dti

ACHIEVING BEST PRACTICE IN YOUR BUSINESS

Information Security: Protecting Your Business Assets

dti

The DTI drives our ambition of ‘prosperity for all’ by working to create the best environment for business success in the UK. We help people and companies become more productive by promoting enterprise, innovation and creativity.

We champion UK business at home and abroad. We invest heavily in world-class science and technology. We protect the rights of working people and consumers. And we stand up for fair and open markets in the UK, Europe and the world.

Achieving best practice in your business is a key theme within DTI’s approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what can help you, and then support you in implementation. This brochure focuses on these solutions.

The information created, used, stored and transmitted by your organisation forms one of its most important assets. This booklet shows how you can use good practice to protect this information from being maliciously or unintentionally changed (integrity); make it available when and where needed (availability); and ensure that only those with a legitimate right can access it (confidentiality).

This booklet should be regarded as a starting point for developing organisation-specific controls and guidance for the classification and protection of information assets. Not all the guidance provided in this booklet may be applicable to an organisation's specific needs. It is therefore important to understand the organisation's business requirements and to apply this guidance appropriately. The booklet provides general guidance only and, if fully implemented, can only reduce, not eliminate, your vulnerability.

Organisations which regularly handle UK government protectively-marked information must continue to follow the procedures agreed with the appropriate UK security authorities. However, this guidance has been developed in conjunction with them, and similar security procedures can therefore be applied to commercial and protectively-marked information.

Who this brochure is for: those responsible for initiating, implementing or maintaining information security in their organisation as well as those who use and process their organisation's information.

What it covers: the issues surrounding your potential vulnerability to the loss and/or damage of your business information.

CONTENTS

1 Executive Summary

This booklet indicates how you can identify your information assets, and who should have responsibility for them. It also suggests how you can assess the best methods of protecting your identified assets; by considering the threats to them, their vulnerability and the impact that compromise of their confidentiality, integrity or availability might have.

The booklet goes on to consider the 'classification' of information assets to ensure that appropriate levels of protection are given to them. It considers examples of five levels of confidentiality, from 'publicly available' to 'strictly confidential'; and suggests what type of assets might fall into each category. Three categories of integrity classification are considered, with examples. Four levels of classification for availability are suggested, with indications as to the timeframes that might be appropriate to each level (for example 12-48 hours for 'basic' and 2-3 hours for 'high availability'). The practical use of these classifications is considered, particularly in relation to information sharing with partner organisations.

The major part of the booklet shows how the advice and guidance contained in the international code of practice for information security management (ISO/IEC 17799) can be applied to ensure that appropriate protection is given to the integrity, availability and confidentiality of your information. This section covers handling and storage of information (whether physically or electronically held); backup and disposal of information; sharing information with third parties (including outsourcing arrangements); exchanging information electronically or physically; planning for new systems or upgrades to old; using computer applications; and using mobile phones, laptops and other devices away from the workplace.

The final part of the booklet indicates how you can integrate information protection into your overall business. It looks at the importance of establishing security awareness and of having appropriate policies, standards and procedures operating within an information security management system, such as that specified within BS 7799-2:2002.

2 Introduction

2.1 NEED FOR INFORMATION PROTECTION

In recent years, the proliferation of interconnected information systems and networks has meant that no business can afford to neglect its information security. Organisations can't make assumptions about how their trading partners or a third party will protect their information. This has led international legislators and regulators to emphasise the importance of the development of a 'culture of security' within business. For example, in 2002 the OECD published its "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (available to download or order from the DTI website, see the Further help and advice section). These guidelines promote the concept that everyone must take appropriate responsibility for maintaining the security of the information systems and networks they use. In particular, businesses must realise that they need to take account of the increasingly strict regulatory and legal frameworks which operate globally.

All organisations acquire and generate information that is vital to their operation and growth. Examples include client and supplier records of various kinds and proprietary information relating to products, processes, business performance and planning.

Protection of an organisation's information resources is vital both for the continued health of the business and for compliance with legal, regulatory and contractual demands. For these reasons information is now recognised as a significant business asset that needs to be managed effectively. Therefore, of necessity, organisations require their information assets to be kept confidential where required, made available when needed and protected from damage and destruction, and loss of integrity.

Information assets can be in the form of paper records, electronic media or the intellectual property stored in people's heads. Whatever form an information asset takes a business must consider how best to protect its security. In particular, organisations must understand who needs access to it, and how to control that access through a variety of protective measures applied to different types of information. This might be information that is shared with external business partners, is outsourced to a third party or is for internal business use only. This process is known as information asset classification and management, which is the subject of this booklet.

2.2 BEST PRACTICE

This booklet provides advice on the protection of information assets by organisations, covering both the assessment of protection needs and the means by which these needs can be addressed. It reflects current best practice in the private and public sectors including that given in the international standard ISO/IEC 17799 (previously BS 7799 Part 1). The advice provided herein is applicable to a wide range of organisations.

Following the guidance in this booklet should help you to:

- protect your organisation's sensitive and critical information in a consistent and appropriate manner,
- protect information entrusted to you by other organisations.

By doing this, you should:

- reduce the risk and damage to your organisation's reputation, profitability or business interests due to loss of, or harm to, sensitive or critical information,
- reduce the risk of embarrassment or loss of business arising from loss of, or damage to, another organisation's sensitive or critical information,
- increase confidence in trading partnerships and outsourcing arrangements.

