems, corrupted or lost data, misdirected email and failure of any security control.

That incidents are so often treated with little concern rather than with respect reflects badly on the prevailing standard of incident management. An incident often puts an increased load on those responsible for investigation and recovery, but procedures should require time to be spent on identifying the true causes of the incident and improving procedures to reduce the risk of a re-occurrence.

Procedures should be maintained to ensure that all incidents are reviewed and investigated where appropriate, that recovery procedures are triggered, and that there is appropriate review including at the management security forum. ISO/IEC 17799, Clause 8.1.3 provides a list of controls that should be applied to properly manage incidents.

Auditing guidance:
The auditor should check that incident management procedures are in place, and that they work well with the reporting scheme described in Section 2.4.3, Incident reporting. ISO/IEC 17799, Clause 8.1.3, identifies the type of incidents that need to be addressed - system failures, errors, security breaches, etc. - and the necessary contingency arrangements, auditing activities and actions to recover from incidents.

Check that all of the activities described in ISO/IEC 17799, Clause 8.1.3 are properly documented in procedures that appropriate management control is exercised and the incidents and their follow-up activities are properly recorded.

2.6.1.4 Segregation of duties (BS 7799-2 - cl. A.8.1.4)

DUTIES AND AREAS OF RESPONSIBILITY SHALL BE SEGREGATED IN ORDER TO REDUCE OPPORTUNITIES FOR UNAUTHORIZED MODIFICATION OR MISUSE OF INFORMATION OR SERVICES.

Implementation guidance:
Segregation of duties is a traditional business control used to reduce vulnerability to staff errors and misuse of all kinds. While most of the people employed in an organization are basically honest there might also be some who are not. A rather greater number will become negligent if their activities are not controlled. This can lead to problems with integrity (people as well as information), loss of confidentiality and resources unavailable for their proper purpose. Ensure that risk assessment properly identifies the risks of un-segregated activities.

Dividing the job up between two or more staff provides a check at the point of hand over where one person can see that another has done what they are supposed to do. In sensitive areas, the use of two keys or passwords by separate staff ensures that no one obtains access to a resource without a second person either authorizing or confirming an authority.

Many frauds, and accounting deceptions, are committed by people who have been given access to too many functions within an accounting system. A well-known disaster of this type was the Baring’s Bank losses, which resulted in the collapse of the entire business. Segregation prevents staff from operating on their own to create such incidents. Although the possibility of collusion remains, it is very rare that more than two will take the personal risk.

In small organisations, where segregation can be difficult to implement, the principle should be applied as far as possible with additional controls, such as increased monitoring, being implemented to compensate for any lack of segregation.

Auditing guidance:
As noted in ISO/IEC 17799, clause 8.1.4, small organizations may have difficulty in this area; this section also identifies typical roles where segregation may be necessary. For the larger set-up this principle should be an established fact and properly demonstrated in the procedures. Of those areas identified in the standard for independent operations, security administration and audit are possibly the most critical and should be considered first.

The auditor should look at what independent verification of data and results is done between processing stages or before release. As part of detailed risk analysis, the organization should have considered critical processes and whether any one person is responsible for making too many of the checks and balances. Look at work arrangements for critical tasks, how are periods of sickness or holidays covered, does this compromise independence? The organization may need to enforce mandatory holiday periods to achieve effective segregation.

2.6.1.5 Separation of development and operational facilities (BS 7799-2 - cl. A.8.1.5)

DEVELOPMENT AND TESTING FACILITIES SHALL BE SEPARATED FROM OPERATIONAL FACILITIES. RULES FOR THE MIGRATION OF SOFTWARE FROM DEVELOPMENT TO OPREATIONAL STATUS SHALL BE DEFINEDAND DOCUMENTED.

Implementation guidance:

Operational systems demand the utmost integrity and reliability. Using the same equipment and software to develop and test new systems makes the organization vulnerable to failures of integrity and loss of availability. Risks are particularly high where new communications equipment is being developed or tested. Errors and omissions can lead to unauthorized access, introduction of malicious code and plenty of other security problems. Therefore, measures such as strong access control should be applied to separate development, test and operational facilities. Fully tested developments should be fed into the change control procedure in readiness for operational acceptance (see also 2.6.1.2 and 2.8.5.1).

Smaller organizations may well find difficulties in providing such separation. Additional controls may be required to compensate, such as tight access control at the file level and careful monitoring of activities.

Auditing guidance:

Smaller organizations may find this difficult to address but it is important that this separation is achieved to avoid disruptions in the operational process. Therefore, the auditor should establish how such separation is operated and what authorisation processes ensure that under development and untested application software is not used on operational systems.

If operational applications software and information are held on the same system as those under development and test, then the auditor should ensure that strong access controls are in place to ensure that no mixing of development and operational facilities takes place.

Different log-ins with different passwords should be necessary for operational and development and test systems, and compliers, system utilities, facilities to edit programmes etc. should not be accessible from operational systems. Check how new software is introduced (see also 2.6.1.2 above), and that this software is no longer in the development or testing state.

2.6.1.6 External facilities management (BS 7799-2 - cl. A.8.1.6)

PRIOR TO USING EXTERNAL FACILITIES MANAGEMENT SERVICES, THE RISKS SHALL BE IDENTIFIED AND APPROPRIATE CONTROLS AGREED WITH THE CONTRACTOR, AND INCORPORATED INTO THE CONTRACT.

Implementation guidance:

A risk assessment is required before any system is turned over to the management of an external contractor. The organization can become highly vulnerable to many possible exposures depending on the precise details of the contract scope, but often including breaches of confidentiality, loss of integrity of equipment and data, and loss of availability.

It is important that the risk assessment is carried out in advance of the decision to outsource so that appropriate security safeguards and management controls can be included in the contract.

IT activities are often outsourced with a view to ‘getting IT off our hands’. However, far from removing the responsibility for managing and controlling the systems and their security, outsourced systems require a particularly carefully thought out control framework to be established. This framework should concentrate on staffing, access control and obtaining, on an ongoing basis, the necessary level of assurance that the systems and their security are being managed according to the standards that should have been laid down in the contract. Reliance on contract terms and clauses will not provide assurance or any certainty of compliance.

Comprehensive documentation should be kept in order to be able to demonstrate the status of systems at given times, and the actions and controls agreed between the parties. This will be necessary to support any case of dispute between the parties.

Auditing guidance:

Organizations employing external facilities management (FM) should fully address these requirements. A risk assessment should be used to identify the security requirements and required controls, followed by contract or service level agreement negotiation and finally monitoring of performance.

The auditor needs to establish that where FM services are employed, these issues have been addressed. Look also at the results of monitoring, how is the organization ensuring that sensitive information is being properly handled? Do they have an insight on what procedures the FM organization is using, both with regard to security and general operations? What do they know about the personnel who have access to their facilities?

2.6.2 System planning and acceptance (BS 7799-2 - cl. A.8.2)

Objective: To minimize the risk of systems failures.

ISO/IEC 17799 extension: Advance planning and preparation are required to ensure the availability of adequate capacity and resources. Projections of future capacity requirements should be made, to reduce the risk of system overload. The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

2.6.2.1 Capacity planning (BS 7799-2 - cl.A.8.2.1)

CAPACITY DEMANDS SHALL BE MONITORED AND PROJECTIONS OF FUTURE CAPACITY REQUIREMENTS MADE TO ENABLE ADEQUATE PROCESSING POWER AND STORAGE TO BE MADE AVAILABLE.

Implementation guidance:

With growing requirements for the use of information processing facilities, an organization will be vulnerable to loss of service due to inadequate resources, both facilities and staff. The risk should be reduced by monitoring the use of present resources and, with the support of user planning input, projecting future requirements. This is especially important for communications networks where changes in load can be very sudden, resulting in poor performance and unproductive users.

The capacity planning process is likely to be cyclical and evidence of requirements should be obtained and documented in a standard manner that enables reliable capacity calculations to be made.

Auditing guidance:

Forward planning of basic operational needs is often overlooked and auditors should assess the organization’s ability to handle this. The first question should be “what is monitored?” This would typically be disk capacity, transmission throughput, printer utilisation and other potential bottlenecks.

Consider then how the information received from the monitoring is used to identify future capacity requirements. Trending information and extrapolating requirements allows planned upgrades with minimal disruption. This should include capacity figures, trended as appropriate, review and identification of needs and upgrade plans. Look also at staff planning. Inadequate human resources at critical times can often compromise security.

2.6.2.2 System acceptance (BS 7799-2 - cl. A.8.2.2)

ACCEPTANCE CRITERIA FOR NEW INFORMATION SYSTEMS, UPGRADES AND NEW VERSIONS SHALL BE ESTABLISHED AND SUITABLE TESTS OF THE SYSTEM CARRIED OUT PRIOR TO ACCEPTANCE.

Implementation guidance:

New systems can bring in un-recognized vulnerabilities. It is important that acceptance criteria are established in advance of delivery and testing carried out to ensure that vulnerabilities are controlled. This control is also applicable where new subsystems and devices are being introduced, and where changes are being made to existing systems.

In particular, any adverse effects on existing systems should be identified and brought under control before acceptance into operational services. It is especially important that new facilities connected to the communications network are properly secured prior to connection.

All levels of acceptance testing should be documented and signed off at an appropriate level.

For major new developments, the operations function should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

Auditing guidance:

Introduction of new or upgraded systems requires careful planning. The introduction of new systems, upgrades and new versions of software needs to be very carefully managed to ensure no loss of service or compromise of data occurs where operational systems are concerned.

The auditor should look for clear acceptance criteria that need to be fulfilled prior to implementing new or upgraded systems. New systems or processes need to be thoroughly tested before operational use. What plans are there, have they been reviewed for adequacy, how have the results been recorded?

Adequate testing usually means more than just testing new functionality; has sufficient consideration been given to regression tests, has the system response to defective data or false operator input been covered, are access controls fully secure, what about other security controls?

With system acceptance may come training; has this been catered for, who has determined its adequacy, have all necessary personnel been involved, both in the preparation of and receiving of training? Who authorises final acceptance before operational use? Check this is defined and recorded.

2.6.3 Protection against malicious software (BS 7799-2 - cl. A.8.3)

Objective: To protect the integrity of software and information.

ISO/IEC 17799 extension: Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses (see also 10.5.4) and logic bombs. Users should be made aware of the dangers of unauthorized or malicious software, and managers should, where appropriate, introduce special controls to detect or prevent its introduction. In particular, it is essential that precautions be taken to detect and prevent computer viruses on personal computers.

2.6.3.1 Controls against malicious software (BS 7799-2 - cl. A.8.3.1)

DETECTION AND PREVENTION CONTROLS TO PROTECT AGAINST MALICIOUS SOFTWARE AND APPROPRIATE USER AWARENESS PROCEDURES SHALL BE IMPLEMENTED.

Implementation guidance:
The standard operating systems are vulnerable to the threat of malicious software. They are easy to catch, but they can be difficult and costly to get rid off, and prevention can only be achieved to a certain level, and it is necessary that this control is strictly applied and followed. Malicious software in a networked system can have a serious impact on confidentiality (Trojan horses), and integrity and availability of all files on a system. Traditionally viruses have affected only executable programs. However, macro viruses in word processing and spreadsheet files are a cause of significant difficulty because such files are quite commonly passed from user to user, and other forms of malicious software can spread to any file in the system.

The key to prevention is user awareness. If staff understands the risks they will generally respond to controls. In many cases, it is still advisable to use controls that run independently in the background, carrying out all necessary checks automatically. Enforced controls can also be implemented where appropriate, such as on network file servers supporting a large number of workstations. It is recommended that dynamic updates be used to ensure that the protection remains effective. The controls described in ISO/IEC 17799, Clause 8.3.1 should be applied to ensure sufficient protection.

Auditing guidance:
Malicious software is a problem in almost all operating systems; therefore the auditor should ensure that necessary controls are fully adequate. A number of options are available when installing software protecting against malicious software: sometimes it is held on a central server and that covers all client systems that are logged on, other systems require the protection software to be installed on each system. Sometimes the installation updates the entire software package, other times libraries only are involved, so auditors need to know how to determine correct versions.

Another important point to check is that the updating is done whenever it is necessary, e.g. through an automatic update or some other form of getting notified of necessary updates. Handling of portable systems may involve particular problems, how is regular update assured? If the checks are not constantly running in the background (very often a good option, but not always possible), procedures should be explicit about regular checking; there should be a clear policy on incoming software.

The actions in the event of virus infection should be covered. Occurrences of malicious software infections must be properly recorded. Look at the type of software used, is it adequate and properly supported?

Free packages from, for example, the Internet, may not give the necessary protection and in extreme cases could cause additional damage. Ensure that operators know and use the correct methods of interfacing with applications, operating systems etc., a request for password information out of sequence, for example, could be an attempt to obtain a password and access vital data.

2.6.4 Housekeeping (BS 7799-2 - cl.A.8.4)

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

ISO/IEC 17799 extension: Routine procedures should be established for carrying out the agreed back-up strategy (see 11.1) taking back-up copies of data and rehearsing their timely restoration, logging events and faults and, where appropriate, monitoring the equipment environment.

2.6.4.1 Information back-up (BS 7799-2 - cl. A.8.4.1)

BACK-UP COPIES OF ESSENTIAL BUSINESS INFORMATION AND SOFTWARE SHALL BE TAKEN AND TESTED REGULARLY.

Implementation guidance:

Every organization is vulnerable to the crashed disk or the failed tape. Data integrity and availability should be maintained by making regular copies to other media. The regularity will depend on the criticality of the data. Some systems can justify dual writing - writing the copy at the same time as the original. Others will be happy with once per day copying. A back-up cycle should be designed to ensure that all data are copied at appropriate intervals while maintaining at least two copies of each file. This can, for instance, be satisfied with a three tape cycle. Risk assessment should be used to identify the most critical data, which may justify more frequent copying.

Copies should be stored in a safe place. Full copies of data should be kept off site or at least in a fireproof safe. It is important to regularly test the ability to restore data from back up.

Some data should be kept in long-term archive. It is essential to maintain the means to recover data that has been archived. This requires the appropriate computer, media reading device, the software to read the data format, e.g. database manager, and the correct version of the application programs to interpret the data fields. Failure to recover data could leave the organization in breach of statutory requirements to maintain records for as long as ten years, e.g. VAT and Inland Revenue records. Comprehensive records of tape contents and program/data relationships should be maintained.

Auditing guidance:

Back up is a key component in maintaining information integrity and availability. The organization should have well defined procedures for dealing with back up. Initially look at the back-up sequence, which needs to be consistent with the business and the security requirements, and compatible with recovery and business continuity plans.

In a typical network environment this is based on full server back up plus a number of incremental updates in defined in a frequency appropriate for the requirements for integrity and availability, e.g. daily, weekly or monthly cycles. Check that this includes the full coverage within the ISMS scope. - ISO/IEC 17799, clause 8.4.1, recommends - as good practice - a minimum three backup generations be kept.

How and where the back-up media is marked and stored is also important; check that each item can be positively identified, is logged correctly and is held securely. Back-up media should be held in separate locations to the systems they back up, and sufficient controls should be in place to give the same level of protection the backed up information normally has.

Establish what the long term storage requirements of critical data are, how does the organization validate this - back-up media may deteriorate and need to be refreshed. Look also in the procedures for back-up, what corrective actions are required if the back-up fails, what arrangements exist for restoring the data, how often is this exercised, what records are kept? Are back-up media tested to ensure they are working properly? Test restoring of back-up files must not compromise data integrity, check this is adequately addressed. Check that requirements for business continuity planning, (see also Section 2.9), are met by the back-ups kept in terms of frequency, media and availability.

2.6.4.2 Operator logs and fault logging (BS 7799-2 - cl. A.8.4.2 & 8.4.3)

OPERATIONAL STAFF SHALL MAINTAIN A LOG OF THEIR ACTIVITIES. OPERATOR LOGS SHALL BE SUBJECT TO REGULAR, INDEPENDENT CHECKS.
FAULTS SHALL BE REPORTED AND CORRECTIVE ACTION TAKEN.

Implementation guidance:
Both automatic and hand written logs of operator activity are important for providing assurance, through monitoring, of the integrity of computer operation. They are often a very useful aid to incident investigation. They should be retained on file for a reasonable period of time and be subject to regular, independent checks against operating procedures.
As with all types of incident, system faults can expose vulnerability to loss of service integrity and availability. All faults should be logged to enable orderly corrective action to be taken. In the longer term, logs can be analysed to identify unacceptably unreliable equipment and fault trends in individual devices. Special care should be taken where the fault or its correction may have compromised security.

