BRITISH STANDARD

BS ISO/IEC 27002:2005
BS 7799-1:2005
Incorporating corrigendum no. 1

Information technology — Security techniques — Code of practice for information security management

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

British Standards
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

National foreword

This British Standard is the UK implementation of ISO/IEC 27002:2005, incorporating corrigendum July 2007. It supersedes BS ISO/IEC 17799:2000 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security Techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 16 June 2005

© BSI 2007

ISBN 978 0 580 59729 9

Amendments issued since publication

Amd. No.	Date	Comments
17310 Corrigendum No. 1	31 July 2007	Identifier of standard renumbered from (BS) ISO/IEC 17799 to (BS) ISO/IEC 27002

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2005-06-15

Information technology — Security techniques — Code of practice for information security management

Technologies de l'information — Techniques de sécurité — Code de pratique pour la gestion de sécurité d'information

Reference number
ISO/IEC 27002:2005(E)

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Contents

Page

FOREWORD ..... **VII**

0 INTRODUCTION ..... **VIII**

0.1 WHAT IS INFORMATION SECURITY? VIII
0.2 WHY INFORMATION SECURITY IS NEEDED? VIII
0.3 HOW TO ESTABLISH SECURITY REQUIREMENTS IX
0.4 ASSESSING SECURITY RISKS IX
0.5 SELECTING CONTROLS IX
0.6 INFORMATION SECURITY STARTING POINT IX
0.7 CRITICAL SUCCESS FACTORS X
0.8 DEVELOPING YOUR OWN GUIDELINES XI

1 SCOPE **1**

2 TERMS AND DEFINITIONS **1**

3 STRUCTURE OF THIS STANDARD **4**

3.1 CLAUSES 4
3.2 MAIN SECURITY CATEGORIES 4

4 RISK ASSESSMENT AND TREATMENT **5**

4.1 ASSESSING SECURITY RISKS 5
4.2 TREATING SECURITY RISKS 5

5 SECURITY POLICY **7**

5.1 INFORMATION SECURITY POLICY 7
5.1.1 Information security policy document *7*
5.1.2 Review of the information security policy *8*

6 ORGANIZATION OF INFORMATION SECURITY **9**

6.1 INTERNAL ORGANIZATION 9
6.1.1 Management commitment to information security *9*
6.1.2 Information security co-ordination *10*
6.1.3 Allocation of information security responsibilities *10*
6.1.4 Authorization process for information processing facilities *11*
6.1.5 Confidentiality agreements *11*
6.1.6 Contact with authorities *12*
6.1.7 Contact with special interest groups *12*
6.1.8 Independent review of information security *13*
6.2 EXTERNAL PARTIES 14
6.2.1 Identification of risks related to external parties *14*
6.2.2 Addressing security when dealing with customers *15*
6.2.3 Addressing security in third party agreements *16*

7 ASSET MANAGEMENT **19**

7.1 RESPONSIBILITY FOR ASSETS 19
7.1.1 Inventory of assets *19*
7.1.2 Ownership of assets *20*
7.1.3 Acceptable use of assets *20*
7.2 INFORMATION CLASSIFICATION 21
7.2.1 Classification guidelines *21*
7.2.2 Information labeling and handling *21*

8 HUMAN RESOURCES SECURITY **23**

8.1 PRIOR TO EMPLOYMENT 23
8.1.1 Roles and responsibilities *23*

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

8.1.2 Screening ... *23*
8.1.3 Terms and conditions of employment ... *24*
8.2 DURING EMPLOYMENT ... 25
8.2.1 Management responsibilities ... *25*
8.2.2 Information security awareness, education, and training ... *26*
8.2.3 Disciplinary process ... *26*
8.3 TERMINATION OR CHANGE OF EMPLOYMENT ... 27
8.3.1 Termination responsibilities ... *27*
8.3.2 Return of assets ... *27*
8.3.3 Removal of access rights ... *28*

9 PHYSICAL AND ENVIRONMENTAL SECURITY ... 29

9.1 SECURE AREAS ... 29
9.1.1 Physical security perimeter ... *29*
9.1.2 Physical entry controls ... *30*
9.1.3 Securing offices, rooms, and facilities ... *30*
9.1.4 Protecting against external and environmental threats ... *31*
9.1.5 Working in secure areas ... *31*
9.1.6 Public access, delivery, and loading areas ... *32*
9.2 EQUIPMENT SECURITY ... 32
9.2.1 Equipment siting and protection ... *32*
9.2.2 Supporting utilities ... *33*
9.2.3 Cabling security ... *34*
9.2.4 Equipment maintenance ... *34*
9.2.5 Security of equipment off-premises ... *35*
9.2.6 Secure disposal or re-use of equipment ... *35*
9.2.7 Removal of property ... *36*