The security controls outlined in this document provide best practice advice for information protection. Controls to provide this protection should be selected based on a risk assessment (see Section 4.2).

3 Definitions

For the purposes of this booklet the following definitions apply:

3.1 INFORMATION SECURITY

Information security involves the preservation of confidentiality, integrity and availability of information (reference ISO/IEC 17799:2000). In general terms this means that information security deals with the maintenance and control of:

- **Confidentiality:** ensuring the information is accessible only to those authorised to have access,
- **Integrity:** protecting the accuracy and completeness of information,
- **Availability:** ensuring that access to information is available when and where required and is not denied to any authorised user.

There are additional security properties that may be used to focus on particular facets of these three fundamental security objectives, such as identification, authentication, access control and non-repudiation.

3.2 RISK ASSESSMENT

Risk assessment is the assessment of threats to, vulnerabilities of, and impacts on, information and information processing facilities and the likelihood of their occurrence.

Risk assessment is the overall process of risk identification, risk analysis and risk evaluation (ISO Guide 73:2002).

3.3 RISK MANAGEMENT

Risk management encompasses a range of activities within an organisation that are directed at the assessment and treatment of risk.

NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication (exchange or sharing of information about risk between the decision-maker and other stakeholders) (ISO Guide 73:2002).

3.4 INFORMATION SECURITY INCIDENT

An information security incident is one or more unwanted or unexpected events that have a significant probability of compromising business operations and threatening information security (ISO/IEC TR 18044:2004).

Examples of security incidents are:

- loss of service, equipment or facilities
- system malfunctions or overloads
- human errors
- fraud
- non-compliance with policies or guidelines
- breaches of physical security arrangements
- uncontrolled system changes
- malfunctions of software or hardware
- access violations.

3.5 THREAT

A threat is a potential cause of an unwanted incident which may result in harm to a system or organisation.

3.6 VULNERABILITY

Vulnerability is a weakness of an asset or group of assets which can be exploited by a threat.

4 Information Protection Framework

4.1 IDENTIFICATION AND OWNERSHIP OF INFORMATION

All assets, including information assets, should be accounted for and have a nominated owner and/or custodian whose responsibility it is to ensure that appropriate protection is maintained.

Business processes which might involve the copying, printing, emailing, placing on websites, publishing and destroying of valuable information assets should also have a nominated and accountable owner.

Owners should be responsible for ensuring that appropriate security controls are implemented and maintained throughout the lifetime of the asset. Responsibility for implementing controls may be delegated; however the accountability should remain with the nominated owner of the asset.

An inventory of all important assets should be produced and it should be updated on a regular basis. This should include information about the type of asset, its owner/custodian, relevant licence information, business value and location.

EXAMPLES (INFORMATION ASSETS)

These are examples of some of the information assets which require protection:

- organisational records (e.g. company accounts, tax and VAT statements)
- personal records (Data Protection Act 1998)
- customer details
- intellectual property (e.g. designs, specifications, research results)
- healthcare records

EXAMPLES (RESPONSIBILITIES)

The Data Protection Act 1998 defines a number of responsibilities including the following:

- Data controller – person who determines the purpose and manner in which personal data is processed.
- Data processor – any person who processes the data on behalf of the data controller.

The Companies Act 1989 defines a number of responsibilities for company directors:

- Management has the responsibility to protect all organisational records from loss, destruction and falsification, in accordance with statutory, regulatory and contractual requirements and obligations.
- All employees, contractors and any other users should be made aware of their responsibility to report any information security incidents as quickly as possible.
- All employees should be aware of their legal responsibilities to protect intellectual property.

An asset inventory:

- helps effective asset protection to take place
- is important for business continuity purposes and in the recovery from a disaster or system failure
- may be required for various other business purposes such as health and safety, insurance, finance and for compliance with certain laws and regulations.

If the organisation maintains more than one inventory, it should make sure that the content of these is aligned so that all assets are fully recorded and can be tracked.

The inventory should have an assigned owner who is responsible for its accuracy and availability and a process should be in place for its maintenance.

4.2 ASSESSMENT OF PROTECTION NEEDS

The security controls an organisation deploys to protect its assets should be justifiable, practical and necessary. Assessment of the protection needs and the resources required to deploy suitable protection should be balanced against the risks to the assets the business faces. The process of compiling an inventory of assets is an important aspect of risk management.

Information security risk is assessed in the following terms:

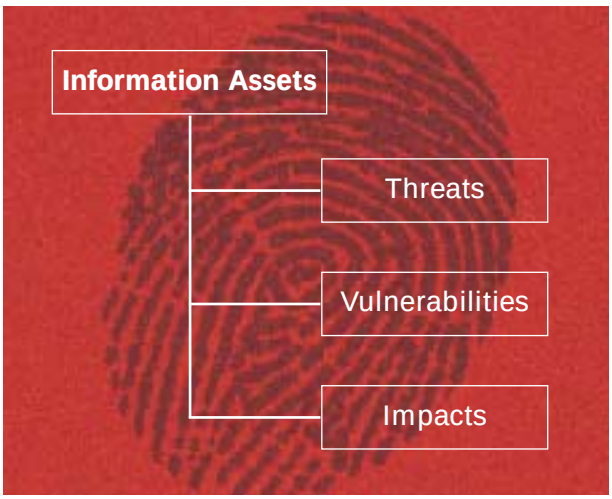
Information Assets

What is the importance, usefulness or value of the information asset to the organisation?