Auditing guidance:
The computer operating procedures should identify the logs that need to be kept, both for normal operations and fault incidence. Logs should have evidence of review as part of internal monitoring. The auditor should check that the logs contain sufficient information, as mentioned in ISO/IEC 17799, clause 8.4.2. When checking operating logs for context look at how shift changes are recorded, occurrence of carry-over operations, special requirements etc. Look also at the archiving of logs, both manually and machine recorded, are they identified, can they be retrieved?
Faults need to be followed to satisfactory corrective actions. Part of the criteria for review should be a check that security has not been compromised, check that this is defined in the procedures and understood by management. It should be ensured that all faults have been satisfactorily resolved. Auditors should also ensure that any corrective action could only be carried out by sufficiently authorised personnel.

2.6.5 Network management (BS 7799-2 - cl. A.8.5)

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

ISO/IEC 17799 extension: The security management of networks which may span organizational boundaries requires attention. Additional controls may also be required to protect sensitive data passing over public networks.

2.6.5.1 Network controls (BS 7799-2 - cl. A.8.5.1)

A RANGE OF CONTROLS SHALL BE IMPLEMENTED TO ACHIEVE AND MAINTAIN SECURITY IN NETWORKS.

Implementation guidance:
Networks are especially vulnerable to misuse and abuse as well as the unintentional failings of technology. They are complex and it is easy to make mistakes in their configuration and control. As a result their integrity can be impaired and their availability lost.

The confidentiality and integrity of data passing over public networks should also be considered, with the implementation of appropriate controls to protect the data and the organization's connected networks and systems.

The only way to reduce these risks is to put in place effective management and security controls together with sound procedures. Good network security begins with network planning and security should be considered in every aspect of implementation, operation, problem management and monitoring. The security management of networks has become a significant part of the overall security management activity within an organization, with specialist knowledge being required for each communications technology. Many specialist security tools are now available to protect the network in different ways:

- Remote control of network equipment and user workstations for problem solving and software management;
- Network monitors (known as 'sniffers') to detect attacks and analyse traffic;
- Encryption of transmitted data to retain confidentiality;
- Restricted routing per user or network address;
- Access control techniques to allow only authorized users;
- Protocol controls to assure data integrity.

Many of these require policies and procedures to be established at the organization level. The implementation and management of encryption, in particular, demands the highest level of control to ensure that integrity of the service is maintained.

All these techniques require comprehensive authorised documentation for network designs, implementation, operation, and changes and monitoring. Constant monitoring of security status is essential in a large network environment with appropriate records being kept of faults, problems and corrective actions.

Auditing guidance:
Network topology and operating environments, particularly where sensitive traffic is involved, should be properly planned and managed; check that management has done this with formal records. Have due consideration and protective mechanisms been employed where networks have access to or use public networks?

For large, complex operations, use of suitable consultants may be appropriate, if not, look carefully at the qualifications of internal network designers. Have the most exposed aspects of network operations been identified, what protective measures have been adopted? Security breaches on networks are not always immediately obvious, data may be intercepted, copied or modified without any apparent trace.

Look to see what monitoring activities are used to identify such breaches, and take care that the incident reporting procedures (see also Section 2.4.3) cover this. Network, data encryption, digital signatures, etc. are all areas of rapid technological change, look to see how the organization is monitoring the developments in this area and identifying new threats to security and their protection mechanisms as they arise.

2.6.6 Media handling and security (BS 7799-2 - cl. A.8.6)

Objective: To prevent damage to assets and interruptions to business activities.
Media should be controlled and physically protected.

ISO/IEC 17799 extension: Appropriate operating procedures should be established to protect documents, computer media (tapes, disks, cassettes), input/output data and system documentation from damage, theft and unauthorized access.

2.6.6.1 Management of removable computer media (BS 7799-2 - cl. A.8.6.1)

THE MANAGEMENT OF REMOVABLE COMPUTER MEDIA, SUCH AS TAPES, DISKS, CASSETTES AND PRINTED REPORTS SHALL BE CONTROLLED.

Implementation guidance:
Removable media, containing the organization's data, presents a serious vulnerability to loss of data and breaches of confidentiality. Controls are required in the management of media items, which include tapes, cartridges, cassettes, etc. Library procedures are necessary to ensure that media are used, maintained and transported in a safe and controlled manner. The supplier's recommendations on storage conditions should be followed.
Authorization should be required for the removal of any item from the premises for transport (see 2.6.7.2). Risk assessment should recognize that the effectiveness of controls is limited by the ease with which small media items can be removed from the premises.

Auditing guidance:
Look at how media is removed from site; this may be for transfer to secure archive storage, by personnel for business use, or for destruction. There should be a well-defined procedure and logging mechanism in each case as appropriate. The procedure should ensure that the removable media are erased to ensure that no information is leaked out. If the media is to be destroyed or otherwise no longer used to hold sensitive information, check to see how it is erased before release, how is the labelling dealt with?
Look also at the transport arrangements for various media, is it sufficient protection? Whatever controls are in place this is a difficult area to police, so check that organizations have properly identified this in the risk assessment and whether any compensating controls have been applied?

2.6.6.2 Disposal of media (BS 7799-2 - cl. A.8.6.2)

MEDIA SHALL BE DISPOSED OF SECURELY AND SAFELY WHEN NO LONGER REQUIRED.

Implementation guidance:
An item no longer required is often regarded as worthless. But if it contains data, it may well be of interest and value to others. Serious breaches of confidentiality occur when apparently worthless disks, tapes, paper files and printer ribbons are dumped without proper regard to their destruction.
The procedures for the handling of classified information should cover the appropriate means of its destruction and disposal (see also Section 2.6.6.3 below). A record of sensitive items should be maintained at the point of destruction.

Auditing guidance:
Erasing of media due for destruction or alternative use was covered above, (see Section 2.5.3.2 Removal of property). The auditor still needs to look at the disposal procedures for those items listed in ISO/IEC 17799, Clause 8.6.2.
Look at what general disposal arrangements there are, where external contractors handle this, check that the organization has done proper security and process checks and that the most sensitive level of information handled in this way is known and verified. It should be checked that – whatever the specific arrangements are – sensitive information cannot be

compromised through the disposal process because it has been erased or destroyed before. There should be some logging process; check that this provides a satisfactory audit trail.

2.6.6.3 Information handling procedures (BS 7799-2 - cl. A.8.6.3)

PROCEDURES FOR THE HANDLING AND STORAGE OF INFORMATION SHALL BE ESTABLISHED IN ORDER TO PROTECT SUCH INFORMATION FROM UNAUTHORIZED DISCLOSURE OR MISUSE.

Implementation guidance:
There is serious risk of a breach of confidentiality when sensitive information is being handled, e.g. invoices, cheques, and financial transaction data. Controls in the shape of good procedures together with appropriate authorities and records are required for the safe handling of all forms of sensitive information. Records should establish who is accountable for the information at all times with clear hand over from one person to another. Where carriers or couriers are transporting the items ensure that there is a clear record of proven identity of the individual. All items should be clearly marked with the name of the ultimate recipient who should provide record of receipt.
Sensitive items should be identified by risk assessment and all activities and movements should be logged for later monitoring.

Auditing guidance:
The auditor should check that procedures are in place to protect sensitive information – regardless which form it takes – in line with the classification scheme used by the organization. What recording is done of who is responsible for the information, which authorises its release?
Where information is being handled by persons unknown to staff - such as couriers - what additional identity checks are made? Are access restrictions in place, and if so, which? ISO/IEC 17799 provides a list of controls that should be applied in the information handling procedures.

2.6.6.4 Security of system documentation (BS 7799-2 - cl. A.8.6.4)

SYSTEM DOCUMENTATION SHALL BE PROTECTED FROM UNAUTHORIZED ACCESS.

Implementation guidance:
Systems are vulnerable to the unauthorized use of system documentation; much of the information should be regarded as confidential and protected as such. Of particular concern should be documents that give an insight into the workings and implementation of the security system and local changes to the whole system. Security procedures, operating manuals and operating records all come into this category.
Ensure that the material is appropriately classified (see Section 2.3.2 above) and secured in lockable cupboards. Document distribution should also be secure and a suitable disposal procedure provided (see next section below). Distribution should be controlled to ensure that copies go only to those with a business need.

Auditing guidance:
Basic documentation procedures may need to be extended for sensitive information such as system operating manuals, configuration information, access control lists, etc. Such system documentation might contain sensitive information. Auditors should ensure that the security classification system (see also Section 2.3.2) is correctly employed and the documents are correctly labelled.
It might be the case that this documentation provided by manufacturers and so issue control will rely on externally supplied material. Distribution of secure documents must be strictly

controlled, where permitted, copying may be required. If system documentation is held on a network, sufficient access controls should be implemented to ensure that only authorised personnel gains access.

2.6.7 Exchanges of information and software (BS 7799-2 - cl. A.8.7)

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

ISO/IEC 17799 extension: Exchanges of information and software between organizations should be controlled, and should be compliant with any relevant legislation. Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit should be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

2.6.7.1 Information and software exchange agreements (BS 7799-2 - cl. A.8.7.1)

AGREEMENTS, SOME OF WHICH MAY BE FORMAL, SHALL BE ESTABLISHED FOR THE EXCHANGE OF INFORMATION AND SOFTWARE (WHETHER ELECTRONIC OR MANUAL) BETWEEN ORGANIZATIONS.

Implementation guidance:
When sending information to another organization there is always the risk that they may not look after it the way you would want them to. This can lead to unauthorized exposure and a breach of confidentiality, and possibly bad publicity, for you, if not for the other organization.
Agreements or contracts should specifically establish the level of security expected to be applied by the other party including specific controls in sensitive cases. Where escrow is involved, procedures must be provided for recovery of the item in escrow, noting the authorities required for release.
Agreements should be authorized at an appropriate level in the organization and periodically reviewed. Changes in practice should always be controlled and reflected where necessary in the agreement.

Auditing guidance:
Auditors need to initially establish which organizations are involved in the transfer of sensitive information, and then to ensure the necessary contractual documents exist. This covers not only information but also software as well; this could be the case in, for example, the situation where a software house has developed programs for handling critical data, the organization may need to ensure access to that software via escrow agreements.
Look at what protection other organizations have for information in their care. Check that the agreements between organizations exchanging sensitive information or software include the items addressed in ISO/IEC 17799, Clause 8.7.1.

2.6.7.2 Security of media in transit (BS 7799-2 - cl. A.8.7.2)

MEDIA BEING TRANSPORTED SHALL BE PROTECTED FROM UNAUTHORIZED ACCESS, MISUSE OR CORRUPTION.

Implementation guidance:
Transport provides a vulnerability to loss, unauthorized access and misuse with attendant risk to confidentiality, integrity and availability. Risk assessment should be used to help

select the right transport method and the controls applied to it (e.g. by post with recorded delivery, secure parcel delivery). Appropriate courier services and packaging should be selected including locked containers for sensitive or valuable items.
All despatches should be recorded and, where appropriate, authorized.

Auditing guidance:
Whenever information is physically transported, it should be considered what protection is in place to protect the media holding the information. What are the transport arrangements? If couriers, do they have secure and tamper proof containers? Data may be transmitted by staff on disks or tapes or indeed on notebook computers, is this secure enough for the information carried?
Who determines the method of transportation, what criteria do they use? Where couriers are employed, the methods of transportation may be the carrier's default methods - are these sufficient? Consider also postal services, are these secure? In all cases where there is a requirement for transport of secure information there should be formal procedures defining the arrangements and the authority for release must be specified and recorded.

2.6.7.3 Electronic commerce security (BS 7799-2 - cl. A.8.7.3)

ELECTRONIC COMMERCE SHALL BE PROTECTED AGAINST FRAUDULENT ACTIVITY, CONTRACT DISPUTE AND DISCLOSURE OR MODIFICATION OF INFORMATION.

Implementation guidance:
Electronic commerce is a common way of conducting business, despite the security problems associated with it. Controls should be implemented to protect the information involved in electronic commerce activity from the various threats related to this way of doing business.
ISO/IEC 17799, Clause 8.7.3 provides a range of controls that are applicable to electronic commerce. For example, the application of cryptographic controls (see also 2.8.3) can achieve protection in several ways:

- encryption can be applied to ensure the confidentiality of information such as billing details, customer information and personal information;
- digital signatures can be applied to ensure the integrity of electronic transactions and to authenticate the partners involved in the transactions;
- encryption and digital signatures can be used to achieve non-repudiation which helps to resolve disputes regarding the occurrence or non-occurrence of events.

When using cryptographic controls, care should be taken that an appropriate policy and key management system is in place, and that these controls comply with any legal requirements (see also 2.10.1.6) that might be applicable.
Any organization applying electronic commerce should have a policy in place that describes who is allowed to carry out electronic commerce activities, what each of these employees is authorized to do, and what controls are in place to protect and monitor such activities.

Auditing guidance:
Auditors should inquire about the current and future electronic commerce activities within the organization. All activities related to the organization's use of electronic commerce, should be reviewed for any security related aspects. This includes checking that:

- an authorization process is in place: can only those employees within the organization that are authorized carry out electronic commerce activities?

- there is suitable segregation of duties: are activities that, in combination, can be used to commit fraud segregated or supervised?
- appropriate cryptographic controls are in place (see also Section 2.10.3) to ensure the authenticity, integrity and confidentiality of information processed in relation with electronic commerce, and is a policy in place to regulate the application of such controls?
- appropriate network security controls are in place to protect the organization's network and the host used for electronic commerce from attacks that can result from the interconnection with other networks (see also Section 2.9.4)?
- sufficient protection is given to guard against risks from the outside: is the organization applying the controls described in ISO/IEC 17799, 8.7.3, to protect itself from security problems related to electronic commerce?

2.6.7.4 Security of electronic mail (BS 7799-2 - cl. A.8.7.4)

A POLICY FOR THE USE OF ELECTRONIC MAIL SHALL BE DEVELOPED AND CONTROLS PUT IN PLACE TO REDUCE SECURITY RISKS CREATED BY ELECTRONIC MAIL.

Implementation guidance:

Email provides several different security risks to any organization using it without appropriate controls. Case history already shows that organizations can be wide open to libel writs as a result of what their staff write in an email message, often informally and supposedly for internal distribution only. The use of Internet email has significantly increased the risks.

Organizations should draw up a clear communications policy regarding the status and use of electronic mail and with particular reference to Internet email. The legal implications of both internal and external messages should be properly understood. The exposure of even an internal message that is critical of another organization or person could result in legal action. An external message may amount to an unintended contract between the parties. Deleted messages may well remain for one or more years in the back-up system from which they could be retrieved if required. The courts and statutory regulators may have the powers to demand extensive disclosure from archives.

Where email is to become the normal means of communication between the organization and another identified organization, there should be a written agreement setting out the precise status of email messages between the two. For example, it may be agreed that an email message cannot be an implied contract and that all contracts will continue to be made in writing, signed and sent by post or fax.

Email can be a source of infection with malicious software, and appropriate controls should be applied (see also 2.6.3.1 above) to protect against that.

All these aspects make email a relatively high risk service. It is essential that staff is properly trained in the organization’s requirements and control mechanisms.

Auditing guidance:

Using e-mail transmission is now very common in almost all organizations. As e-mail is extremely vulnerable, the controls in place to protect it should be carefully considered: How is information included in and attached to e-mail messages controlled, how is correct receipt verified? How is incoming data verified as to source and integrity?

If applicable, what encryption methods are applied? If encryption and digital signatures are used, are the controls discussed in Section 2.10.3 applied to ensure sufficient security? Is information received from e-mail checked for virus infection before use? Does e-mail within the organization have a different integrity status from that sent externally, if so how is this defined and monitored?

There are considerable legal risks in the use of e-mail and organizations should have a clear and implemented policy on this issue. Internal messages could inadvertently be sent to external parties, contracts may be implied, messages and any attachments could be held on back up for years. Standard disclaimers attached to e-mail messages may help but their legal status as protection is dubious.

Auditors should investigate, particularly where access to external e-mail is permitted, that due risk assessment has been performed and managed. For example, it may be appropriate to restrict access to e-mail transmission to a limited number of individuals, if so, how is this enforced? Test the protection mechanism.

2.6.7.5 Security in electronic office systems (BS 7799-2 - cl. A.8.7.5)

POLICIES AND GUIDELINES SHALL BE PREPARED AND IMPLEMENTED TO CONTROL THE BUSINESS AND SECURITY RISKS ASSOCIATED WITH ELECTRONIC OFFICE SYSTEMS.

Implementation guidance:

Office systems have improved the effectiveness and efficiency of many staff but they have increased the risks of exposure and misuse of information. The simplicity with which files can be copied to other users emphasises the need to ensure proper protection for confidential material.