10 COMMUNICATIONS AND OPERATIONS MANAGEMENT ... 37

10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES ... 37
10.1.1 Documented operating procedures ... *37*
10.1.2 Change management ... *37*
10.1.3 Segregation of duties ... *38*
10.1.4 Separation of development, test, and operational facilities ... *38*
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT ... 39
10.2.1 Service delivery ... *39*
10.2.2 Monitoring and review of third party services ... *40*
10.2.3 Managing changes to third party services ... *40*
10.3 SYSTEM PLANNING AND ACCEPTANCE ... 41
10.3.1 Capacity management ... *41*
10.3.2 System acceptance ... *41*
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE ... 42
10.4.1 Controls against malicious code ... *42*
10.4.2 Controls against mobile code ... *43*
10.5 BACK-UP ... 44
10.5.1 Information back-up ... *44*
10.6 NETWORK SECURITY MANAGEMENT ... 45
10.6.1 Network controls ... *45*
10.6.2 Security of network services ... *46*
10.7 MEDIA HANDLING ... 46
10.7.1 Management of removable media ... *46*
10.7.2 Disposal of media ... *47*
10.7.3 Information handling procedures ... *47*
10.7.4 Security of system documentation ... *48*
10.8 EXCHANGE OF INFORMATION ... 48
10.8.1 Information exchange policies and procedures ... *49*
10.8.2 Exchange agreements ... *50*
10.8.3 Physical media in transit ... *51*
10.8.4 Electronic messaging ... *52*
10.8.5 Business information systems ... *52*

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

10.9 ELECTRONIC COMMERCE SERVICES 53
10.9.1 Electronic commerce 53
10.9.2 On-Line Transactions 54
10.9.3 Publicly available information 55
10.10 MONITORING 55
10.10.1 Audit logging 55
10.10.2 Monitoring system use 56
10.10.3 Protection of log information 57
10.10.4 Administrator and operator logs 58
10.10.5 Fault logging 58
10.10.6 Clock synchronization 58

11 ACCESS CONTROL 60

11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 60
11.1.1 Access control policy 60
11.2 USER ACCESS MANAGEMENT 61
11.2.1 User registration 61
11.2.2 Privilege management 62
11.2.3 User password management 62
11.2.4 Review of user access rights 63
11.3 USER RESPONSIBILITIES 63
11.3.1 Password use 64
11.3.2 Unattended user equipment 64
11.3.3 Clear desk and clear screen policy 65
11.4 NETWORK ACCESS CONTROL 65
11.4.1 Policy on use of network services 66
11.4.2 User authentication for external connections 66
11.4.3 Equipment identification in networks 67
11.4.4 Remote diagnostic and configuration port protection 67
11.4.5 Segregation in networks 68
11.4.6 Network connection control 68
11.4.7 Network routing control 69
11.5 OPERATING SYSTEM ACCESS CONTROL 69
11.5.1 Secure log-on procedures 69
11.5.2 User identification and authentication 70
11.5.3 Password management system 71
11.5.4 Use of system utilities 72
11.5.5 Session time-out 72
11.5.6 Limitation of connection time 72
11.6 APPLICATION AND INFORMATION ACCESS CONTROL 73
11.6.1 Information access restriction 73
11.6.2 Sensitive system isolation 74
11.7 MOBILE COMPUTING AND TELEWORKING 74
11.7.1 Mobile computing and communications 74
11.7.2 Teleworking 75

12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 77

12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS 77
12.1.1 Security requirements analysis and specification 77
12.2 CORRECT PROCESSING IN APPLICATIONS 78
12.2.1 Input data validation 78
12.2.2 Control of internal processing 78
12.2.3 Message integrity 79
12.2.4 Output data validation 79
12.3 CRYPTOGRAPHIC CONTROLS 80
12.3.1 Policy on the use of cryptographic controls 80
12.3.2 Key management 81
12.4 SECURITY OF SYSTEM FILES 83
12.4.1 Control of operational software 83
12.4.2 Protection of system test data 84

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

12.4.3 Access control to program source code ... *84*
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES ... 85
12.5.1 Change control procedures ... *85*
12.5.2 Technical review of applications after operating system changes ... *86*
12.5.3 Restrictions on changes to software packages ... *86*
12.5.4 Information leakage ... *87*
12.5.5 Outsourced software development ... *87*
12.6 TECHNICAL VULNERABILITY MANAGEMENT ... 88
12.6.1 Control of technical vulnerabilities ... *88*

13 INFORMATION SECURITY INCIDENT MANAGEMENT ... 90

13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES ... 90
13.1.1 Reporting information security events ... *90*
13.1.2 Reporting security weaknesses ... *91*
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS ... 91
13.2.1 Responsibilities and procedures ... *92*
13.2.2 Learning from information security incidents ... *93*
13.2.3 Collection of evidence ... *93*

14 BUSINESS CONTINUITY MANAGEMENT ... 95

14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT ... 95
14.1.1 Including information security in the business continuity management process ... *95*
14.1.2 Business continuity and risk assessment ... *96*
14.1.3 Developing and implementing continuity plans including information security ... *96*
14.1.4 Business continuity planning framework ... *97*
14.1.5 Testing, maintaining and re-assessing business continuity plans ... *98*

15 COMPLIANCE ... 100

15.1 COMPLIANCE WITH LEGAL REQUIREMENTS ... 100
15.1.1 Identification of applicable legislation ... *100*
15.1.2 Intellectual property rights (IPR) ... *100*
15.1.3 Protection of organizational records ... *101*
15.1.4 Data protection and privacy of personal information ... *102*
15.1.5 Prevention of misuse of information processing facilities ... *102*
15.1.6 Regulation of cryptographic controls ... *103*
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE ... 103
15.2.1 Compliance with security policies and standards ... *104*
15.2.2 Technical compliance checking ... *104*
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS ... 105
15.3.1 Information systems audit controls ... *105*
15.3.2 Protection of information systems audit tools ... *105*

BIBLIOGRAPHY ... 107

INDEX ... 108

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27002 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 17799:2000), which has been technically revised.