Threats

What are the threats which might cause harm, damage or loss to the organisation's information? How real or likely is the threat? For example, threats might include:

- system failure
- disgruntled employee
- unauthorised access by competitor
- denial of service attack
- malicious software attack
- theft of laptop
- fraud and deception
- online theft and forgeries
- identity theft



Vulnerabilities

How and where is your information asset most vulnerable? How can it be exploited and/or compromised by the threats? For example, vulnerabilities might include:

- lack of effective procedures and instructions for handling information
- lack of user training and awareness
- weak access control on IT systems
- no allocation of responsibilities
- no information backup

Impacts

What would be the impact on the integrity, availability and/or confidentiality of the asset if a threat were able to exploit a vulnerability?

The process of risk assessment is good business practice. It should be the basis of any information asset classification or grading and be used to determine classification levels. By assessing these aspects, you'll get an idea of the threats to your information and the business risk to the organisation.

4.3 INFORMATION ASSURANCE

Organisations need to manage their information protection arrangements to give assurance that they are effective in mitigating anticipated threats and related risks to an adequate extent. Security controls will need to be selected so as to deliver an appropriate level of robustness and resilience in countering risks to the integrity, availability and confidentiality of information assets.

Exactly how information protection is achieved will vary from organisation to organisation, or even from department to department. But it is important that the information assurance delivered by such diverse approaches is broadly comparable in the context of comparable risks. This is particularly important for organisations that are sharing valuable or otherwise sensitive information.

Maintaining information assurance in the light of changing threats, business needs and compliance needs is important. Regular reviews of these matters are needed. In addition, any major change to the business should be accompanied by such a review.

5 Information Classification

5.1 OBJECTIVE

Information assets need to be suitably classified or graded to ensure that they receive an appropriate level of protection commensurate with their sensitivity and criticality. This classification is related to the risks the business faces and the associated impact, loss or damage to the organisation.

5.2 CLASSIFICATIONS

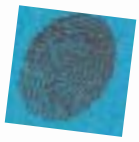
The protection requirements of information assets can be classified in ways that reflect the value of the information to the business and the impact on the business of incidents affecting these assets. This booklet defines a classification based on integrity, availability and confidentiality requirements for information assets.

LEVELS OF INTEGRITY

This booklet specifies levels of integrity that are defined to reflect the criticality of information assets and the impact of their unauthorised modification and the subsequent loss of accuracy. The following are some examples:

- **BASIC INTEGRITY (Routine) for normal purposes**
  This covers information where unauthorised damage or modification is not critical to business applications and business impact is minor.
- **MEDIUM INTEGRITY where independent verification is required**
  This covers information where unauthorised damage or modification is not critical but noticeable to business applications and business impact is significant.
- **HIGH INTEGRITY**
  This covers information where unauthorised damage or modification is highly critical to business applications and the business impact is major and could lead to serious or total failure of the business application, total shutdown of business operations or even closure of the business.

Case studies



MANAGED SERVICES COMPANY

A company supplies data management and processing services to its clients. This provides clients with HIGH AVAILABILITY on-line access to a 24 hour processing, storage and archiving capability for its data.

CALL CENTRE SERVICES

A company relies heavily on off-shore call centre services for its UK branded IT products. The company had a service level agreement (SLA) with an overseas centre to provide help desk services to its customers on all problems associated with its products. The SLA was set at MEDIUM AVAILABILITY as part of a cost cutting measure. Unfortunately the company underestimated the demand for such services and soon the volume of complaints escalated. The company revised its SLA to give HIGH AVAILABILITY access and reviewed this availability level on a regular basis.

LEVELS OF AVAILABILITY

Levels of availability that are defined to reflect the accessibility of information assets and the impact if such assets are not available within a specified timeframe are as follows:

- **BASIC AVAILABILITY (Routine)**
  Information and services required for business applications and processes to be available within 12-48 hours
- **MEDIUM AVAILABILITY (Priority)**
  Information and services required for business applications and processes to be available within 12 hours
- **HIGH AVAILABILITY (High Priority)**
  Information and services required for business applications and processes to be available within 2-3 hours
- **VERY HIGH AVAILABILITY (Immediate)**
  Information and services required for business applications and processes to be immediately available at all times

LEVELS OF CONFIDENTIALITY

Levels of confidentiality that are defined to reflect the sensitivity of information assets and the impact of their unauthorised disclosure are as follows:

- **PUBLICLY AVAILABLE INFORMATION**
  This refers to information that would cause no damage to the company if disclosed.

This could be information that appears on the organisation's web site, in marketing and sales materials, public presentations and product user manuals.

- **"INTERNAL USE ONLY" INFORMATION**
  This refers to information available to any employee in the organisation, but to which external access is granted only with authorisation. The disclosure or loss of such information would be inappropriate and inconvenient, and could have an **appreciable impact** on the organisation.

This information is generally that which an organisation simply wishes to keep private and it is likely to be of a routine, operational nature. It will constitute the largest category of information in most organisations.

- **"CONFIDENTIAL" INFORMATION**
  This refers to information which is commercially sensitive and whose disclosure or loss would have a **significant impact** on the organisation. For example, the impact might be financial or it might affect profitability, competitive advantage or business opportunities or it might involve embarrassment or loss of reputation.

- **"STRICTLY CONFIDENTIAL" INFORMATION**
  This refers to information which is commercially sensitive and whose disclosure or loss would have a **very significant impact** on the organisation. Again, the impact might be on the company's finances or might affect its profits, competitive advantage or business opportunities, or involve embarrassment or loss of reputation but the loss or effect, whatever its nature, would be very serious.