Risk assessment should identify information that needs full protection, perhaps away from the general mass of office information. Common diary systems can expose the movements of senior staff who may be conducting confidential business that could, for instance, affect share prices. The status of individual users may need to be indicated in directories; the directories themselves may be a source of sensitive information. Other aspects of control to be considered include access control, fallback and the business recovery plan, and many of the controls referred to in other sections of this guide.

Auditing guidance:

Whilst considerable increases in efficiency can result from electronic office systems, so can the risks of misuse, disclosure or destruction of the information sent, due to poorly defined procedures. Auditors should determine which procedures have been developed, how they have been implemented, what information is needed to be kept and where and whether the attendant risks have been identified.

Use of electronic diaries may distribute sensitive information, movements of key personnel beyond those who should see it; common personnel databases may contain sensitive personal information; workflow packages may rely on key data that has been corrupted, omitted or entered by someone without the necessary authority or knowledge.

Look at access control to these systems and to the information being sent around. Are employees aware of the fact that the information they are passing on might be easily accessed by anybody else having access to the office system?

Where external access to office facilities is permitted - such as for home workers or other organizations - then these links can severely downgrade the overall security of the network, and the implementation of further controls should be considered. This is even truer where the access is via public links such as the Internet.

2.6.7.6 Publicly available systems (BS 7799-2 - cl. A.8.7.6)

THERE SHALL BE A FORMAL AUTHORIZATION PROCESS BEFORE INFORMATION IS MADE PUBLICLY AVAILABLE AND THE INTEGRITY OF SUCH INFORMATION SHALL BE PROTECTED TO PREVENT UNAUTHORIZED MODIFICATION.

Implementation guidance:
The organization should ensure that all employees are aware of the rules and authorization process that applies to information that is intended to be made publicly available. This includes the disciplinary action that is taken if these rules are not complied with. Publishing incorrect or inappropriate information could have a damaging impact on the organization's reputation and its business. The information should also be checked carefully for correctness, completeness, topicality and compliance with legislation prior to its publication.

The information once published should then be protected from any unauthorized modification. Such modifications can easily be made if no appropriate protection is in place, and this has happened many times, damaging the reputation of those organizations.

If information is obtained via publicly available systems, care should be taken that this information can be verified, if necessary, and that any processing of this information is accurate, timely and compliant with the applicable legislation.

Auditing guidance:
If the organization is using publicly available systems, such as a Web server connected to the Internet to publish information or to retrieve information or data, auditors should inquire about the protective controls that are in place and review that they are applied correctly.

This includes a check of the authorization process for publishing of information. Is it possible for employees to add to or to update already published Web pages without authorization? Is anybody in the organization regularly checking the content of the published information? Has anybody within the organization checked the information published or obtained through publicly available systems for compliance with applicable legislation, especially legislation in the country where it is made public? Is the information published protected to ensure that nobody from the outside can manipulate it?

In addition to protecting published information, it might be necessary to protect the organization's network from intruders that are using the connection as a means to achieve unauthorized access. Auditors should check that access controls as described in Section 2.9 are in place to protect from such unauthorized access.

2.6.7.7 Other forms of information exchange (BS 7799-2 - cl. A.8.7.7)

POLICIES, PROCEDURES AND CONTROLS SHALL BE IN PLACE TO PROTECT THE EXCHANGE OF INFORMATION THROUGH THE USE OF VOICE, FACSIMILE AND VIDEO COMMUNICATIONS FACILITIES.

Implementation guidance:
The exchange of information using common communication media such as normal or mobile phones, answer machines, video or faxes carry a lot of risks for compromise of this information. All employees should be aware of the possibilities of:

- being overheard when using mobile phones in public places,
- sensitive or confidential information being intercepted when communicated using phones,
- messages and faxes being received by the wrong person through mis-dialling,
- the wrong person picking up a fax or listening to an answer machine message despite the right number being dialed.

An appropriate policy dealing with these issues should be communicated to all employees that use such forms of information exchange, and awareness training with real life examples should be used to illustrate the risks involved.

Auditing guidance:
This control refers to the secure use of mobile computing devices, telephones and mobiles, fax machines, hand held computers, answering machines and so on. Auditors should inquire the procedures that have been developed to manage such information exchange and to review these against the controls described in ISO/IEC 17799, Clause 8.7.7.
It should be ensured that employees are aware of these procedures, for example, by asking them about their use of mobile phones, answer machines or fax machines, to find out whether they are aware of the risks involved.

2.7 Access control (BS 7799-2 - cl. A.9)

2.7.1 Business requirement for system access (BS 7799-2 - cl. A.9.1)

Objective: To control access to information.

ISO/IEC 17799 extension: Access to information, and business processes should be controlled on the basis of business and security requirements. This should take account of policies for information dissemination and authorization.

2.7.1.1 Access control policy (BS 7799-2 - cl. A.9.1.1)

BUSINESS REQUIREMENTS FOR ACCESS CONTROL SHALL BE DEFINED AND DOCUMENTED, AND ACCESS SHALL BE RESTRICTED TO WHAT IS DEFINED IN THE ACCESS CONTROL POLICY.

Implementation guidance:
Access control is the fundamental pre-requisite to managing any of the activities undertaken on a computer. The confidentiality, integrity and availability of the organization's business information and processes, and therewith a lot of other business assets, are at stake.
In principle, access should be driven by business requirements, and this should be clearly stated in the access control policy. Failure to implement the policy effectively will very soon result in too many people having access and at higher levels than necessary. This leads to unjustified access to information and a serious risk of unauthorized disclosure, unauthorized modification, loss of data integrity and, ultimately, its unavailability while recovery takes place.
Standard user access profiles for specific jobs are a useful way of controlling access where many users are involved.

Auditing guidance:
Auditors need to ensure that access control is clearly defined in the access control policy document and that the mechanisms for enforcement of this policy are in place and implemented. Any access to sensitive information should be based on the "need to know" principle. Any access granted should be based on the business requirements and be necessary for the job carried out.
Auditors should be prepared to question why, possibly senior, people need access to certain information if the principle of "need to know" appears not to be evident. Check also that access to sensitive information takes place in line with the classification given and that

personnel with access to such information have been properly trained as unrestricted use of sensitive information by untrained staff can have disastrous consequences.

2.7.2 User access management (BS 7799-2 - cl. A.9.2)

Objective: To prevent unauthorized access to information systems.

ISO/IEC 17799 extension: Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

2.7.2.1 User registration (BS 7799-2 - cl. A.9.2.1)

THERE SHALL BE A FORMAL USER REGISTRATION AND DE-REGISTRATION PROCEDURE FOR GRANTING ACCESS TO ALL MULTI-USER INFORMATION SYSTEMS AND SERVICES.

Implementation guidance:
Every user should be formally authorized and registered to each service for which he/she has a business requirement to access. Failure to control registration can result in exposure of information to breach of confidentiality and the added risk of modification or loss.
A user registration form should be prepared upon which the service required is described as well as the conditions of access. This should be signed by the applicant as acceptance of the conditions and by the system owner as authority for the applicant to be registered. This form should have the user ID added to it and then be filed for the record.
It is equally important that users are promptly removed from the system on their ceasing to have a business reason to access it, e.g. termination of employment, internal job move, and procedures should be put in place to ensure this. Redundant user IDs should not be reissued to other users because of the risk of inadvertently giving unauthorized access to resources.

Auditing guidance:
User access should be formally controlled and logged. Consistent with the policies, as discussed above, auditors should ensure that access levels of all users are based on formal registration and authorisation of the users, and that the access taking place is recorded. Check that these records are consistent with actual use, have staff have moved away or changed to other responsibilities been immediately removed from this list?
Auditors will usually need to spend a substantial amount of time with the system administrators looking at operating system setting for access control of specific group and individuals, ensuring that access can only take place for registered and authorised users. ISO/IEC 17799, clause 9.2.1, gives further information on issues to be checked regarding a formal user registration and deregistration process.

2.7.2.2 Privilege management (BS 7799-2- cl. A.9.2.2)

THE ALLOCATION AND USE OF PRIVILEGES SHALL BE RESTRICTED AND CONTROLLED.

Implementation guidance:
Special privileges are any features or facilities of IT systems that enable the user to carry out system management activities in the most sensitive parts of the system, such as maintaining the security system or the data management system. Where they are uncontrolled, an increasing number of users will be using privileges and rendering pointless the properly

implemented access controls. The unnecessary allocation and use of system privileges is often found to be a major contributing factor to the vulnerability of systems that have been breached. Loss of confidentiality through exposure, loss of integrity through modification of data and unavailability of data are typical consequences.

Privileged access to systems is often a difficult aspect for management to control. Systems engineers might try to browbeat managers into providing privilege that is not really required. Privilege is seen as an authorized means to shortcut well placed controls. The fact is that most systems require very little use of privilege to manage them in a perfectly efficient manner.

Risk assessment should address not only the risk of providing special privileges but also the consequences of not having them. Authorization should be provided at a senior level on the basis of a proper justification, which, in some cases, may need support from independent expertise.

An important need for special privilege can be in the event of a system failure. A fast recovery may require the skilled attention of a system engineer who may need to access the internals of a system and make changes that not only require privilege but also ignore controls that have been put in place to protect the system. Such occasions require their own controls, which will often be post event. It is essential that all the actions that are taken are properly logged, assessed and reviewed and further checks of the system made to ensure that its integrity has been re-established.

What happens when the privileged person is not available? An emergency arrangement is required, such as a procedure to enable another systems engineer to obtain privilege out of hours. A user ID and password may be held in the safe under strict procedures for issue. This procedure should ensure that management will find out at the earliest convenient moment that the facility has been used and should be followed up by review, as described above.

Auditing guidance:

By definition, special privileges provide access to system features, which are normally limited. Pay particular attention to system administrators, systems engineers and supplier's engineers and those whose job gives them "super user" access to facilities. Check that whilst this level of access should be restricted, at the same time more than one person should have this facility as without any monitoring availability and ability to supervise activities may be compromised.

Access to secure information may also include codes for safes and other secure areas, these also need to be recorded and regularly changed. Again, ensure that availability of information is not compromised by having access restricted to a single person. It should also be checked that privileges are allocated on a "need to use" and "event by event" basis, immediately removed when they are no longer necessary, and are using a different user identity then the one used for the normal job functions.

2.7.2.3 User Password Management (BS 7799-2 - cl. A.9.2.3)

THE ALLOCATION OF PASSWORDS SHALL BE CONTROLLED THROUGH A FORMAL MANAGEMENT PROCESS.

Implementation guidance:

Passwords are the keys providing access to computers, their services and data. They should only be issued under the fullest control otherwise the organization will be vulnerable to every kind of security problem. Passwords authenticate the use of the related user ID, and are the basis of accountability. If password issue is not controlled then accountability for

computer use is never established. This can lead to loss of integrity due to unaccountable activity. The sharing of passwords, itself a breach of confidentiality, can lead to further exposure and perhaps unauthorized modification and loss of data, as well as a breakdown in accountability.
A procedure is required to ensure that user IDs and passwords are issued only to those with a business need for access and properly authorized by the owner of the resource being accessed. Where other methods of user authentication are being used, similar controls will be required but perhaps with additional controls relevant to the system employed.

Auditing guidance:
Hand in hand with privileged access is password control; this is the main - but not only - mechanism that authorised users gain access to facilities. Look at how passwords are allocated and controlled, sometimes this is under the personal control of the user, at other times the system administrator may issue them. If centrally controlled, where are they held, is this secure, who has access? Whatever process is used for the allocation of passwords, it should be based on the positive identification of the user and applying a formal process enforcing users to change initial temporary passwords. Check that users have signed a statement to keep their passwords confidential, and that they are aware of this responsibility.

2.7.2.4 Review of user access rights (BS 7799-2 - cl. A.9.2.4)

MANAGEMENT SHALL CONDUCT A FORMAL PROCESS AT REGULAR INTERVALS TO REVIEW USERS' ACCESS RIGHTS.

Implementation guidance:
The unjustified allocation of access rights increases the organization's vulnerability to breaches of confidentiality, loss of data integrity and availability through misuse. Access rights should always be based on business need — when the need is passed then the access should be cancelled. The continued need for access should therefore be reviewed periodically and access rights should be withdrawn once the requirement is ended. This is particularly important where users have access to sensitive information or have special privileges to the system.
Procedures should contain the requirement for reviews, they should be logged, and an authorised person should acknowledge that the users listed continue to have authority for the access rights.

Auditing guidance:
Defining access rights without regular review and update is not sufficient. Auditors should check that procedures for the regular review of all kinds of user access rights are in place and followed. This may be a formal audit to check compliance followed by a management level review to check for consistency with business and policy requirements.
It is important that as situations change, people leave and join, jobs change, systems evolve, the access rights of individuals are properly controlled and keep step with developments. Check that special checks (e.g. at higher frequency or spot checks) are applied for privileges.

2.7.3 User responsibilities (BS 7799-2 - cl. A.9.3)

Objective: To prevent unauthorized user access.

ISO/IEC 17799 extension: The co-operation of authorized users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

2.7.3.1 Password use (BS 7799-2 - cl. A.9.3.1)

USERS SHALL BE REQUIRED TO FOLLOW GOOD SECURITY PRACTICES IN THE SELECTION AND USE OF PASSWORDS.

Implementation guidance:
Poor quality passwords are of little value, especially if tested by a serious attacker. Users should be made aware of the good and bad practices when selecting their passwords. Exposed (written down) or obvious and easily guessed passwords lead to misuse of systems by unauthorized persons, with the attendant risk of breaches of confidentiality, loss of integrity and availability of data. ISO/IEC 17799, Clause 9.3.1 contains guidelines for users for allocating and managing their passwords.

Auditing guidance:
Check that the policy on changing passwords, frequency, length and content is sufficient for the security requirements of the organization and the information protected. Some systems enforce rules of this type, others do not – check what other measures are in place if the system does not automatically enforce such rules. If necessary, ask staff to show you they change their password, do they know the criteria, are the codes currently used consistent with policy?
Look also for instances of passwords that are written down on memos, stuck to monitors etc. ISO/IEC 17799, Clause 9.3.1 gives examples of good password practices that should be followed. See also under "password management" above and other sections referenced there. Auditors should ensure proper management authority is obtained when investigating password use.

2.7.3.2 Unattended user equipment (BS 7799-2 - cl. A.9.3.1)

USERS SHALL BE REQUIRED TO ENSURE THAT UNATTENDED EQUIPMENT HAS APPROPRIATE PROTECTION.

Implementation guidance:
Where equipment is accessible it is vulnerable to disclosure, misuse, tampering and theft leading to loss of confidentiality, integrity and/or availability. Where the equipment is an unattended PC that is logged on to a service then greater risks are exposed.
Sensitive equipment, such as communications panels and controllers, should be locked away in equipment rooms or purpose built cupboards. Desktop equipment such as PC base units should be locked or shut down when unattended. Keyboard and mouse use should be protected by password while the PC or terminal is unattended. Screen savers with passwords should be used to hide the screen contents while unattended. Ensure that the strength of the password system is sufficient for the resources being protected.

Auditing guidance:
From an auditors standpoint this is largely a case of having procedures, checking staff are aware of the requirements and the dangers and seeing that they are followed. Look for instances of unattended terminals without some password protection or left logged on. Screen savers on PC's should have some password protection - check. Ask to turn on any terminals switched off; ensure access to information is not possible.

High security equipment such as network servers, communications equipment etc., normally left unattended, should be in some protected environment - check for this and whether it is properly secured.

2.7.4 Network access control (BS 7799-2 - cl. A.9.4)

Objective: Protection of networked services.

ISO/IEC 17799 extension: Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services by ensuring:

a) appropriate interfaces between the organization's network and networks owned by other organizations, or public networks;

b) appropriate authentication mechanisms for users and equipment;

c) control of user access to information services.

Note: The controls below focus on a number of areas where potential security breaches could occur. Before embarking on the implementation or assessment a clear overview is needed of the network topology and its operational and security requirements. In general, one should look at the overall network planning and monitoring aspects - possibly in the context of a much larger system in which the system under investigation forms but a subset - to verify that these have all been identified where applicable, sufficient controls have been applied, incidents are recorded and, particularly important, that there is some verification of their effectiveness. Another important point is how the access facilities are managed, how often and when linking and validation arrangements are changed (this may be for security or technical reasons), how this is promulgated and again verified. See also the note under section. 2.6.5, Network management.

2.7.4.1 Policy on use of network services (BS 7799-2 - cl. A.9.4.1)

USERS SHALL ONLY HAVE DIRECT ACCESS TO THE SERVICES THAT THEY HAVE BEEN SPECIFICALLY AUTHORIZED TO USE.

Implementation guidance:

A major computer service may provide dozens of individual services to thousands of users undertaking a wide variety of activities. Most users may only require two or three of these services. Each user should only have access to those services that they are actually authorized to use, in line with the access control policy (see also Section 2.7.1 above).