Case study

WEB BASED SHOPPING

Any business advertising, selling or providing product information on a web site is providing PUBLICLY AVAILABLE INFORMATION. Confidentiality is not an issue but availability and integrity of that information needs consideration. The aim of such web sites is to attract as many customers as possible and to provide accurate and up to date information about products and services.

Case study

MANUFACTURING COMPANY

A company produces a range of high quality products. This company's brand name is well known in many parts of the world. The product specifications are highly guarded trade secrets and are protected with a "STRICTLY CONFIDENTIAL" marking.

Organisations may also have information which is sector specific and which may influence the levels of classification described above. One such type of information, held by many organisations, is:

- **"PERSONAL DATA/INFORMATION"**
  This covers information about employees, customers and other individuals that is protected by the Data Protection Act. Disclosure of such information could have serious legal consequences. Information falling into this category must be treated as 'CONFIDENTIAL' or 'STRICTLY CONFIDENTIAL'.

Information that might be considered in the "Confidential" or "Strictly Confidential" category includes:

- negotiating positions
- investment strategies
- marketing information
- competitor assessments
- personal information (see above)
- customer information
- details of major acquisitions, divestments, and mergers
- high-level business and competition strategy
- very sensitive competitor, partner or contractor assessments
- high-level business plans and potential options
- patent/copyright information

5.3 CLASSIFICATIONS IN PRACTICE

When matching existing or new security classification schemes against the definitions in 5.2, organisations must take business and sector specific requirements and sensitivities into account. Arbitrary mapping to the definitions above could lead to an inappropriate scheme that will be ignored by users.

Before sharing information with another organisation, a mutually acceptable classification scheme should be agreed. If existing classifications are used, these should be clearly related to their equivalent in the partner organisation. In this latter case mismatches between schemes should be handled by classifying information at a higher level. If one of your categories falls between two levels of your partner's scheme, it must be classified at the higher level to ensure that appropriate protection is given.

5.4 MARKINGS

Classified information should be appropriately marked or labelled for both physical and electronic formats. It is important good practice for the organisation to define procedures for marking/labelling information and for the handling of information in accordance with its classification (see section 6 of this booklet for some good practice on this subject).

5.5 DOWNGRADING

Some information is only sensitive or critical for a specific period of time. In such cases, the marking should indicate a date or event after which the information can be declassified or downgraded to a lower level. This avoids unnecessary protection of information.

5.6 DISPOSAL

When information is to be disposed of, appropriate precautions should be taken to ensure it is securely destroyed (see section 6 of this booklet for some good practice on this subject).

Before sharing information with another organisation, a mutually acceptable classification scheme should be agreed. If existing classifications are used, these should be clearly related to their equivalent in the partner organisation.

6 Information Protection and Control

Organisations can implement and maintain effective information security management by applying the processes for risk management and continuous review, monitoring and improvement specified in BS 7799 – 2 (Specification for an Information Security Management System), together with combinations of physical, technical and procedural controls described in ISO/IEC 17799 (the international Code of Practice for Information Security Management). The advice in this section is mainly drawn from ISO/IEC 17799.

The level of information protection required depends on the classification level that reflects information security requirements. The higher the level of sensitivity and/or criticality of the information, the greater the need for protection. For example, information classified as publicly available requires no controls to protect its confidentiality but may require levels of control to ensure its integrity and availability. On the other hand "confidential" or "strictly confidential" information does require confidentiality controls.

Specific controls can be selected based on the need to achieve a specific task or objective. Conversely, controls can be selected based on the need to achieve a specific level of strength/effectiveness. The controls outlined below should be considered for implementation appropriate to the level of classification and any other information security requirements.

6.1 HANDLING AND STORAGE OF PAPERS AND OTHER PHYSICAL MATERIAL AND MEDIA:

OBJECTIVE: To prevent unauthorised physical access, damage and interference to papers and other media. The protection required should be commensurate with the risks the business faces and the classification level of the information (references ISO/IEC 17799:2000 clauses 7.1 to 7.3).

INTEGRITY AND AVAILABILITY

Typical controls include:

- regular maintenance and testing of physical storage media
- development and implementation of appropriate handling procedures for papers and media containing information classified as medium or high integrity and/or availability
- storage of papers and other physical media in areas that are suitably protected from environmental risks

CONFIDENTIALITY

Typical controls to protect against unauthorised access include:

- physical entry controls to protect buildings and offices
- securing of individual offices, rooms and other facilities
- use of lockable cabinets, drawers and safes to ensure material is securely stored away when not in use
- clear desk policy i.e. put papers and media away when unattended and at the end of the day
- clear screen policy to ensure material cannot be observed by unauthorised people
- physical separation of papers with different classifications to ensure that strictly confidential information is not accidentally left with less sensitive information
- ensuring the user has the appropriate rights and privileges for physical access to information (depending on the level of classification)

6.2 HANDLING AND STORAGE OF INFORMATION IN ICT SYSTEMS

OBJECTIVE: To control access to information stored and processed by ICT systems (reference ISO/IEC 17799:2000 clauses 8.3.1, 8.6.3, 9.1).