Additional control can be provided by restricting the views of the services. Where every user can see the full range of services the organization is vulnerable to unauthorized access attempts with the attendant risk of breach of confidentiality and loss of data integrity. Some computer systems do not provide the means to limit service visibility in the way described. In this situation it may be necessary to consider alternative controls such as preventing logon from terminals outside the organizational area authorized to use a particular service. Particularly sensitive services may have to be implemented on a separate system to fully segregate it.

Network systems provide tools that may be used to manage routing and user access to the various branches of a network (see also Section 2.7.4.2 below). A scheme of access requirements should be superimposed on the network layout and then implemented in the system. Good change control and management is essential to keep the accesses correct and regular monitoring is required to provide assurance.

Auditing guidance:
User logging on to a terminal or application should have access only to those information and services required for their business function and they have been authorised to use. This could, for example, be in a database application where the terminal user is able to access personal training records but not salary details held in the same database. What access is provided to what users needs to be explicitly defined, for some applications total availability of all information may not be a problem, for others in could be critical. It may be that access needs to be limited not only for confidentiality reasons, possibly the integrity of information may be compromised - or could cause other data to be compromised if used.
The auditor needs to establish that necessary restrictions have been identified and implemented in line with the access control policy (see also section 2.7.1.1, Access control policy), that the manuals reflect this, that the access has been incorporated into the design or configuration of the application, and finally, that it is effective. Look also for access at the operating system level where personnel log on as a terminal user to the main server or mainframe, what access is permitted here to directory structures, operating settings and so on?

2.7.4.2 Enforced path (BS 7799-2 - cl. A.9.4.2)

THE PATH FROM THE USER TERMINAL TO THE COMPUTER SERVICE SHALL BE CONTROLLED.

Implementation guidance:
Networks and their connected systems are vulnerable to users roaming around looking for services and facilities that might interest them. These users might also have come through the external access gateway or ‘firewall’. There is a risk of unauthorized access attempts leading to breach of confidentiality and loss of information and services, and data integrity.
Where possible and practical users should be tied to an enforced path through the network between their terminal and the service they are authorized to use. This can be achieved by using network routers, dedicated logical or physical lines, ports dedicated to applications.
Controls may also be required on a location basis. Users may access an application from a secure area but the same users may not access the application from a less secure area (see also Section 2.7.5.1 below).

Auditing guidance:
Where the organization has an enforced path policy – in line with the access control policy, see above – look to see how this is implemented technically and check that there is no way of circumventing this. Flexible network routing may allow certain users to use any terminal for logging on - from a less secure environment this may be contrary to security policy; messages may be routed over alternative network bridges; telephone or other external links could be changed in times of capacity shortage or maintenance.
The organization should be able to show a detailed plan of the network’s topology and to explain which controls have been implemented to enforce the user path – check that the controls implement the desired restrictions.

2.7.4.3 User authentication for external connections and node authentication (BS 7799-2 - cl. A.9.4.3 & cl. A.9.4.4)

ACCESS BY REMOTE USERS SHALL BE SUBJECT TO AUTHENTICATION.

CONNECTIONS TO REMOTE COMPUTER SYSTEMS SHALL BE AUTHENTICATED.

Implementation guidance:
Organizations are very vulnerable to unauthorized access from outside the organization particularly through dial-up ports. Uncontrolled ports can lead to serious cases of computer hacking often resulting in damage to system and application data, as well as breach of confidentiality.

While passwords may be considered adequate in most circumstances internally, they require the support of more sophisticated controls for external access. Authentication techniques involving the use of a physical token and a generated password that is valid only on one occasion reduce the risks to an acceptable level.

Stout policies are required for this aspect of protection and rigid compliance should be demanded by management. Every dial-up line should be identified and risk assessed. No uncontrolled external access should be permitted to any network device or networked system. A risk assessment should be carried out to analyse the full scope of the situation.

Network environments are very vulnerable to unauthorized access, particularly from external sources. Confidentiality, integrity and availability are at risk unless the organization's network nodes properly establish the identity, and hence the authority, of remote communications nodes that attempt to connect. Control can be implemented using automatic node authentication.

Risk assessment should identify the nodes giving the greatest cause for concern and therefore the justification for the particular level of control.

Auditing guidance:
Any organization running secure systems that permit external access or remote connections should fully address these control requirements. Auditors must check that all ports have been identified and a complete risk assessment has been applied.

Initially determine at what level the authentication is handled, application specific or network operating system? If at the application level, have any evaluations and tests been performed to determine whether penetration at the operating system level can invalidate this? Are the actual authentication mechanisms adequate given the sensitivity of the information? Ensure management are fully aware of the risks and have given due consideration to the controls required and that they have been correctly implemented and are reviewed regularly.

There are various authentication mechanisms, ensure that the one(s) used meet the security requirements. If direct dial in facilities are provided check how this operates, a dial back operation to confirm the identity of the calling node is one approach but a more secure authenticator may be needed such as one involving a token device.

2.7.4.4 Remote diagnostic port protection (BS 7799-2 - cl. A.9.4.5)

ACCESS TO DIAGNOSTIC PORTS SHALL BE SECURELY CONTROLLED.

Implementation guidance:
Major computer equipment suppliers are often only able to maintain their level of service by fitting the equipment with a remote diagnostic port. This gives access to the remote engineer who has programmed tools at his disposal to get at the most sensitive internals of the system. The port is very vulnerable to unauthorized access attempts, with risk of serious loss of integrity and unavailability if the internals of the system are tampered with.

While the suppliers are very conscious of the security implications of this facility and generally provide a number of sophisticated controls, the user organization remains responsible for assuring them that the facility is adequately controlled. Procedures to physically disable the port when not in use should be considered. Each use of the port should be specifically authorized by the user organization and logged.

Auditing guidance:
Facilities such as diagnostic ports may be a source of unauthorised access because they are not normally considered part of the overall operation and also that access is often directly at the operating system level, independent of applications - check that the diagnostic ports are appropriately protected.

It may be that they are only a temporary connection, in which case check that they are disabled and secured when not required. Diagnostic ports may be used by external support to investigate problems or update applications code, reconstruct databases etc. Where this is the case, check not only for the proper levels of authorisation for access but also the procedures that have to be followed - what permission and authorisation is required before access, are any operational activities suspended, what records of access, changes etc. are kept?

2.7.4.5 Segregation in networks (BS 7799-2 - cl. A.9.4.6)

CONTROLS SHALL BE INTRODUCED IN NETWORKS TO SEGREGATE GROUPS OF INFORMATION SERVICES, USERS AND INFORMATION SYSTEMS.

Implementation guidance:
Networks are always vulnerable to unauthorized access attempts, which can result in breaches of confidentiality and loss of integrity for the network or its attached systems. The bigger the network the greater the risk. Security is easier to manage if the network is divided up into physical or logical domains. Tight security can then be provided to manage the gateways or ‘firewalls’ between the domains. A firewall can also be used to protect the organization’s networks from unauthorised external access while allowing public access to, for instance, the organization’s web server and to receive email from the Internet.

Network modelling should be used to design the individual domains and risk assessment will show the level of security needed to be applied to each domain.

The domains and their relationships should be carefully documented. The network security plan should be specific about which systems and network devices are in which domain. It is possible for different parts of a single system to be in more than one domain, e.g. by department or business unit. Provided that the security system keeps them apart logically this is acceptable.

Auditing guidance:
The larger the domain, the harder it is to secure it. This is true of networks as much as any other structure. It is highly likely that secure networks will need access to wider aspects of corporate operations - e-mail, intranet web pages, networks of other organizations, etc. - so separation of particularly sensitive areas is needed.

Appropriate segregation in networks could be achieved by physically segmenting the network or by applying network connection and routing controls, e.g. via bridges, routers, firewalls etc, see also section 2.7.4.6 below.

The auditor needs to establish what the security domains are, that they are appropriate for the security requirements, how they are defined and incorporated into network operations. Consider also that security domains may impose restrictions in operational performance, so ensure that these considerations have not led to any compromises in the security of the protected areas.

2.7.4.6 Network connection and routing control (BS 7799-2 - cl. A.9.4.7, & cl. A.9.4.8)

THE CONNECTION CAPABILITY OF USERS SHALL BE RESTRICTED IN SHARED NETWORKS, IN ACCORDANCE WITH THE ACCESS CONTROL POLICY.

SHARED NETWORKS SHALL HAVE ROUTING CONTROLS TO ENSURE THAT COMPUTER CONNECTIONS AND INFORMATION FLOWS DO NOT BREACH THE ACCESS CONTROL POLICY OF THE BUSINESS APPLICATIONS.

Implementation guidance:

Networks are vulnerable to users attempting to use them for purposes for which they have not been specifically authorized. Controls are required to ensure that each user is only able to connect to authorized facilities according to business need. Sophisticated tools such as network routers are available to control the flow of different types of transaction, e.g. email, file transfers, interactive access. These tools should be employed where justified to improve control and reduce risk.

Where networks are shared between organizations the vulnerability to misuse and abuse increases significantly. Routing controls requiring origin and destination address checking will reduce these risks. Risk assessment should be carried out on each connection and its use and controls, and fully documented.

Auditing guidance:

Where shared networks are involved, it might be necessary to restrict the connection capability of users, in line with the access control policy (see also section 2.7.1.1). If users or services will be outside physically secure areas and using inter network links that may use public transmission media, auditors need to determine whether access of this type is permitted into applications and systems, if so are any additional restrictions applied above those for in-house users or services? If limited service restrictions are not applied at the application level, it is quite likely this will be a different network control to that applied locally, how is this handled, is it consistent with policy?

Enforced paths between remote networks may rely on external suppliers, if so what assurance does the organization have of the route's integrity and availability and how is its continual use ensured? What happens when maintenance or breakdowns force alternative paths to be used? Fixed paths over public domain networks will be impossible to enforce and so has this been considered, what alternative transport mechanisms are employed?

2.7.4.7 Security of network services (BS 7799-2 - cl. A.9.4.9)

A CLEAR DESCRIPTION OF THE SECURITY ATTRIBUTES OF ALL NETWORK SERVICES USED BY THE ORGANIZATION SHALL BE PROVIDED.

Implementation guidance:

Connection to third party supplied network services opens up vulnerability to unauthorized access attempts by other parties leading to breaches of confidentiality and loss of integrity. Availability should also be given special attention, checking on the resilience of the supplier's fallback in the event of line or equipment failures. Establish that security standards will be maintained when the supplier is in fallback. It is necessary that the detailed security arrangements being offered be considered by the risk assessment. Additional controls may be needed in some circumstances to offset any identified weakness.

Auditing guidance:

Where the organization is dependent on external suppliers for any networked services, then it is essential that the full extent of all security related attributes are known. Check that the organization has obtained this information, that it is documented, that the security attributes are sufficient and relevant to needs, that it has been incorporated into operational procedures and security controls and that it is regularly reviewed and verified. Remember that these controls need to cover all aspects of confidentiality, integrity and availability.

2.7.5 Operating system access control (BS 7799-2 - cl. A.9.5)

Objective: To prevent unauthorized computer access.

ISO/IEC 17799 extension: Security facilities at the operating system level should be used to restrict access to computer resources. These facilities should be capable of the following:

a) identifying and verifying the identity, and if necessary the terminal or location of each authorized user;

b) recording successful and failed system accesses;

c) providing appropriate means for authentication; if a password management system is used, it should ensure quality passwords [see 9.3.1 d]];

d) where appropriate, restricting the connection times of users.

Other access control methods, such as challenge-response, are available if these are justified on the basis of business risk.

2.7.5.1 Automatic terminal identification and terminal log-on procedures (BS 7799-2 - cl. A.9.5.1 & cl. A.9.5.2)

AUTOMATIC TERMINAL IDENTIFICATION SHALL BE CONSIDERED TO AUTHENTICATE CONNECTIONS TO SPECIFIC LOCATIONS AND TO PORTABLE EQUIPMENT.
ACCESS TO INFORMATION SERVICES SHALL USE A SECURE LOG-ON PROCESS.

Implementation guidance:
It is always useful to know (and be able to log) the identity of a terminal from which an attempt at logon is being made. For sensitive applications, where security is of the essence, it may be necessary to limit access to specific terminals located in a secure area. Risk assessment should highlight this type of application and appropriate terminal identification and authentication should be selected where justified. In some systems it is provided by default, sometimes by the port address of the terminal's cable.

While a logon process should be friendly, it should not disclose information about the system and services that are not appropriate for any unauthorized person who may be testing the system. Systems are vulnerable at the logon screen - the least information given away the better.

The logon procedures should be risk assessed. Some systems do not have the facility to enable this aspect to be controlled and the user has no choice but to accept the system as provided. Users should implement what features are available and introduce compensating controls where necessary.

ISO/IEC 17799, Clause 9.5.2 provides more details of a good log-on procedure.

Auditing guidance:
For specific locations and portable equipment, automatic terminal identification can be used to authenticate these systems, and access should only be permitted after successful authentication. Where this is the case, establish how the authentication is verified, what happens when the terminal malfunctions and has to be replaced? What other protection is applied is some form of user ID still needed, is the terminal physically locked or located in a restricted area?

Logon procedures may be more involved than simply typing the correct name and password. Does the user need to go through a series of logon activities, what happens if the wrong information is entered, is there a delay period, is a lockout situation imposed after repeated false attempts? If so, what is the recovery mechanism?
ISO/IEC 17799, Clause 9.5.2 provides some examples of good logon practices. Sometimes an application may not provide the necessary level of logon protection - for example if the number of unsuccessful logons is not restricted. In this situation determine if any other controls have been added - for example by physically restricting access to the terminal. The risk assessment should have considered each system and application, the access methods and whether these are considered adequate - check for this.

2.7.5.2 User identification and authentication (BS 7799-2 - cl. A.9.5.3)

ALL USERS SHALL HAVE A UNIQUE IDENTIFIER (USER ID) FOR THEIR PERSONAL AND SOLE USE SO THAT ACTIVITIES CAN BE TRACED TO THE RESPONSIBLE INDIVIDUAL. A SUITABLE AUTHENTICATION TECHNIQUE SHALL BE CHOSEN TO SUBSTANTIATE THE CLAIMED IDENTITY OF A USER.

Implementation guidance:
The sharing of user IDs creates an especially risky vulnerability leading to problems with confidentiality, integrity and availability and loss of accountability. All users should be accountable for all actions carried out using their unique user ID.
It is sometimes necessary for the system operators or database managers to use a particular user ID. Their use should be authorized and strictly controlled with clear allocation of responsibility for their use, e.g. for the period of a shift. Systems should keep a log of the actions carried out under such user IDs.
In such exceptional circumstances the risk assessment should be used to analyse the situation and to identify the appropriate identification and authentication technique. Additional controls may be required to maintain accountability.

Auditing guidance:
The term ‘user’ should be taken to include all users of information processing facilities including system administrators, managers and application users. Check to see if user ID’s are unique or if are they shared. If shared, why is this necessary, look at the management and authorisation for this? For critical functions, such as system administration, there should be a special user ID assigned solely for this purpose and some logging of both the time and person initiating the event. Look for where these logs are required; how long are they kept, can they be modified, when and under what circumstances are they reviewed? If the application does not provide this traceability, look to see what other controls have been applied.
It should be considered whether the authentication procedures used by the organization provide sufficient security for the information, systems and applications they are supposed to protect. The use of passwords alone is not generally appropriate for high risk situations. The risk assessment should have been used to identify the appropriate user identification and authentication procedure.

2.7.5.3 Password management system (BS 7799-2 - cl. A.9.5.4)

PASSWORD MANAGEMENT SYSTEMS SHALL PROVIDE AN EFFECTIVE, INTERACTIVE FACILITY WHICH AIMS TO ENSURE QUALITY PASSWORDS.

(More about passwords can also be found above in sections. 2.7.2.3 and 2.7.3.1.)

Implementation guidance:
Weak password management leads to vulnerability to misuse of systems by unauthorized persons, with the attendant risk of breaches of confidentiality, loss of integrity and availability of data. Where systems provide automatic controls over password quality and frequency of change, these should be used. Compensating controls and monitoring may be required elsewhere.

ISO/IEC 17799 contains guidelines for users for allocating and managing their passwords (see ISO/IEC 17799, Clauses 9.3.1 and 9.5.4).

Auditing guidance:
There should be some overall policy covering the use of passwords throughout the organization. Any additional requirements for particularly sensitive areas should be additional to and consistent with this policy where possible. Aspects that auditors should check for include:

- length and make-up of passwords;
- frequency of changing passwords;
- use of common passwords between individuals and access applications;
- secure handling and storage of passwords;
- changing of default passwords.

Additional controls are included in ISO/IEC 17799, Clause 9.5.4. Look also at the process for changing of passwords, what logs are kept, are old passwords disallowed, does the application require verification before accepting a new password - e.g. double entry? If necessary get users to demonstrate how passwords are changed.

2.7.5.4 Use of system utilities (BS 7799-2 - cl. A.9.5.5)

USE OF SYSTEM UTILITY PROGRAMS SHALL BE RESTRICTED AND TIGHTLY CONTROLLED.

Implementation guidance:
System utilities provide a high vulnerability to misuse, which can damage the integrity of the security control of a system. Utilities often circumvent the security of the system - they are often needed when control problems arise.

It is essential that all system utilities are identified, risk assessed and brought under tight control. Their use should be authorized and monitored, as described in ISO/IEC 17799, Clause 9.5.5.

Auditing guidance:
Some utilities allow access to parts of the system that applications do not, and might also allow overriding of system controls. Auditors should first establish that organizations have overall control on the utilities installed, check that they are known and authorised for use, and that appropriate access control and use restrictions are applied. Check on individual systems that no additional or modified utilities are installed.

In less well regulated environments shareware utilities may have been installed which could have consequences for not only the confidentiality of information but also its integrity and availability. Check also that no forgotten utilities are still resident on systems that should have been removed. Finally check that nobody without appropriate authorisation can access or use system utilities. Further controls to secure the use of system utilities are provided in ISO/IEC 17799, clause 9.5.5.

2.7.5.5 Duress alarm to safeguard users (BS 7799-2 - cl. A.9.5.6)

DURESS ALARMS SHALL BE PROVIDED FOR USERS WHO MIGHT BE THE TARGET OF COERCION.

Implementation guidance:
This control will not be applicable in all cases. There is a risk that staff that work with sensitive or valuable information might become a target for coercion, particularly if they are also accessible to potential assailants. Risk assessment should consider this and identify the circumstances where it could be relevant.

A duress alarm is a mechanism by which the user can indicate that they are under duress. For example, the use of an alternative password; the substitution or inclusion of special characters in a password could be used to trigger the alarm at a system monitoring point; where a PIN code is used, use of a special alarm code. More traditional alarms could also be considered, e.g. triggered by a button under the desk.

There should be defined responsibilities and procedures for responding to a duress alarm. These should be simple enough to enable first response from memory without having to resort to written procedures. Staff should be trained to handle both sides of the situation.

Auditing guidance:
Where the organization has identified the need for duress alarms, the auditor should first establish that the provision adequately covers the requirement, for example, are sufficient points covered, are the alarms raised in appropriate locations, can they be disabled?

The initiation of an alarm should be simple but not so simple as to cause false alarms. The alarms may be physical actuators such as emergency pushes or perhaps the entry of a specific code into an application. Some alarms may need to be raised covertly so as not to endanger personnel.

Look also at the procedures for dealing with alarms, responsibilities and defined actions that should be specifically defined. The initial actions should be easily understood and immediately, if necessary, and here the auditor should check that appropriate personnel know what to do without having to resort to the written documents, at least for the initial responses.

2.7.5.6 Terminal time-out and limitation of connection time (BS 7799-2 - cl. A.9.5.7 & cl. A.9.5.8)

INACTIVE TERMINALS IN HIGH RISK LOCATIONS OR SERVING HIGH RISK SYSTEMS SHALL SHUT DOWN AFTER A DEFINED PERIOD OF INACTIVITY TO PREVENT ACCESS BY UNAUTHORIZED PERSONS.

RESTRICTIONS ON CONNECTION TIMES SHALL BE USED TO PROVIDE ADDITIONAL SECURITY FOR HIGH-RISK APPLICATIONS.

Implementation guidance:
An unattended terminal, logged on to a service, is vulnerable to misuse providing concerns for confidentiality, integrity and availability. Risk assessment should determine the maximum time a terminal can be left before it is automatically disabled. The capability of the system will determine whether the service is dynamically logged off or whether the limited form of terminal time-out facility provided by some PCs is used. This latter clears the screen to a screen saver, hiding the user's work, and prevents unauthorized access, but does not close down the application or network sessions. Properly evaluate these types of system before relying on them.

Vulnerability to misuse can be limited by reducing the time when a system is available to the user. A typical example in use would be where a file has to be regularly transmitted from a high risk connection. The connection can be scheduled for the task and otherwise disabled. Network firewalls can also provide this kind of control. Such particularly high risk applications should be determined by risk assessment.

Auditing guidance:
Timeouts from specific terminals should be considered where any public access or access from less security cleared personnel is possible. Look at where this has been defined, and determine whether the periods allocated are sufficient given the access level, the vulnerability and the operational needs. Determine what the timeout is based on, specific use of the application or simply movements of a mouse cursor. Check that this timeout is employed consistently at all locations under high risk - particular public offices may have a number of terminals requiring this protection - check that they all work. Where timeouts rely on operating system features such as Windows screen saver, check that the facility is not disabled and of course check that password use is as per policy.

Some applications may, in addition to inactive timeouts, employ time restrictions on connections. Restrictions on the connection time should be applied for high risk applications. Again, determine where these are applied, that the use is consistent with requirements and that the timeouts cannot be circumvented, for example, by leaving a particular transaction half completed.

2.7.6 Application access control (BS 7799-2 - cl. A.9.6)

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

ISO/IEC 17799 extension: Security facilities should be used to restrict access within application systems.

Logical access to software and information should be restricted to authorized users. Application systems should:

a) control user access to information and application system functions, in accordance with a defined business access control policy;

b) provide protection from unauthorized access for any utility and operating system software that is capable of overriding system or application controls;

c) not compromise the security of other systems with which information resources are shared;

d) be able to provide access to information to the owner only, other nominated authorized individuals, or defined groups of users.

2.7.6.1 Information access restriction (BS 7799-2 - cl. A.9.6.1)

ACCESS TO INFORMATION AND APPLICATION SYSTEM FUNCTIONS SHALL BE RESTRICTED IN ACCORDANCE WITH THE ACCESS CONTROL POLICY.

Implementation guidance:
The business owner of an application and its related data should develop a policy, which defines who will have access and, in the case of data, at what level, e.g. read, write, delete. Without this there is a serious risk that users will be given too high a level of access to too much data and this brings risks of breach of confidentiality and loss of integrity. Over accessibility can lead to the practical possibility of fraud in financial applications.

Be particularly cautious where a shared database is used. Ensure that each group of users can only access the data relevant to its business.

Access and the related levels should be reviewed periodically in order to eliminate excesses.

Auditing guidance:
Auditors should first ensure that access to information provided by individual applications matches the business requirements and takes place in line with the access control policy (see also Section 2.7.1). For example, different applications may access the same database, can sensitive information be accessed from one program that is restricted in another?

In many cases users should not be aware of information or application functions they are not allowed to access, so menu options that are not accessible for security reasons should be avoided; likewise user manuals. Pay particular attention to little used parts of applications, such as maintenance utilities, are these properly controlled?

Look also at what happens to information that is accessible, do users have read and write ability - is this necessary, are there restrictions to its output? Print options on networked systems may be to share devices physically removed from the operators, how is this controlled? It should be ensured that information is protected in line with the classification scheme.

2.7.6.2 Sensitive system isolation (BS 7799-2 - cl. A.9.6.2)

SENSITIVE SYSTEMS SHALL HAVE A DEDICATED (ISOLATED) COMPUTING ENVIRONMENT.

Implementation guidance:
Risk assessment will identify systems that are just so sensitive that they must be isolated in a dedicated computing environment. Such systems will include those where the normal vulnerabilities to unauthorized access must be reduced to as near zero as is possible, consistent with still being able to operate the system.

System documentation, including the risk assessment, is a part of the sensitive system and should be secured in an appropriate manner. In view of the increased cost of isolation, an appropriate level of authorization should be obtained against a proper justification.

Auditing guidance:
Where highly sensitive information is handled it may be necessary to introduce a degree of isolation. This needs to be identified by the organization and the appropriate considerations in terms of security, accessibility and operational use considered. The system may have high security requirements so that total isolation is required, or alternatively links to other systems is via some dedicated secure port.

Apart from the normal procedures and definitions, look to see that these systems are identified in the risk assessment and a suitable case made for its isolation – tight access control might conflict with business requirements for the use, check to see that the right balance is achieved. If a dedicated system is required, look at contingency arrangements should that system fail, what restrictions there are for inputting data or programs from media and what back-ups are taken.

2.7.7 Monitoring system access and use (BS 7799-2 - cl. A.9.7)

Objective: To detect unauthorized activities.

ISO/IEC 17799 extension: Systems should be monitored to detect deviation from access control policy and record monitorable events to provide evidence in case of security incidents.
System monitoring allows the effectiveness of controls adopted to be checked and conformity to an access policy model (see 9.1) to be verified.

2.7.7.1 Event logging (BS 7799-2 - cl. A.9.7.1)

AUDIT LOGS RECORDING EXCEPTIONS AND OTHER SECURITY-RELEVANT EVENTS SHALL BE PRODUCED AND KEPT FOR AN AGREED PERIOD TO ASSIST IN FUTURE INVESTIGATIONS AND ACCESS CONTROL MONITORING.

Implementation guidance:
Audit trails are an essential pre-requisite to investigating what went wrong. They are often necessary to establish the events leading up to an incident as well as to determine the indisputable accountability for an incident.
Logging policy should be determined by an appropriate level of management. Some systems can produce very large logs covering a wide range of activities within the system. Generally such a mass of data is difficult to monitor in a way that is likely to provide value when trying to identify possible misuse. An analysis of monitoring requirements (see Section 2.7.7.2 below) should be made and the result used to manage the log information to be collected.
At a minimum logs should record the user ID, activity, date and time, location (network address) and the result, e.g. access denied. Logs should be kept for sufficient time in case they may be needed for an investigation. They should also be protected in their own right, particularly against unauthorized modification designed to cover up other unauthorized activity.

Auditing guidance:
For all systems processing information there should be some form of audit log kept which is independent of and not accessible by the user. Auditors need to determine where this is appropriate for the security requirements and to investigate the organization’s approach. Check that all records that are being required to be kept because of record retention policy, or in order to collect evidence are properly archived (see also 2.10.1.3). What is recorded?
As a minimum this should identify the event, the person causing the event, changes made if appropriate, the date and time; in addition transaction codes and terminal ID may also be needed. Determine what constitutes an event, ensure the exceptions are included. Determine how long this information is required to be held, in what form and under what protection - verify these. Example events include changes made by system administrators and failed logins or access attempts.

2.7.7.2 Monitoring system use (BS 7799-2 - cl. A.9.7.2)

PROCEDURES FOR MONITORING USE OF INFORMATION PROCESSING FACILITIES SHALL BE ESTABLISHED AND THE RESULT OF THE MONITORING ACTIVITIES REVIEWED REGULARLY.

Implementation guidance:
Monitoring is the means by which we confirm the effectiveness of other controls. Satisfactory monitoring provides a measure of assurance (but not certainty) that the system is secure. ISO/IEC 17799, Clause 9.7.2 describes examples of what could be monitored, depending on the security requirements of the information system considered.

The level, type and frequency of monitoring will depend on the sensitivities of the system and should be established from the risk assessment. The handling and storage of the log files should ensure that no unauthorised modifications or deletions could be made.

Automated procedures and appropriate tools are recommended in order to highlight the truly significant items from the mass of logging information.

Auditing guidance:
Monitoring involves checking security event logs for signs of abnormal activities. The risk assessment performed should indicate where and what monitoring needs to be applied. Examples may include:

- false access attempts;
- abnormal value assigned to data values;
- attempts to change restricted data items;
- excessive use of certain data;
- invalid entries in event logs;
- access with rarely used or redundant user ID's.

As before check how these records are maintained and ensure that they cannot be modified or deleted. The auditors should check what provisions the organization has in place to ensure segregation of duties between the reviewing activities and the activities that are reviewed to ensure correct results.

A check should be made on how often the logs are reviewed – the higher the related security risks are, the more frequently the logs should be reviewed. This check should also made to ensure that the review process itself is effective and efficient.

The logs produced by a system or event logging process can easily result in large volumes of data. Subsequently this might result in important audit information related to security relevant incidents getting lost in a mass of other less important data. Therefore, tools should be used to filter audit logs with filter rules designed to ensure that all relevant incidents and activities are recognised by such filters. The auditor should inquire about the use and adoption of such tools and to review how these tools are applied to detect and react to incidents.

2.7.7.3 Clock synchronization (BS 7799-2 - cl. A.9.7.3)

COMPUTER CLOCKS SHALL BE SYNCHRONIZED FOR ACCURATE RECORDING.

Implementation guidance:
Most output from computers and communications equipment is time and date stamped. This information will form part of the audit trail for transactions moving between computers. It may also be required in investigations or to resolve disputes and should therefore be accurate. Radio receivers are available that will provide a computer with the atomic clock signal and maintain accuracy every second.

Auditing guidance:
Without proper timing across all systems, event logging can be inaccurate and hence compromised. The organization needs to establish what the base time is, for most this will be

local time but for international organizations some other base may be used, e.g. GMT. There should be some facility to monitor system clocks and correct them, if necessary.

Look at how the transitions to and from summer daylight saving is made. Are any additional checks made when portable systems log into the network? Event logging will rely on accurate system clocks, modified system time could be used to falsify records, check for restrictions on clock access. Don't forget also wall clocks, which may be used for any manual logging, e.g. goods received, incident reports.

2.7.8 Mobile computing and teleworking (BS 7799-2 - cl. A.9.8)

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

ISO/IEC 17799 extension: The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangement are in place for this way of working.

2.7.8.1 Mobile computing (BS 7799-2 - cl. A.9.8.1)

A FORMAL POLICY SHALL BE IN PLACE AND APPROPRIATE CONTROLS SHALL BE ADOPTED TO PROTECT AGAINST THE RISKS OF WORKING WITH MOBILE COMPUTING FACILITIES, IN PARTICULAR IN UNPROTECTED ENVIRONMENTS.

Implementation guidance:

In most cases, the use of mobile computing facilities is taking place outside of the organization, e.g. in airports, planes or trains when travelling; during conferences and meetings; or with customers at their organization or home. There are many additional risks to mobile equipment that result from this way of working.

Employees using mobile equipment should be aware of these risks and should adapt their behaviour to this situation. The organization should develop a mobile computing policy describing the controls that should be in place, and employees should only be allowed to use mobile computing facilities after they received the policy and sufficient training and awareness education.

Other security risks when using mobile computing facilities are related to information exchange. Because of the high amount of data transfer that might take place, effective and frequently updated virus protection and back-ups should be used. In case of remote connections to the organization's site, authentication not only for the machine but also for the authorized user should be in place, to avoid such connections to be made e.g. by somebody that has stolen a laptop.

ISO/IEC 17799 describes in Clause 9.8.1 a number of controls that can be applied to protect information and facilities used in mobile computing.

Auditing guidance:

The use of all mobile computing devices and equipment should be identified by the organization; this includes the use of mobile phones, and the use of laptops, notebooks or palmtops outside the organization's premises (e.g. at home, customer sites, hotels or at conference venues) and any remote connections to the organization's internal information processing facilities using such devices. Since such devices and equipment are generally used and mobile computing activities take place outside the organization, their use will be normally difficult to directly audit.

It is therefore particularly important to look closely at the controls, rules and procedures that the organization has in place to ensure that such devices are used in a secure way. This includes the controls that should be implemented to physically protect such devices. User training and awareness, authorization processes and security arrangements for using such devices should be in place as described in ISO/IEC 17799, Clause 9.8.1.

Checks should be made that all these controls are implemented correctly. Checks for controls should include what the policy says about password and virus protection on mobile computers? Check that there are sufficient controls in place to secure remote access, and that cryptographic controls are applied where necessary.

2.7.8.2 Teleworking (BS 7799-2 - cl. A.9.8.2)

POLICIES PROCEDURES AND STANDARDS SHALL BE DEVELOPED TO AUTHORIZE AND CONTROL TELEWORKING ACTIVITIES.

Implementation guidance:

As in the mobile computing environment, the main security problems with teleworking arise from the location where this work is taking place. The employee's home does not normally have the same level of physical security, and the work area is often easily accessible by family members and visitors. In order to reduce these risks, teleworking should only take place after the organization has developed appropriate policies and procedures, has put in physical controls to secure the work area and has raised the awareness of the employee doing teleworking sufficiently to control the physical and logical access to the information processing facilities used for the teleworking activities.

The connections between the organization's site and the teleworking facilities should be secured to ensure that information cannot be destroyed, damaged, compromised or modified and the information that is accessible remotely should be restricted to a minimum.

ISO/IEC 17799, Clause 9.8.2 contains a detailed list of actions the organization should take prior to authorizing any teleworking activities.