INTEGRITY

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to ensure that only authorised persons can modify information
- ensuring input data is correct and complete, that processing is properly completed and that output validation is applied
- applying controls against malicious software to protect the integrity of information

AVAILABILITY

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to allow access by authorised persons and to ensure that only authorised persons can delete information
- controls against malicious software should be applied to protect the availability of information
- controls for information back-up should be in place to ensure its continued availability (see also 6.3)

CONFIDENTIALITY

Typical controls include:

- access controls (to control access to application system functions and user rights, such as read, write, delete and execute) should be in place in line with the business access control policy, to ensure that only authorised persons have access to the information
- protection of outputs from application systems (e.g. print outs) in accordance with their classification level
- regular reviews of distribution lists to ensure they are up to date and regular maintenance of formal records of recipients of information

6.3 INFORMATION BACKUP

OBJECTIVE: To maintain the integrity and availability of information (reference ISO/IEC 17799:2000 clause 8.4.1).

INTEGRITY, AVAILABILITY AND CONFIDENTIALITY

Typical controls include:

- take regular back-up copies of sensitive and/or critical business information
- give back-up information an appropriate level of protection against unauthorised access and physical and environmental risks
- ensure the protection given to back-up information is consistent with the standards applied to the information itself
- store a minimum level of back-up information (as well as accurate and complete records of the back-up copies) in a remote location
- adequate back-up arrangements and facilities should be provided and regularly tested to ensure that all critical business information can be recovered following a disaster or systems failure
- back-up and restoration procedures should be available and should be regularly checked and tested to ensure they remain effective

6.4 DISPOSAL OF INFORMATION

OBJECTIVE: To prevent loss, damage or compromise of assets (reference ISO/IEC 17799:2000 clause 7.2.6).

INTEGRITY AND AVAILABILITY

Typical controls include:

- information for disposal should be clearly and unambiguously identified and appropriate approval should be obtained (e.g. by the information owner) before disposal
- a record of all disposals should be kept

CONFIDENTIALITY

Typical controls include:

- dispose of office waste, using an approved company where appropriate
- destroy by approved cross-cut shredding, physical destruction, burning or pulping, carried out by a trusted approved person or organisation
- delete files on desk top computers, laptops and other devices (including backup copies) using a wipe utility to overwrite

6.5 DISPOSAL OR REUSE OF EQUIPMENT AND MEDIA

OBJECTIVE: To prevent loss, damage or compromise of assets (reference ISO/IEC 17799:2000 clauses 7.2.6 and 8.6.2).

INTEGRITY AND AVAILABILITY

Typical controls include:

- consider if damaged storage devices containing sensitive data require a risk assessment to determine if the items should be destroyed or discarded or whether they could be repaired and re-used
- test equipment and media prior to re-use to ensure reliable functioning
- overwrite removable media before re-use
- overwrite hard disc before relinquishing control of an IT system

CONFIDENTIALITY

Typical controls include:

- dispose of equipment and storage devices (sensitive information should be physically destroyed or securely overwritten rather than using the standard delete function)
- overwrite removable media before re-use
- overwrite hard discs before relinquishing control of an IT system
- use an approved company to destroy media which cannot be overwritten, or is damaged
- ensure all images, archive and back-up copies are destroyed or protected as appropriate and subsequently removed from the asset register

6.6 THIRD PARTY ACCESS AND OUTSOURCING

OBJECTIVE: To maintain the security of the organisation's information assets accessed by third parties (reference ISO/IEC 17799:2000 clauses 4.2-4.3).

INTEGRITY, AVAILABILITY AND CONFIDENTIALITY

(In the following, the term external party is used collectively to refer to a third party or the organisation to which information and/or services are outsourced). Typical controls include:

- identify the value and sensitivity of the information accessed by the external party, and its criticality to the business processes
- identify the forms and methods used for information exchange and implement appropriate controls
- take steps to ensure that the external party applies appropriate controls for the confidentiality, integrity and availability of the information processed and the services provided
- identify the types of access (e.g. physical or logical access) to be given, when and to whom, the risks resulting from this access, and the controls to be implemented, including those to identify and authenticate the external party
- assess the consequences and impact of any failure on the part of the external party handling information (i.e. disclosure of confidential information, or the modification, corruption or unavailability of information) and the remedial action to be taken as a result of any failure
- ensure a contract or agreement is in place which requires the external party to store and process information securely (addressing all the issues mentioned above) and to specify the controls in place for the protection of the confidentiality, integrity and availability of the organisation's information
- make sure any contract or agreement specifies how the external party addresses legal requirements related to the information involved
- take steps to ensure that a contract or agreement is in place and the specified security arrangements have been implemented before the external party is given access to the organisation's assets and systems.

6.7 EXCHANGES OF INFORMATION INCLUDING THE USE OF INTERNET AND OTHER PUBLICLY ACCESSIBLE NETWORKS

OBJECTIVE: To prevent loss, modification or misuse of information exchanged between organisations. This covers the security of media in transit, information sent via email as well as e-commerce and the use of other network services for transferring information (reference ISO/IEC 17799:2000 clause 8.7).

INTEGRITY AND AVAILABILITY

Typical controls include:

- verify the integrity of on-line transactions e.g. using electronic signatures
- check the integrity of electronically published information e.g. on the internet prior to publishing, and ensure the information is only published after appropriate authorisation
- review information that is electronically published e.g. on a website on a regular basis for accuracy and completeness

CONFIDENTIALITY

Typical controls include:

- protect physical media against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries
- protect internal systems from external connections and networked systems using an appropriately configured and maintained firewall
- ensure that information that is sensitive or critical is not stored on an ICT system connected in any way to the internet or other publicly accessible network (i.e. any network you don't control or trust)
- only send information that is sensitive over the internet or other publicly accessible network in an encrypted form (e.g. using currently available mechanisms such as SSL – Secure Sockets Layer)
- encrypt on-line transactions

6.8 SYSTEMS ACCEPTANCE AND CAPACITY PLANNING

OBJECTIVE: To minimise the risk of system failures and to ensure availability of adequate capacity and resources (reference ISO/IEC 17799:2000 clause 8.2).

INTEGRITY

Typical controls include:

- ensure the capacity of existing systems is sufficient to allow correct working and interaction of all business applications
- ensure system acceptance criteria have been met before new systems are put into operation; all associated controls and procedures should be in place
- error recovery and restart procedures (and business continuity arrangements) should be in place for new systems, to ensure that the system and the information processed on the system, is not corrupted
- test the correct functioning of new systems and the interaction with existing systems to ensure correct processing
- ensure users are given appropriate training in the operation of new systems

AVAILABILITY

Typical controls include:

- apply monitoring controls to identify current system use and potential problems, especially for important systems and system resources, and use controls to indicate capacity problems immediately
- make projections of future requirements, taking account of new business applications and related system requirements
- ensure new systems fulfil the identified performance and capacity requirements
- put error recovery and restart procedures in place for new systems, as well as business continuity and fallback arrangements, to ensure sufficient availability of the systems
- test the reliable working of new systems, taking into account the effect on existing systems, especially in peak processing times, to ensure the required availability of all systems
- train users in the operation of new systems

CONFIDENTIALITY

Typical controls include:

- identify confidentiality requirements of new systems and implement appropriate controls and procedures, ensuring the required confidentiality protection
- test new systems before introducing them, taking into account the possible effects on existing systems as well as the confidentiality of information processed

6.9 USER APPLICATIONS

OBJECTIVE: To prevent loss, modification or misuse of user data in application systems. This covers control of internal processing of information as well as input and output validation and checking of data in user applications (reference ISO/IEC 17799:2000 clause 10.2).

INTEGRITY

Typical controls include:

- put procedures in place to validate data input into systems to ensure it is correct and appropriate
- incorporate validation checks into processing systems to detect corruption and modification of data
- put procedures in place to ensure programmes run at the correct time and in the correct order
- use programmes correctly to ensure recovery from processing failures
- validate data output from application systems to ensure the processing of information is correct and appropriate
- identify and document all responsibilities in the data input, processing and output processes
- define procedures and actions for responding to any validation errors in the input, processing and output processes

AVAILABILITY

Typical controls include:

- keep, where necessary, the original data input into systems to ensure availability of the correct data in case of input or processing errors
- apply procedures to ensure programmes run in the right order and that no information is accidentally deleted or corrupted
- put procedures in place to recover from failures, to avoid any loss of information
- confirm expected outputs of application systems, to ensure information is not lost during processing

CONFIDENTIALITY

Typical controls include:

- check, prior to data input, that the file or application system into which the data is entered, has the appropriate confidentiality labelling (i.e. confidential information should be entered into a file marked ‘confidential’)
- put procedures in place to ensure that confidential data is not processed by application systems that do not have appropriate confidentiality controls in place
- put procedures in place to validate the confidentiality marking of outputs, to ensure they are appropriate to the content

6.10 MOBILE COMPUTING DEVICES AND PHONES AND SECURITY OF OTHER EQUIPMENT OFF-PREMISES

OBJECTIVE: To ensure information security is in place and appropriate when using mobile computing and teleworking facilities (reference ISO/IEC 17799:2000 clauses 7.2.5 and 9.8).

INTEGRITY, AVAILABILITY AND CONFIDENTIALITY

Typical controls include:

- warn company personnel not to discuss information of a sensitive or critical nature in public places to avoid being overheard or intercepted e.g. when using mobile phones, when travelling with colleagues or at external meetings or conferences
- ensure that the information security of off-site equipment is equivalent to that of on-site equipment used for the same level of information classification; this should take into account the risks of working outside the organisation's premises. For example documents, laptops and other mobile computing devices should be locked inside hotel safety deposit boxes or should be supervised at all times
- put in place protection for the connection of mobile devices to the organisation's networks; this should include user identification and authentication to avoid compromise of the information on the organisation's network, e.g. in case the equipment has been stolen
- put guidelines in place for protection against malicious code, and take appropriate backup of all information on mobile devices to protect against information loss should the equipment itself be lost or stolen

6.11 POSTAL AND COURIER SERVICES

OBJECTIVE: To ensure the protection of information being sent by post, avoiding disclosure, theft, damage, misuse or corruption of the information in transit.

INTEGRITY AND AVAILABILITY

Information being sent through the post should be protected against theft, damage, misuse or corruption during transportation beyond an organisation's physical boundaries. This can be done by:

- using a trustworthy courier service and using packaging that makes any attempt to access the content obvious
- asking the recipient to verify receipt and to confirm that the envelope or package does not appear to have been tampered with

CONFIDENTIALITY

Sensitive information should be protected against unauthorised access during transportation beyond an organisation's physical boundaries. Typical controls include:

- package sensitive information in such a way that the sensitivity level of the information is not externally apparent
- send information that is sensitive but not at the highest level in a single sealed envelope optionally marked 'to be opened by the addressee only'. If sent externally, no security marking should appear on the outer envelope
- the use of double envelopes is recommended for the highest levels of sensitive information and these should be sent by a trustworthy courier. The outer envelope should bear no security marking

6.12 FACSIMILE TRANSMISSIONS

OBJECTIVE: To ensure the protection of information being sent by fax, avoiding disclosure, misuse or loss.