Auditing guidance:

Teleworking activities should only be authorized if sufficient controls are in place, including physical controls, access control and the security of the remote connection. The homeworking equipment should be included in the asset register. There needs to be some mechanism for establishing and controlling what information is transmitted to, from and used at home.

There should be some defined policy on the use of the equipment for other activities such as games software, accessing the Internet etc., any of which can introduce problems when allowed to interfere with sensitive data. Check that the controls in ISO/IEC 17799, Clause 9.8.2 are implemented to sufficiently secure the teleworking environment.

2.8 Systems development and maintenance (BS 7799-2 - cl. A.10)

2.8.1 Security requirements of systems (BS 7799-2 - cl. A.10.1)

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

ISO/IEC 17799 extension: This will include infrastructure, business applications and user-developed applications. The design and implementation of the business process supporting the application or service can be crucial for security. Security requirements should be identified and agreed prior to the development of information systems.

All security requirements, including the need for fallback arrangements, should be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an information system.

2.8.1.1 Security requirements analysis and specification (BS 7799-2 - cl. A.10.1.1)

BUSINESS REQUIREMENTS FOR NEW SYSTEMS, OR ENHANCEMENTS TO EXISTING SYSTEMS SHALL SPECIFY THE REQUIREMENTS FOR CONTROLS.

Implementation guidance:
Security vulnerabilities should be recognized from the first stages of systems development and the requirements for security specified along with the functional requirements. Requirements analysis procedures should contain reference to establishing security requirements using a risk assessment.
ISO/IEC 17799, Clause 10.1.1 contains a useful list of specific subjects to consider.

Auditing guidance:
Organizations should be able to demonstrate that the security requirements have been identified and taken into account for the development of applications, new systems, enhancements and upgrades to systems. This really falls into two categories, those where bespoke applications software is developed either specifically for or by the organization or where commercial off the shelf (COTS) software is acquired for use in a secure environment. (Note that COTS software may comprise the entire application or a component, which is built into it.)
The initial analysis of requirements needs to identify security issues and these shown to be considered in the application user requirements documents for new systems and/or evaluation report. Having established this the auditor should look to see how these requirements are monitored and reviewed during system development and installation. Any identified deficiencies need to be analysed, raised at the appropriate management level and satisfactorily resolved.

2.8.2 Security in application systems (BS 7799-2 - cl. A.10.2)

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

ISO/IEC 17799 extension: Appropriate controls and audit trails or activity logs should be designed into application systems, including user written applications. These should include the validation of input data, internal processing and output data. Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical organizational assets. Such controls should be determined on the basis of security requirements and risk assessment.

2.8.2.1 Input data validation and control of internal processing (BS 7799-2 - cl. A.10.2.1 & cl. A.10.2.2)

DATA INPUT TO APPLICATION SYSTEMS SHALL BE VALIDATED TO ENSURE THAT IT IS CORRECT AND APPROPRIATE.
VALIDATION CHECKS SHALL BE INCORPORATED INTO SYSTEMS TO DETECT ANY CORRUPTION OF THE DATA PROCESSED.

Implementation guidance:
Applications are vulnerable to the deliberate or accidental input of invalid data. This can lead to integrity and availability problems, in addition to when systems fail, data becomes

corrupted or crimes such as fraud are perpetrated through loopholes. Appropriate validation controls should be implemented to restrict the input to known or reasonable limits, which must be within the processing capabilities of the system to be effective.

The data inside an application can be seriously compromised by faulty programs or by deliberate programming changes. This can lead to a loss of integrity and availability in systems wherever the data is subsequently used. Opportunities for fraudulent misuse may be exposed to application users. There should be control checks at strategic points throughout an application designed to confirm that the results so far obtained are true and correct.

Risk assessment should identify danger spots, and appropriate processing controls should be selected to safeguard them.

Auditing guidance:

The application should be providing the appropriate level of data integrity checking, both at the input stage and also when data are processed. Where data is entered manually the auditor should check to ensure that obviously incorrect values such as out-of-range, invalid characters and incomplete data are rejected. Where data is supplied in hard copy form, (to then be typed in by operators), look to see what validation is done of this information - can the documents be accessed by unauthorised personnel? If changes are evident, are these checked and authorised? If data input is via other media, such as tape or disk, check that these are properly marked and again, cannot be tampered with before use.

Once the data have been entered into the system, corruption might take place because of system errors or deliberate modification. Establish from design documentation what other integrity checks are performed - check that these comply with requirements and if possible exercise them. The design of the system should minimise the risks of data being corrupted, and checks should be in place to detect any corruption. ISO/IEC 17799, clauses 10.1.1 and 10.1.2 give examples of integrity checks that can be performed for data input and control of internal processing.

2.8.2.2 Message authentication (BS 7799-2 - cl. A.10.2.3)

MESSAGE AUTHENTICATION SHALL BE USED FOR APPLICATIONS WHERE THERE IS A SECURITY REQUIREMENT TO PROTECT THE INTEGRITY OF THE MESSAGE CONTENT.

Implementation guidance:

Message authentication, or electronic signature, is a means of providing assurance that the message is certainly from the person it claims to be from and that it has arrived without any change having been made during transmission.

The organization may need confirmation that data, such as instructions to carry out financial transactions, is actually a genuine request. Failure to confirm could result in loss of integrity and fraud. The risk assessment of transaction systems should show the risks being faced and message authentication should be considered in appropriate cases. This technology is changing rapidly and expert advice should be obtained.

Auditing guidance:

Auditors should inquire whether message authentication is being applied by the organization and if so, to review whether the mechanisms used is appropriate. The organization should have carried out a risk assessment to identify the risks to find out whether message authentication is needed to protect the integrity of the message content and if so the most appropriate form of implementation. In reviewing the mechanisms used the auditor needs to take account of the results of the risk assessment. Examples where message authentication might be appropriate include:

- exchange of documents and messages as a part of some electronic commerce or trading activity;
- exchanges of email messages and/or file attachments; and
- any other application where it is important or critical that the content of the message should not be altered.

2.8.2.3 Output data validation (BS 7799-2 - cl. A.10.2.4)

DATA OUTPUT FROM AN APPLICATION SYSTEM SHALL BE VALIDATED TO ENSURE THAT THE PROCESSING OF STORED INFORMATION IS CORRECT AND APPROPRIATE TO THE CIRCUMSTANCES.

Implementation guidance:
Despite correct input and processing of data, the output might still contain errors or unwanted modifications. Therefore, output validation should be applied to ensure that output data are reasonable, accurate and complete. Care should be taken that classification labels are not modified or destroyed. ISO/IEC 17799, Clause 10.2.4 provides a list of possible output validation checks.

Auditing guidance:
The application system should provide accurate outputs, and the organization should have procedures in place to test the accuracy of outputs, and to respond to any incorrect or incomplete outputs. Auditors should take part in such an output validation test to ensure that employees are familiar with such procedures, look for possible incompleteness of, or possibilities to circumvent, these procedures. They should also check that persons responsible are identified and that they are aware of their responsibilities. Once output validation tests have been completed, it should be ensured that they cannot be modified in an unauthorized way. ISO/IEC 17799, Clause 10.2.4 includes output validation checks that can be applied by an organization.

2.8.3 Cryptographic controls (BS 7799-2 - cl. A.10.3)

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

ISO/IEC 17799 extension: Cryptographic systems and techniques should be used for the protection of information that is considered at risk and for which other controls do not provide adequate protection.

2.8.3.1 Policy on the use of cryptographic controls (BS 7799-2 - cl. A.10.3.1)

A POLICY ON THE USE OF CRYPTOGRAPHIC CONTROLS FOR THE PROTECTION OF INFORMATION SHALL BE DEVELOPED.

Implementation guidance:
The effective use of cryptographic techniques is only possible if some basic principles are identified, agreed and applied organization-wide. For example, the algorithms used should be suitable for the business processes and services they are supporting, the key length should be appropriate for the security requirements of the information that will be protected, and the solutions implemented should be consistent throughout the whole organization.
In order to achieve this, a risk assessment should be used to determine the most suitable solutions and a policy on the use of cryptographic controls should be communicated to all users of such controls prior to any application. This policy should take into account the

relevant key management activities (see also Section 2.8.3.5) and legal issues involved in the use of cryptographic techniques.

For example, the organization might want to retain copies of the employee's encryption keys to avoid any misuse, such as the unauthorized distribution of the organization's information or disgruntled employee first encrypting information and then destroying the encryption key.

Auditing guidance:

An important aspect of the secure and effective use of cryptographic controls is to make sure that the right decisions have been made about what mechanisms to use and to have a policy in place supporting the day-to-day use of these controls. This policy should cover the key management approach applied (see ISO/IEC 17799, clause 10.3.5 and below), the roles and responsibilities related to the use of cryptographic controls, and the information and circumstances for which cryptographic controls should be applied.

If the organization applies cryptographic controls auditors should check that a policy on the use of cryptographic controls has been developed, communicated, and is known and followed by employees. They should question whether the decisions that have been made are supported by the results of a risk assessment, and that the controls used are commensurate with this policy.

The strength of cryptographic controls does vary and is related to the algorithms employed and the key sizes and parameters used. A factor to be taken into account is the environment and application in which cryptographic controls are applied. Some application environments may require the use of stronger cryptographic controls.

Therefore, auditors will need to have at least a general knowledge of cryptographic techniques and mechanisms, key management and their application to assess whether what the organization is using is adequate or appropriate.

2.8.3.2 Encryption, digital signatures and non-repudiation services (BS 7799-2 - cl. A.10.3.2, A.10.3.3 & A.10.3.4)

ENCRYPTION SHALL BE APPLIED TO PROTECT THE CONFIDENTIALITY OF SENSITIVE OR CRITICAL INFORMATION.

DIGITAL SIGNATURES SHALL BE APPLIED TO PROTECT THE AUTHENTICITY AND INTEGRITY OF ELECTRONIC INFORMATION.

NON-REPUDIATION SERVICES SHALL BE USED TO RESOLVE DISPUTES ABOUT OCCURRENCE OR NON-OCCURRENCE OF AN EVENT OR ACTION.

Implementation guidance:

Risk assessment should be used to highlight those, probably few, data files or transmissions whose unauthorized exposure would have serious adverse consequences for the organization. The two principle uses for encryption are:

- transactions while being transmitted through open and public networks;
- sensitive data held on portable PCs.

Encryption should be applied with careful consideration. It's management requirements, particularly for keys, are complex and will provide their own risks.

The use of encryption algorithms might be controlled by government, depending on the legislation in the country(s) involved. The permissibility of use should be established for the purposes and locations intended.

Expert advice should be obtained to identify the right strength and appropriate key length when using encryption algorithms.

Digital signatures can be used to secure electronic commerce and other payment information, to electronically sign contracts and do any other way of electronic trading. One important aspect of the use of digital signatures is the possibility of having legal recognition of such a signature, similar to a hand-written signature.

Therefore, an organization should carefully identify the legal situation and investigate what is necessary to comply with such legislation, and whether the efforts and investments related to that are appropriate for the business processes where the signatures will be used.

As with any other cryptographic control, protection and key management of the public and the private keys used for digital signatures should be in place. The private keys need to be protected from unauthorized disclosure, but nevertheless the organization might still want to retain copies of those keys, if that is possible in the legal environment considered. The certification and management of the public keys might best be carried out by a well recognized certification authority, to achieve easy verification of the integrity of the public key by communication partners.

Non-repudiation services can support business processes and collection of evidence (see also 2.10.1.7) about actions that have taken place. There are different forms of non-repudiation services, like non-repudiation of sending or of receiving a message. A risk assessment should be used to identify those non-repudiation services that are most suitable for the business processes where they will be applied.

Key management is important for all cryptographic services (see also Section 2.8.3.3 below).

Auditing guidance:

Auditors should check the conditions under which encryption, digital signatures and/or non-repudiation services are used, and whether these are in line with the policy and the identified security and business requirements. In addition, they should review whether:

- a risk assessment has been used to decide whether to use encryption, digital signatures and/or non-repudiation, and to determine the exact protection requirements,
- appropriate algorithms and suitable key length have been chosen commensurate with the identified protection requirements and the results of the risk assessment,
- any existing legislation, including export and import rules and procedures relating to the use and application of cryptographic mechanisms have been identified and are complied with (see also ISO/IEC 17799, clause 12.1.6, Regulation of cryptographic controls),
- an appropriate key management system is in place to protect the keys and which will allow their secure handling and use (see ISO/IEC 17799, clause 10.3.5 and below for further details).

Auditors should inquire and investigate as to whether employees are aware of the policy, rules for cryptographic controls, and when to use them and when not, e.g. by an auditor observing the use of a cryptographic control.

2.8.3.3 Key management (BS 7799-2 - cl. A.10.3.5)

A KEY MANAGEMENT SYSTEM BASED ON AN AGREED SET OF STANDARDS, PROCEDURES AND METHODS SHALL BE USED TO SUPPORT THE USE OF CRYPTOGRAPHIC TECHNIQUES.

Implementation guidance:

The key management system used should provide protection of the cryptographic keys according to their use, and management methods that support the handling and use of keys as required by the business processes for which the cryptographic controls will be used.

The requirements for key management will be different depending on which cryptographic technique, secret or public key technique, will be used and what type of key, public or private, is considered. The protection of secret and private cryptographic keys is different from the protection necessary for the public keys. When defining a key management system, these protection requirements should be analyzed with help of a risk assessment and appropriate protection should be in place before the first keys are generated and used.

A set of standards and procedures for the key management activities as described in ISO/IEC 17799, Control 10.3.5, should be agreed and implemented before using cryptographic controls. The lifetime of cryptographic keys should be defined for each application in relation to the risks of and possible damage if they are compromised, and the deactivation of keys should take place immediately when this time period is finished.

The organization should also consider its needs for keeping copies of keys or parts of keys used for cryptographic controls, either for their own use or to satisfy legal requirements. It might be necessary to agree with certification authorities details about the management of public keys, and the organization might also want to consider the use of other services like key generation, distribution and revocation, directory services or time stamping, offered by third party organizations.

Auditing guidance:

Key management is an essential pre-requisite for the secure use of cryptographic controls, and no cryptography should be used without a secure key management system in place. Auditors should check that the organization has implemented adequate controls to protect:

- secret and private keys against disclosure, modification and destruction,
- public keys and public-key certificates against unauthorized modification and destruction; if the organization is using a certification authority (public or internal) for the management of their public keys, it should be ensured that this certification authority is adequately protected, trustworthy and suitably managed.

The protection of cryptographic keys should encompass both logical and physical protection. Auditors should review the physical and logical access controls that are being applied to protect cryptographic keys.

In addition, they should check that the other key management procedures as described in ISO/IEC 17799 clause 10.3.5, are in place. If a key escrow or key recovery mechanism or process is applied to cryptographic keys, it should be ensured that the employees are aware of that, and that there are no possibilities to circumvent key escrow.

2.8.4 Security of system files (BS 7799-2 - cl. A.10.4)

Objective: To ensure that IT projects and support activities are conducted in a secure manner. Access to system files should be controlled.

ISO/IEC 17799 extension: Maintaining system integrity should be the responsibility of the user function or development group to whom the application system or software belongs.

2.8.4.1 Control of operational software (BS 7799-2 - cl. A.10.4.1)

PROCEDURES SHALL BE IN PLACE TO CONTROL THE IMPLEMENTATION OF SOFTWARE ON OPERATIONAL SYSTEMS.

Implementation guidance:

The organization is vulnerable to the installation of unauthorized software and unauthorized changes to software with a resulting loss of system and data integrity. Controls are necessary to reduce the risk of system failure and the possibility of fraud. All software

updates should be subjected to change control and authorized prior to implementation. Back-ups of old configurations should be retained to be equipped for the case of failure of the new system.
New products should be obtained against a business requirement and appropriately authorized. Ensure that valid licences are provided to cover the extent of use intended.

Auditing guidance:
Auditors should check the controls applied for the implementation of software on operational systems - how is the code held on the system, is source code included, how are new versions introduced, how are system files and libraries protected, what records are kept of changes? Developers and maintenance staff need to be aware of the potential dangers of introducing untested or of allowing unauthorised code onto operational systems, check that this awareness exists.
Next, look at the implementation - what protection is applied to source and object code, what testing stages have to be completed before new or modified code is introduced, is regression testing adequate, can previous issues of code be reinstalled, are full data back-ups performed before changes?
Look at the records of changes to operational code, are they complete, sufficiently descriptive and show proper authorisation? Complex or critical operations may require carefully thought out and detailed plans for the introduction of new or modified code, look for examples of this.

2.8.4.2 Protection of system test data (BS 7799-2 - cl. A.10.4.2)

TEST DATA SHALL BE PROTECTED AND CONTROLLED.