INTEGRITY AND AVAILABILITY

Typical controls include:

- take steps to ensure that the fax is being sent to the right destination i.e. the correct number fax machine or other receiving equipment
- ask the recipient to confirm receipt by other means (e.g. phone or email) and to confirm transmission of the correct number of pages

CONFIDENTIALITY

Typical controls include:

- take steps to ensure that the fax is being sent to the correct destination i.e. fax machine or other receiving equipment,
- for the higher levels of sensitive information, confirm that the receiving equipment is ready to receive and that the machine is physically secured or attended by a trusted person

7 Integration into the broader business security regime

An organisation needs to view information protection as just one aspect of its security regime. Indeed this broader regime needs to provide the framework that enables information protection to be effective. This requires a combination of proactive management, monitoring and verification, and must be supported by security awareness among employees and, crucially, commitment from top management.

7.1 SECURITY CULTURE AND AWARENESS OF THE RISKS

It is vital that management and staff are aware of the risks. Keeping summary records of internal and external security incidents, and briefing staff on them and other threats, is of great value. Ongoing awareness programmes are essential.

The OECD Guidelines for the Security of Information Systems and Networks emphasise the importance of awareness in the following terms: "Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks." The Guidelines go on to say that all users of systems should: "… understand that security failures may significantly harm systems and networks under their control." As part of awareness they also need to know: "… good practices that they can implement to enhance security". Organisations must implement appropriate programmes to develop such awareness and knowledge, and must ensure that they are regularly reviewed and updated.

7.2 INFORMATION SECURITY POLICY

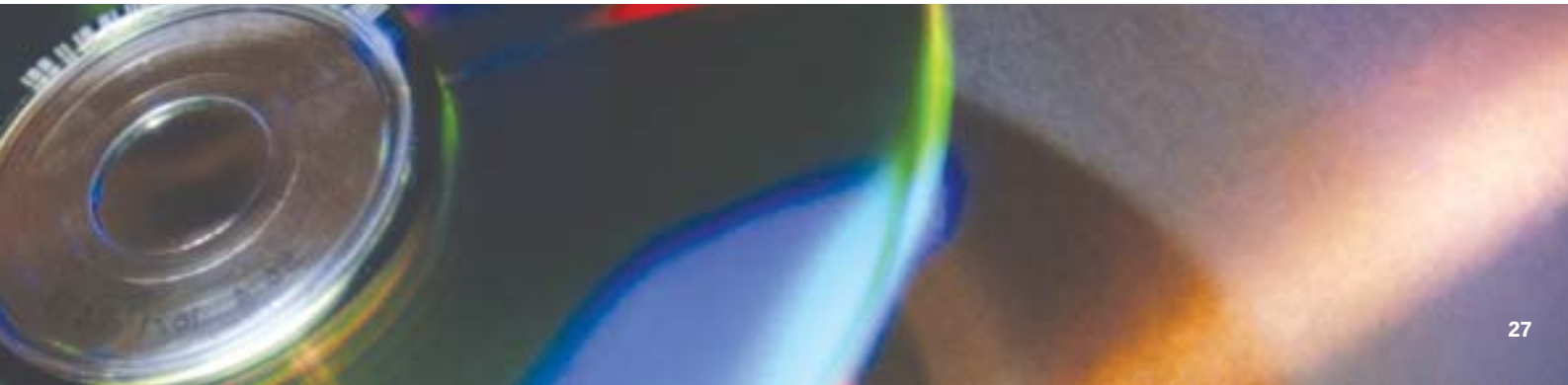
The organisation should have a policy in place which demonstrates management commitment and its approach to managing information security and the protection of its information assets (the DTI publication, "Information Security: A Business Manager's Guide" URN 04/623 includes a security policy template). This policy should cover all types of information and will apply to information owned by the organisation or owned by someone else but in the care of the organisation. At a minimum this policy should:

- make statements about the business objectives, scope and importance of information security as an enabling mechanism for information sharing within the organisation
- recognise the need for necessary security resources
- define clear responsibilities and accountabilities for information security
- provide a framework for the management of risk and setting control objectives and controls proportionate to the assessed risks
- ensure regular monitoring and reporting of security performance and incidents
- appoint an Information Security Manager to maintain the policy and to provide guidance on security measures
- ensure clear and simple security standards are developed and are followed by employees.

7.3 INFORMATION SECURITY MANAGEMENT PROCESSES

Effective protection can be implemented as a proactive management system with a process cycle for establishing, monitoring and ensuring continual improvement of the organisation's information security.

The diagram below is the model used in BS 7799-2:2002 for such a system:



7.4 BUSINESS PARTNERS AND THIRD PARTY ACCESS

Exchanging information between organisations, business partners and third party suppliers should be simplified if all parties follow this guidance. Secure sharing of sensitive and critical information is always important, but especially during activities such as:

- forming or operating a joint venture. This might involve exchanging sensitive strategies, marketing plans, commercial information and product plans
- contracting out work which is likely to involve handling sensitive information
- negotiating with other organisations, perhaps as part of a company disposal, merger or acquisition and,
- discussions with Government.