Implementation guidance:
Test data should normally be fictitious but there are occasions when operational or depersonalised operational data is used. The organization is vulnerable to breaches of confidentiality when such data is used and it should be controlled and protected to at least the same extent as operational data.
The use of operational data should be recognized in risk assessments and the higher security requirements noted in test plans. Each use should be authorized.

Auditing guidance:
Auditors need to ensure that data used for testing is properly controlled. Tests should be reproducible and so the data used should be distinct and available for any re-testing. Use of live data for testing is discouraged and if used it should be modified to remove any personal or otherwise sensitive information. This is not always completely possible - or not possible to completely assure - so check how this and any results of the testing, both data files and recorded results, are protected.
Use of live data for testing should be properly authorised - on each occasion - check that this is done. Check also that there is a method to completely remove any data put into live databases during testing, and the access control in place. Access to test application systems should be as tightly controlled as the access to operational systems is.

2.8.4.3 Access to program source library (BS 7799-2 - cl. A.10.4.3)

STRICT CONTROL SHALL BE MAINTAINED OVER ACCESS TO PROGRAM SOURCE LIBRARIES.

Implementation guidance:
The program source library is the repository of the operational system. It contains every detail on how the system and its controls are implemented. It provides a perfect starting

point for unauthorized modification of the system. Serious security problems can result from unauthorized and uncontrolled access to a library.

Strong procedures are required to ensure proper maintenance and protection of the program source libraries. These should include logging of copies sent, after authorization, to maintenance staff and the subsequent updates.

Auditing guidance:

Access to any source code files should be protected, best by not holding it on operational systems. Access to such code and the means to re-compile and re-link it may effectively bypass all of the security features normally imposed by the application. Highly secure applications may need to provide some means of verifying object code check sums to identify whether changes have been made.

Consider also macros and database report programs that may be much easier to change and could cause loss of integrity or make information unavailable. Such restrictions should not be limited to potential malicious incidents, normal update and re-introduction of application source code needs to be properly controlled to ensure recording and testing of changes before access to live and vulnerable data is permitted. Auditors need to look for these documented procedures and records.

ISO/IEC 17799, clause 10.4.3 provides additional controls that should be applied to secure access to program source libraries.

2.8.5 Security in development and support processes (BS 7799-2 - cl. A.10.5)

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

ISO/IEC 17799 extension: Project and support environments should be strictly controlled. Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

2.8.5.1 Change control procedures (BS 7799-2 - cl. A.10.5.1)

THE IMPLEMENTATION OF CHANGES SHALL BE STRICTLY CONTROLLED BY THE USE OF FORMAL CHANGE CONTROL PRODECURES.

Implementation guidance:

A system is always vulnerable to changes - even fully authorized changes can have damaging effects. There are risks of loss of data integrity, application unavailability, and possibly exposure of confidential information.

Formal control and co-ordination of all changes should be implemented together with business and technical authorization for each change at all stages of development - requirements, design, code, test, operational implementation. Changes should be planned and prepared with appropriate testing and review. Code changes to sensitive applications should be checked by a second person. Final testing should be signed off by the business as their authority to implement the change operationally.

Auditing guidance:

Auditors should check that formal change control procedures are in place for all changes made to applications in the operating and system environment. These procedures may need to be in quality plans rather than standard procedures. Check also that similar procedures exist within support and that where necessary they provide for changes to design and requirements documents.

In particular, look at how changes to on-line operational (and often critical) systems are handled, these often need to be very carefully and extensively planned. Are sufficient fallback arrangements provided if things go wrong? Support staff access to sensitive parts of the system should be restricted to only that necessary, look to see how this is implemented.

Check that all changes are properly authorised (that the authorisation is from the correct level of management and that operations management are involved), that changes are correctly reviewed and tested and finally that full authorisation is given before changes can be incorporated.

Often changes will be grouped together and incorporated into a release rather than introduced on an ad-hoc basis, in this situation look to see that release records correctly identify changes made. It is likely that an emergency change procedure is also employed to correct operational system failure situations; check that this meets all of the above criteria.

Check that proper configuration control is applied during changes and that correct records of the implemented release are in place.

2.8.5.2 Technical review of operating system changes (BS 7799-2 - cl. A.10.5.2)

APPLICATION SYSTEMS SHALL BE REVIEWED AND TESTED WHEN CHANGES OCCUR.

Implementation guidance:

Changes to operating system software should be under control (see also Section 2.8.5.1 above). However, the impact of those changes on security in general and on the application systems should also be assessed. Where new operating software and applications are not properly tested there is a vulnerability to breakdowns leading to non-availability of service, loss of integrity and compromise of information. Therefore, organizations should have procedures in place for the review of such changes.

Auditing guidance:

The organization should have a review procedure covering operating system changes. This should occur before the planned installation, if possible a test installation should be evaluated. This review should include an assessment of the controls planned to be in place after the change, and check that they are sufficient for the requirements. Auditors should look at the inputs to such reviews, such as manufacturers data sheets and release notes, evaluation data if available, identified software changes that will be needed - for example, where a “work around” has been applied to operating system defects - and support arrangements. Outputs from these reviews should include any necessary application changes and a plan for installation of the new operating system version. The version of operating system (plus any patches) needs to be specified in the configuration records. In some situations organizations may decide not to upgrade the operating system, check under these situations however that they still have access to the necessary levels of support and if not, that this is identified and reacted to in the risk assessment.

2.8.5.3 Restrictions on changes to software packages (BS 7799-2 - cl. A.10.5.3)

MODIFICATIONS TO SOFTWARE PACKAGES SHALL BE DISCOURAGED AND ESSENTIAL CHANGES STRICTLY CONTROLLED.

Implementation guidance:

Modern software is immensely complex and subjected to much control and testing during its development. There is therefore considerable risk in making modifications within the user organization that changes will introduce vulnerabilities leading to a breakdown in its internal controls. Loss of confidentiality, integrity and availability can result.

Where changes appear to be essential a risk assessment should spell out the vulnerabilities and compensating controls should be selected. Such changes should be authorized at an appropriate level and subjected to change control procedures.

Auditing guidance:

This requires the use of a properly documented and authorized change control procedure. Any changes should be introduced in a controlled fashion and ensure that changes have to be fully justified and authorized before implementation. Software packages should only be modified if there is a business requirement to do so.

Sometimes changes to code may be made as patches, to be incorporated later into future releases; where this is done ensure that the patch is correctly removed and all necessary documentation updated. Sometimes organizations may have access to the source code but they are not the design authority; such rights to make modifications should be defined in contracts but make sure that modifications are properly incorporated since, possibly not having full access to design records, these may further risk system integrity.

Look also at how such changes are handled when new releases of the original program are issued, they may need to be re-inserted. Check that there is a complete history of all changes made and that these records are retained for as long as is required. The application should have a defined suite of regression tests that can be used to validate the performance of modified code, look at the control of this.

2.8.5.4 Covert channels and Trojan code (BS 7799-2 - cl. A.10.5.4)

THE PURCHASE, USE AND MODIFICATION OF SOFTWARE SHALL BE CONTROLLED AND CHECKED TO PROTECT AGAINST POSSIBLE COVERT CHANNELS AND TROJAN CODE.

Implementation guidance:

Almost all software products used nowadays contain some sort of covert channels. A lot of them are harmless, like special key combinations giving information about the programmers involved in producing the software, but others might be damaging. Organizations should identify their concerns about covert channels and decide on whether action to protect against them should be taken. When making such a decision, it should be kept in mind that covert channels might only be detected through a resource and time consuming process.

Trojan code can be introduced in the system without being detected and can be used to perform functions unwanted and not even noticed by the users, such as the sending out of passwords previously collected. Actions that can be taken to protect against Trojan code are listed in ISO/IEC 17799, Clauses 8.3.1 and 10.5.4, but again this might involve a lot of resources and time.

Auditing guidance:

Many pieces of software contain various forms of hidden code. Some of this code is in general harmless and is not considered vulnerability. On the other hand some of this code can be exploited and can become the route for covert channels, and they, like Trojan code, are not easy to detect.

An auditor should check what provisions the organization has in place to deal with covert channels and Trojan code. This should take into account that covert channels and Trojan code can lead to unauthorized disclosure, modification and destruction of information. Auditors should consider the controls listed in ISO/IEC 17799, clause 10.5.4, that can be applied to protect against covert channels and Trojan code.

2.8.5.5 Outsourced software development (BS 7799-2 - cl. A.10.5.5)

CONTROLS SHALL BE APPLIED TO SECURE OUTSOURCED SOFTWARE DEVELOPMENT.

Implementation guidance:
Outsourcing of software development includes several risks because of the lack of control during the development process. These risks include a lack of quality in the product, as well as unwanted software such as covert channels or Trojan code being integrated in the product. Contractual agreements should be used to protect against these risks, to ensure the timely delivery, and to clearly identify the intellectual property rights of the work carried out.

Auditing guidance:
The risks of outsourcing of software development should be examined by the organization. Ideally the development environment and processes involved should be inspected and reviewed. The risks associated with such developments should be reviewed and the security requirements, controls and responsibilities of both parties relating to such developments and any identified risks should be covered in any development contract. Auditors should check that such a contract covers:

- conditions to measure the timeliness and quality of developed software and requirements for the quality of code,
- access rights in case an audit is necessary to ensure quality of work done,
- regulations and agreements defining IPR and ownership of developed software,
- sufficient testing the functionality of developed code, including checks for viruses, covert channels and Trojan code.

2.9 Business continuity management (BS 7799-2 - cl. A.11)

2.9.1 Aspects of business continuity management (BS 7799-2 - cl. A.11.1)

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

ISO/IEC 17799 extension: A business continuity management process should be implemented to reduce the disruption caused by disasters and security failures (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventative and recovery controls. The consequences of disasters, security failures and loss of service should be analyzed. Contingency plans should be developed and implemented to ensure that business processes can be restored within the required time-scales. Such plans should be maintained and practiced to become an integral part of all other management processes. Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

2.9.1.1 Business continuity management process and impact analysis (BS 7799-2 - cl. A.11.1.1 & A.11.1.2)

THERE SHALL BE A MANAGED PROCESS IN PLACE FOR DEVELOPING AND MAINTAINING BUSINESS CONTINUITY THROUGHOUT THE ORGANIZATION.
A STRATEGY PLAN, BASED ON APPROPRIATE RISK ASSESSMENT, SHALL BE DEVELOPED FOR THE OVERALL APPROACH TO BUSINESS CONTINUITY.

Implementation guidance:
The best run organization can find itself involved in a disaster or business interruption of one kind or another. Every organization is therefore vulnerable to the serious consequences of having its business brought to a standstill, perhaps potentially fatal to the organization. We might think of fires, floods and explosions as the main cause of disaster but these are, happily, fairly rare. More common reasons for invoking the business continuity plan are viruses, unreliable data, and hardware and software failures. As many as 80% of organizations suffering a disaster or business interruption, but having no properly tested continuity plan, go out of business within a couple of years.

There should be a process to ensure that the critical activities of the organization are identified by risk assessment and plans put in place to recover from, and offset the consequences of, their interruption. This is not just an IT problem - the loss of other business processes can be equally damaging, and they should be included in the continuity planning process.

When developing the overall approach an organization is taking to business continuity, two major elements need to be identified and analysed: those events that can cause interruptions to the business process, and the impacts such interruptions can have on the organization. This impact analysis should take into account the damages resulting from interruptions, as well as any recovery and replacement costs, and the costs related to not being able to conduct business for a certain period of time. It should be noted that this assessment process includes all of the organization's facilities, equipment, personnel and processes, not only those related to information processing.

Auditing guidance:
Business continuity planning should be the output of an effective risk assessment process and a sufficient amount of protection against business disruptions and disasters should be in place for any organization. The scope and detail of these plans should of course be commensurate with the security and business requirements.

Auditors should check that a business continuity management process is in place, and review that it is being maintained, and it is being applied throughout the whole organization. Auditors should examine the documentation associated with this process, and ensure that it contains the elements listed in ISO/IEC 17799, Clause 11.1.1.

Business continuity planning should be based on the analysis of the risks and impacts related to business interruptions. Auditors should check that the risk assessment is complete and comprises all parts of the organization that are related to business interruptions, and is not only focused on information processing facilities. The results of the risk and impact analysis should be used for the development of the business continuity plan. Auditors should ensure that the scope and details of this plan fulfil the organization's business and security requirements, and that it has been signed off by management.

2.9.1.2 Writing and implementing continuity plans (BS 7799-2 - cl. A.11.1.3)

PLANS SHALL BE DEVELOPED TO MAINTAIN OR RESTORE BUSINESS OPERATIONS IN A TIMELY MANNER FOLLOWING INTERRUPTION TO, OR FAILURE OF, CRITICAL BUSINESS PROCESSES.

Implementation guidance:
These plans should include the detailed actions that are to be taken in case of an emergency or interruption to business and who is responsible for the actions to be carried out. These plans should be agreed within the organization, and training, awareness, testing and maintenance activities (see also Section 2.9.1.4) should be in place to ensure that they are

and remain effective. The plans should ensure that a timely recovery is possible, and they should include a clear description of the circumstances under which they are activated.

Auditing guidance:
Business continuity plans should concentrate on achieving the identified business and security requirements as described above. Auditors should review whether the time scales associated with these plans are sufficient for the business requirements, and that they are realistic. In addition, it should be reviewed that:

- all responsibilities are agreed and assigned,
- employees are aware of their responsibilities and what they are supposed to do in case emergencies and business interruptions,
- all procedures defined in the plans are documented and implemented according to the implementation schedule,
- all staff are aware and understand what they are supposed to do in case of emergencies and business interruptions,
- the plans are tested and updated according to a defined schedule (see also 2.9.1.4 below).

2.9.1.3 Business continuity planning framework (BS 7799-2 - cl. A.11.1.4)

A SINGLE FRAMEWORK OF BUSINESS CONTINUITY PLANS SHALL BE MAINTAINED TO ENSURE THAT ALL PLANS ARE CONSISTENT, AND TO IDENTIFY PRIORITIES FOR TESTING AND MAINTENANCE.

Implementation guidance:
Because of its all encompassing nature, business continuity planning is likely to produce several plans, each providing for a specific part of the organization. These plans are vulnerable to failure if they have not been related together, and to existing procedures, by a well thought out and established framework.

The framework should include co-ordination, priority setting, domain plans, testing and continuous maintenance within its scope, as lined out in more detail in ISO/IEC 17799, Clause 11.1.4.

Auditing guidance:
In all organizations where several plans covering different departments or catering for different scenarios exist, it should be ensured that a consistent framework for plans exist; check that this framework exists and that the plans are consistent. Plans need to be consistent with levels of service obligation, check for this.

Check that the plan is readily available, that proper document control is applied and that key personnel know what is initially required and where essential items - such as keys or codes to safes, support telephone numbers etc. - are located. Look at the staffing of the plans, do they rely on one or a few key personnel, what happens if they are not available? Look at the requirements to keep updated information that will be needed in emergencies - contact names and numbers, access codes and so on - check that this is done.

Have typical scenarios such as data corruption, virus attack, fire, loss of key personnel, extended loss of supply etc. been considered? Is there provision to test fallback operations, data recovery, transfer to alternative location and so on? ISO/IEC 17799, clause 11.1.4 provides a detailed checklist for a business continuity planning framework.

2.9.1.4 Testing, maintaining and re-assessing business continuity plans (BS 7799-2 - cl. A.11.1.5)

BUSINESS CONTINUITY PLANS SHALL BE TESTED REGULARLY AND MAINTAINED BY REGULAR REVIEWS TO ENSURE THAT THEY ARE UP TO DATE AND EFFECTIVE.

Implementation guidance:
The organization may have developed contingency plans but if they are untested the organization remains vulnerable to disaster. Regular testing and maintenance are necessary to provide the necessary assurance of satisfactory recovery.
The rate of change in the modern organization increases vulnerability to obsolescence in plans and documentation of all kinds. Failure to maintain the continuity plan on a regular basis will result in its failure to provide the continuity planned for. A documented plan for updates should be maintained along with evidence of regular reviews of the continuity plans.

Auditing guidance:
Testing of continuity plans is essential and auditors should determine the testing schedule, which may be defined in the framework or the plan itself. It is extremely unlikely that plans with any degree of complexity will work perfectly first time, individuals need to follow the procedures to handle the situation effectively and this can only be done with practice.
There should be a well defined development plan for the plans themselves; full review and debate before initial issue, scheduled tests followed by analysis and review and finally unannounced tests to validate their continued suitability and provide staff training. Look for the results of tests, were any problems encountered, have these been analysed and corrected, what where the performance measures, did these meet the service level obligations? Look also for the inclusion of new employees and third parties in the testing.
Very often continued operations will depend on their effective co-operation. Be suspicious of plans that have not been regularly updated, are there records to demonstrate that these have been reviewed for adequacy, incorporation of new facilities, changes to regulatory requirements? Check that responsibilities for the maintenance and updating of the plans have been defined, and that any changes to the plans can only be made with appropriate authorization.

2.10 Compliance (BS 7799-2 - cl. A.12)

2.10.1 Compliance with legal requirements (BS 7799-2 - cl. A.12.1)

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

ISO/IEC 17799 extension: The design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal requirements should be sought from the organization’s legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and for information created in one country that is transmitted to another country (i.e. trans-border data flow).

2.10.1.1 Identification of applicable legislation (BS 7799-2 - cl. A.12.1.1)

ALL RELEVANT STATUTORY, REGULATORY AND CONTRACTUAL REQUIREMENTS SHALL BE DEFINED EXPLICITLY AND DOCUMENTED FOR EACH INFORMATION SYSTEM.

Implementation guidance:
All legal, regulatory and contractual requirements should be identified by the organization to ensure their fulfilment. Especially when thinking of conducting business in other countries, the identification of applicable legislation should be supported by an expert, e.g. a lawyer. Special attention is required when conducting on-line business or trading to ensure compliance with all relevant legislation in the countries involved.

Auditing guidance:
The organization should present to the auditors the actions they have been taken to identify and comply with applicable legislation. The auditors should check that no applicable legislation has been forgotten or was missed by mistake. The organization should have controls in place to comply with the legal requirements that have been identified. Responsibilities for these controls should be identified and documented, and those responsible should be aware of their responsibilities.

2.10.1.2 Intellectual property rights (IPR) (BS 7799-2 - cl. A.12.1.2)

APPROPRIATE PROCEDURES SHALL BE IMPLEMENTED TO ENSURE COMPLIANCE WITH LEGAL RESTRICTIONS ON THE USE OF MATERIAL IN RESPECT OF INTELLECTUAL PROPERTY RIGHTS, AND ON THE USE OF PROPRIETARY SOFTWARE PRODUCTS.

Implementation guidance:
Organizations are vulnerable to their failure to comply with restrictions on copying copyright material. There is a serious risk of legal action being taken against the organization and individual staff where, for example, PC software is being used on more than the number of systems it is licensed for.

Staff should be made aware of the rules and inventory checks should be carried out at least annually to provide assurance that all software in use (that is, software loaded on the system) is properly licensed. Documentary records should be maintained of the inventory of software on each system (see also Section 2.3.1 above).

In the UK, under the Copyright, Designs and Patents Act 1988, certain software copyright infringements are a criminal offence.

Auditing guidance:
Auditors should examine the procedures that the organization has in place to protect the intellectual property rights of information and software. These procedures should describe rules for handling material that is marked as copyright, design rights or trademarks, and employees should be aware of how to handle such material. Users should also be aware that any unauthorized use or copying of intellectual property rights material or software might lead to legal action.

There needs to be strict controls on the use of software in the organization. Auditors should investigate what licenses have been purchased and then how compliance is maintained. Many commercial packages provide licence agreements on packaging and this comes in various forms, there is no common format so information such as number of users, restrictions to use etc., therefore further information needs to be gathered to check that the software is used in compliance with the licensing agreement.

One possibility is to see how the organization has addressed this, one way would be to draw up a table of key packages and then identify the key aspects of each licence and together with a record of actual use from asset audits. Look for the use of development tools and libraries, have these been used correctly? With bespoke software developed for the organization, look at the development or support contract; is access to source provided, may in-house changes be applied, are their restrictions on the use or location of the software. Ensure that the responsible personnel in the organization are fully aware of their obligations regarding software copyright. Check PCs at random for unlicensed software.

2.10.1.3 Safeguarding of organizational records (BS 7799-2 - cl. A.12.1.3)

IMPORTANT RECORDS OF AN ORGANIZATION SHALL BE PROTECTED FROM LOSS, DESTRUCTION AND FALSIFICATION.

Implementation guidance:
Organizations will have a number of essential documents and computer held records that, for instance, demonstrate their title to various assets, contracts, etc. that must be protected from loss or modification at all costs. These items should be listed in the inventory (see also Section 2.3.1 above) and appropriate controls selected and implemented. The continued presence of the items should be confirmed by documented inventory check at least annually.

For example, in the UK organizations are also obliged under various regulations to maintain business records of certain types for periods up to ten years. The organization is open to prosecution by the Inland Revenue or HM Customs and Excise where this is not done.

Auditing guidance:
Those records required for legal or regulatory purposes are usually a subset of all the records an organization will require to keep for business purposes or other reasons. Ensure that withal records required for legal or regulatory purposes are identified and that all requirements are complied with. This will include, for example, financial records, customs records, legal records and environmental records.

The exact requirements will vary from country to country and the organization needs to be aware of and comply with all applicable requirements. Ensure that this has been done and verified by the appropriate personnel. The storage arrangements (including security), requirements for review and disposal should all be defined in procedures.

There should be some form of clearly identifiable index of what records there are and auditors should check this for accuracy. Some documentation may now be held electronically, either because that was the original format or because they have been scanned. Check that the organization has reviewed the legal admissibility of this storage medium and are complying with any specified requirements.

2.10.1.4 Data protection and privacy of personal information (BS 7799-2 - cl. A.12.1.4)

CONTROLS SHALL BE APPLIED TO PROTECT PERSONAL INFORMATION IN ACCORDANCE WITH RELEVANT LEGISLATION.

Implementation guidance:
In plenty of countries, some legislation or regulation is in place to protect the privacy of personal information. For example, in the UK the storage and use of personal data on a computer should be registered under the Data Protection Act 1984. Failure to comply with such legislation may leave the organization open to prosecution and a fine, or at least too serious loss of image and reputation, if it became public. Several legislations also specify a number of requirements for the collection, processing, accessibility and protection of personal information on computers. Failure here can also lead to prosecution.

Registration should be based on an inventory of personal data assets. Procedures are necessary to ensure that changes in the use of personal data are reflected as necessary in the registration. A documented review should be carried out at least annually, and compliance with all requirements stated in the relevant laws or regulations need to be ensured.

Auditing guidance:
Careful control of personal information is necessary to comply with the Data Protection Act in the UK; plenty of other countries, for example in Europe, have similar requirements. The legislation might also require the organization to register their use, look for evidence of this. Look also at the type of data held, is it necessary, has it been validated, is it transmitted or otherwise conveyed outside of the organization? Who has access to this data, is it necessary for their job function?
Check that the organization monitors changes to requirements in this area, new, tighter restrictions may be introduced with specified periods for compliance. Is there awareness, are there plans to introduce compliance within the time frame? Auditors must ensure that they themselves are fully up to date with this area of legislation.

2.10.1.5 Prevention of misuse of information processing facilities (BS 7799-2 - cl. A.12.1.5)

MANAGEMENT SHALL AUTHORIZE THE USE OF INFORMATION PROCESSING FACILITIES AND CONTROLS SHALL BE APPLIED TO PREVENT THE MISUSE OF SUCH FACILITIES.

Implementation guidance:
Every organization that makes widespread use of IT facilities is vulnerable to staff, and others, misusing it to their own ends. There is a risk that misuse can imperil the integrity of data and systems threaten availability and expose confidential information. Controls should be in place to properly authorize all use of IT facilities for justified business purposes. Misuse should be subject to disciplinary action (see also Section 2.4.3.5 above).
In the UK, in some circumstances, misuse of computers can be a criminal offence under the Computer Misuse Act 1989 and misuse of personal data a criminal offence under the Data Protection Act 1984. Similar legislation is in place in lots of other countries. The details of the applicable legislation should be checked out to ensure compliance.

Auditing guidance:
Misuse of information processing facilities may prove not only expensive to the organization in terms of telephone costs, disk space, CPU time, network loading, lost working time etc., but could cause inadvertent release, corruption or access from unauthorised sources to sensitive information. It can also lead to malicious software infections, such as viruses, Trojan horses etc or to conflict with legislation, if the organization's information processing facilities are used to by employees to carry out unlawful activities.
There should be a clear policy, defined by management and understood and formally acknowledged by employees. Procedures should deal with actions on discovering intentional misuse, see also ISO/IEC 17799, Clause 6.3.5, Disciplinary process. If staff is permitted to use computers for games, Internet access etc., then these should be separate and isolated from those handling sensitive information. Investigate the use of other, peripheral or associated equipment such as printers, copiers etc., what is the policy here?

2.10.1.6 Regulation of cryptographic controls (BS 7799-2 - cl. A.12.1.6)

CONTROLS SHALL BE IN PLACE TO ENSURE COMPLIANCE WITH NATIONAL AGREEMENTS, LAWS, REGULATIONS OR OTHER INSTRUMENTS TO CONTROL THE ACCESS TO OR USE OF CRYPTOGRAPHIC CONTROLS.

Implementation guidance:
The legal and regulatory requirements and rules for the use of cryptographic controls and the effort and resources necessary to comply with them should be assessed. The results of these assessments should be taken into account in the decision about the use of cryptographic

controls. This assessment should not only include the laws and regulations applicable for encryption controls, but also the legal environment for the use of digital signatures and other electronic communications. Because of the differences in the legal situation of various countries, special care should be taken to ensure compliance with legislation in all those countries that are involved in business or travel.

Auditing guidance:
The organization should present to the auditors the actions they have taken to identify applicable legislation and regulations for cryptographic controls and the legal advice they have taken where necessary to ensure compliance. The controls that are taken to fulfil these requirements should be documented, implemented and maintained. The auditor should check that the implementation of cryptographic controls as described in Section 2.8.3 are commensurate with the legal requirements identified.

2.10.1.7 Collection of evidence (BS 7799-2 - cl. A.12.1.7)

WHERE ACTION AGAINST A PERSON OR ORGANIZATION INVOLVES THE LAW, EITHER CIVIL OR CRIMINAL, THE EVIDENCE PRESENTED SHALL CONFORM TO THE RULES FOR EVIDENCE LAID DOWN IN THE RELEVANT LAW OR IN THE RULES OF THE SPECIFIC COURT IN WHICH THE CASE WILL BE HEARD. THIS SHALL INCLUDE COMPLIANCE WITH ANY PUBLISHED STANDARD OR CODE OF PRACTICE FOR THE PRODUCTION OF ADMISSIBLE EVIDENCE.

Implementation guidance:
It is important that an organization ensures the collection of admissible and complete evidence for any incident that is taking place, since it is very often not obvious whether an incident might finally result in a court case or not. The organization should have guidelines and procedures for the collection of evidence that ensure appropriate quality.
Once evidence is collected, it should be managed and stored securely, to guarantee that nobody can modify or destroy it without authorization. It should also be ensured that the evidence is available in a timely manner and in a form that is required by court.

Auditing guidance:
Collection of evidence is important to be able to provide adequate support in legal procedures and actions that might ensue as a result of some breach of civil or criminal law. The organization should have procedures in place to collect evidence and auditors should check that these procedures ensure:

- that the information collected comply with applicable standards or codes of practice for the production of such evidence to be deemed admissible as evidence,
- the quality and completeness of such evidence, i.e. the weight of evidence is appropriate,
- that completeness and correctness of the information can be proved, as described in ISO/IEC 17799, clause 12.1.7.3.

Auditors should check where collected evidence is stored, and whether it is possible for unauthorized persons to modify or destroy such evidence. In addition, auditors should consider the conditions when the collection of evidence needs to be activated. Collection of evidence should start at an early stage to ensue that no information is destroyed.

2.10.2 Review of security policy and technical compliance (BS 7799-2 - cl. A.12.2)

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

ISO/IEC 17799 extension: The security of information systems should be regularly reviewed. Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards.

2.10.2.1 Compliance with security policy (BS 7799-2 - cl. A.12.2.1)

MANAGERS SHALL TAKE ACTION TO ENSURE THAT ALL SECURITY PROCEDURES WITHIN THEIR AREA OF RESPONSIBILITY ARE CARRIED OUT CORRECTLY AND ALL AREAS WITHIN THE ORGANIZATION SHALL BE SUBJECT TO REGULAR REVIEW TO ENSURE COMPLIANCE WITH SECURITY POLICIES AND STANDARDS.

Implementation guidance:
Although effort is expended throughout an organization to implement the controls recommended in ISO/IEC 17799 and BS 7799 Part 2, respectively, that is no assurance that they are operating effectively. Every part of the organization should be reviewed at least annually (and more frequently if the risk assessment has shown that this is necessary) to provide the required assurance. Reviews can be carried out internally within departments, although an independent review (e.g. security department, internal audit) might be of more value. A documented record of the review should be maintained, noting non-compliances, agreed action, and follow-up.

Auditing guidance:
In order to determine the degree to which security policies and procedures are being complied with management should ensure that regular internal compliance audits are performed. These should be planned, performed by competent personnel, fully documented, followed up to ensure resolution of non-compliant items, and reported on to senior management.
The periodicity of audits should be dependent on the security requirements and auditors must consider whether the frequency demonstrated is consistent with the risk, criticality of the information, changes in technology and any other factors that may impact the organization. A minimum frequency of six months is recommended but all organizations should conduct reviews at least annually covering all sections of BS 7799-2.

2.10.2.2 Technical compliance checking (BS 7799-2 - cl.A.12.2.2)

INFORMATION SYSTEMS SHALL BE REGULARLY CHECKED FOR COMPLIANCE WITH SECURITY IMPLEMENTATION STANDARDS.

Implementation guidance:
The complexity of computer systems such as firewalls means that, with the best will in the world, it is possible to leave them in an insecure state. Organizations are vulnerable to misuse while management are otherwise sure that they have implemented the necessary controls. A full, technical, review should be carried out at intervals determined by risk assessment.
The operational systems require skilled analysis, aided sometimes by special programs. Indeed, the availability of programs will allow checks to be carried out more frequently as well as faster. Checks should be documented together with the results, non-compliances, actions and follow up.
These checks should only be carried out by, or under the supervision of, competent, authorized persons. The integrity of the system could be jeopardised when an unskilled

person attempts this work. Access controls should generally prevent unauthorized persons from doing this work.

Auditing guidance:
Organizations should check that their systems comply with security implementation standards. There should be a compliance checking plan showing what needs to be covered, the frequency and methods employed. It is important that this type of compliance checking is performed by, or at least under supervision of suitably qualified personnel.
If tools are used, assess what aspects of the facility it is actually covering, it could be purely a monitor or conducting an audit of facilities - has it been validated in any way? Check the individuals completing or reviewing the checks; full compliance can often only really be assessed by technically competent personnel.

2.10.3 System audit consideration (BS 7799-2 - cl. A.12.3)

Objective: To maximize the effectiveness of and to minimize interference to/from the system audit process.

ISO/IEC 17799 extension: There should be controls to safeguard operational systems and audit tools during system audits. Protection is also required to safeguard the integrity and prevent misuse of audit tools.

2.10.3.1 System audit controls (BS 7799-2 - cl. A.12.3.1)

AUDITS OF OPERATIONAL SYSTEMS SHALL BE PLANNED AND AGREED TO MINIMIZE THE RISK OF DISRUPTIONS TO BUSINESS PROCESSES.

Implementation guidance:
Audit activity on operational systems may require the use of special programs, which access data files used by the system or its applications. Such use should be planned to avoid causing problems and disruption in operational systems. Audit plans should be documented and authorized.

Auditing guidance:
Use of system audit controls and tools should not compromise either the information or operations being checked. Where audits are planned, check that appropriate authorisation has been obtained from operational management. No information should be changed for the purpose of these activities and access to information should be logged as for any other operation.
It should also be ensured that the interruptions to business activities are minimized. Make sure the audit results are kept and that use of any tools is properly recorded. Check also that any tools are themselves formally validated before use.

2.10.3.2 Protection of system audit tools (BS 7799-2 - cl. A.12.3.2)

ACCESS TO SYSTEM AUDIT TOOLS SHALL BE PROTECTED TO PREVENT POSSIBLE MISUSE OR COMPROMISE.

Implementation guidance:
The programs and special data files used by auditors may provide risk to system integrity and confidentiality if used by unauthorized persons for purposes not connected with auditing. These tools should be fully protected and controlled in use. Each use should be recorded and, in some cases, authorized by the relevant managers.

Auditing guidance:

These tools will allow access to information or controls that could be used to read or change sensitive information. In the wrong hands, these tools could be very dangerous and there strict controls need to be applied to their application.

Where possible, such tools should be kept separate from operational and test systems; if the tools kept resident on systems, what access controls are there? Manuals describing the tools operating should be similarly protected and the procedures should ensure that only suitably qualified personnel are able to deploy them.