If sensitive or critical information is given to another organisation, you should ensure that the other party understands the need for protection and agrees to take appropriate measures. They can follow the guidance in this booklet which should help them to give appropriate protection to information bearing a unified classification marking.

You may wish to satisfy yourself that they meet your security requirements, either by self-audit or external audit review.

You should also consider including confidentiality clauses and other security requirements in contracts with third parties. These might reference this guidance and specify how it applies to your organisation. Effective security measures will only work if everyone involved is familiar with appropriate security procedures.

When information is passed to another organisation, it should be marked with the appropriate classification label. The receiving organisation should handle and protect it appropriately.

In some circumstances, for example where there is a higher level of threat, you may need to give the recipient additional advice and build special security provisions into contracts.

7.5 ASSURANCE

It is important that security policies and standards are followed and that these standards are in line with good practice guidance. You could achieve this using one of the following methods:

- First party audit, internal self-assessment/audit, based on limited implementation of this guidance.
- Second party audit or peer assessment in which case organisations exchanging sensitive information might agree with each other the scope of compliance. This would typically involve a combination of self-assessment and peer assessment, based on implementation of this guidance. Contractual agreements should make it clear that detailed security arrangements within each other's organisation will remain in line with stated minimum standards.
- Third party audit or assessment. Organisations are externally reviewed and formally certified e.g. against the requirements of BS 7799-2:2002. Each organisation must fully implement its own documented security procedures taken from the minimum standards, as well as any facilities it documents as 'approved'.

This assurance can then be relied upon within contractual arrangements, without the need for contract-specific agreements and verification. Each approved facility should be documented, showing the grounds for approval. The documented security procedures and approvals should be made available on request to any organisation which has signed a confidentiality agreement and with which confidential information is shared.

Annex 1
Marking Correspondence Matrix

This publication is intended to replace two previous DTI publications: “Protecting Business Information: Understanding the Risks” (URN96/939) and “Protecting Business Information: Keeping it Confidential” (URN96/938).

The following matrix shows an approximate correspondence between classification markings defined in “Protecting Business Information: Keeping it Confidential”, and the markings defined in this guide. It is important to note that the marking in the previous publication only covered the confidentiality aspect of information security, whereas this guide also covers integrity and availability.

URN 96/938 Marking Scheme	Marking scheme in this guide for confidentiality
	PUBLICLY AVAILABLE
SEC1	INTERNAL USE ONLY
SEC2	CONFIDENTIAL
SEC3	STRICTLY CONFIDENTIAL

Annex 2 References

1. ISO/IEC 17799:2000, Information technology – Code of practice for information security management.
2. BS 7799-2: 2002 – Information security management systems – Specification with guidance for use.
3. ISO Guide 73: 2002, Risk management – Vocabulary – Guidelines for use in standards.
4. ISO/IEC TR18044: 2004, Information technology – Security techniques – Information security incident management.
5. Information Security: A Business Manager's Guide (URN 04/623: 04/04).
6. Data Protection Act 1998.
7. Companies Act 1989.

Annex 3 Acknowledgements

The guidance in this booklet has been developed by the following companies, organisations and government departments:

AEXIS Security Consultants

British Computer Society

British Standards Institution

British Telecommunications plc

Cabinet Office

Department of Trade and Industry

Communications-Electronics Security Group

ISMS International User Group

Pfizer Global Pharmaceuticals

QinetiQ Ltd

Reuters

Royal Bank of Scotland

Sapphire Technologies Ltd

Shell International Ltd

Symantec

The Royal Military College of Science

XiSEC Consultants Ltd

Further help and advice

INFORMATION SECURITY ISSUES

For help and advice on information security issues contact:

The Information Security Policy Team
Department of Trade and Industry
151 Buckingham Palace Road
London SW1W 9SS
Tel: 020 7215 1962
Fax: 020 7215 1966
E-mail: InfosecPolicyTeam@dti.gsi.gov.uk

Further guidance and a full listing of all our information security publications can be found at: www.dti.gov.uk/industries/information_security

Or look at our information security business advice pages at: www.dti.gov.uk/bestpractice/infosec

ACHIEVING BEST PRACTICE IN YOUR BUSINESS

Achieving best practice in your business is a key theme within DTI's approach to business support solutions, providing ideas and insights into how you can improve performance across your business. By showing what works in other businesses, we can help you see what approaches can help you, and then support you in implementation.

To access free information and publications on best practice:

- visit our website at www.dti.gov.uk/bestpractice
- call the DTI Publications Orderline on 0870 150 2500 or visit www.dti.gov.uk/publications

SUPPORT TO IMPLEMENT BEST BUSINESS PRACTICE

To get help bringing best practice to your business, contact Business Link – the national business advice service. Backed by the DTI, Business Link is an easy-to-use business support and information service, which can put you in touch with one of its network of experienced business advisers:

- Visit the Business Link website at www.businesslink.gov.uk
- Call Business Link on 0845 600 9 006.

GENERAL BUSINESS ADVICE
You can also get a range of general business advice from the following organisations:

England
- Call Business Link on 0845 600 9 006
- Visit the website at www.businesslink.gov.uk

Scotland
- Call Business Gateway on 0845 609 6611
- Visit the website at www.bgateway.com

Wales
- Call Business Eye/Llygad Busnes on 08457 96 97 98
- Visit the website at www.businesseye.org.uk

Northern Ireland
- Call Invest Northern Ireland on 028 9023 9090
- Visit the website at www.investni.com

Published by the Department of Trade and Industry. www.dti.gov.uk