A family of Information Security Management System (ISMS) International Standards is being developed within ISO/IEC JTC 1/SC 27. The family includes International Standards on information security management system requirements, risk management, metrics and measurement, and implementation guidance. This family will adopt a numbering scheme using the series of numbers 27000 et seq.

From 2007, it is proposed to incorporate the new edition of ISO/IEC 17799 into this new numbering scheme as ISO/IEC 27002.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

0 Introduction

0.1 What is information security?

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see also OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

0.2 Why information security is needed?

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage such as malicious code, computer hacking, and denial of service attacks have become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties. Specialist advice from outside organizations may also be needed.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

0.3 How to establish security requirements

It is essential that an organization identifies its security requirements. There are three main sources of security requirements.

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.

3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations.

0.4 Assessing security risks

Security requirements are identified by a methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures.

The results of the risk assessment will help to guide and determine the appropriate management action and priorities for managing information security risks, and for implementing controls selected to protect against these risks.

Risk assessment should be repeated periodically to address any changes that might influence the risk assessment results.

More information about the assessment of security risks can be found in clause 4.1 "Assessing security risks".

0.5 Selecting controls

Once security requirements and risks have been identified and decisions for the treatment of risks have been made, appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level. Controls can be selected from this standard or from other control sets, or new controls can be designed to meet specific needs as appropriate. The selection of security controls is dependent upon organizational decisions based on the criteria for risk acceptance, risk treatment options, and the general risk management approach applied to the organization, and should also be subject to all relevant national and international legislation and regulations.

Some of the controls in this standard can be considered as guiding principles for information security management and applicable for most organizations. They are explained in more detail below under the heading "Information security starting point".

More information about selecting controls and other risk treatment options can be found in clause 4.2 "Treating security risks".

0.6 Information security starting point

A number of controls can be considered as a good starting point for implementing information security. They are either based on essential legislative requirements or considered to be common practice for information security.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Controls considered to be essential to an organization from a legislative point of view include, depending on applicable legislation:

a) data protection and privacy of personal information (see 15.1.4);

b) protection of organizational records (see 15.1.3);

c) intellectual property rights (see 15.1.2).

Controls considered to be common practice for information security include:

a) information security policy document (see 5.1.1);

b) allocation of information security responsibilities (see 6.1.3);

c) information security awareness, education, and training (see 8.2.2);

d) correct processing in applications (see 12.2);

e) technical vulnerability management (see 12.6);

f) business continuity management (see 14);

g) management of information security incidents and improvements (see 13.2).

These controls apply to most organizations and in most environments.

It should be noted that although all controls in this standard are important and should be considered, the relevance of any control should be determined in the light of the specific risks an organization is facing. Hence, although the above approach is considered a good starting point, it does not replace selection of controls based on a risk assessment.

0.7 Critical success factors

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

a) information security policy, objectives, and activities that reflect business objectives;

b) an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture;

c) visible support and commitment from all levels of management;

d) a good understanding of the information security requirements, risk assessment, and risk management;

e) effective marketing of information security to all managers, employees, and other parties to achieve awareness;

f) distribution of guidance on information security policy and standards to all managers, employees and other parties;

g) provision to fund information security management activities;

h) providing appropriate awareness, training, and education;

i) establishing an effective information security incident management process;

j) implementation of a measurement [1] system that is used to evaluate performance in information security management and feedback suggestions for improvement.

[1] Note that information security measurements are outside of the scope of this standard.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

0.8 Developing your own guidelines

This code of practice may be regarded as a starting point for developing organization specific guidelines. Not all of the controls and guidance in this code of practice may be applicable. Furthermore, additional controls and guidelines not included in this standard may be required. When documents are developed containing additional guidelines or controls, it may be useful to include cross-references to clauses in this standard where applicable to facilitate compliance checking by auditors and business partners.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

blank

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Information technology — Security techniques — Code of practice for information security management

1 Scope

This International Standard establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined in this International Standard provide general guidance on the commonly accepted goals of information security management.

The control objectives and controls of this International Standard are intended to be implemented to meet the requirements identified by a risk assessment. This International Standard may serve as a practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1

asset
anything that has value to the organization
[ISO/IEC 13335-1:2004]

2.2

control
means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
NOTE Control is also used as a synonym for safeguard or countermeasure.

2.3

guideline
a description that clarifies what should be done and how, to achieve the objectives set out in policies
[ISO/IEC 13335-1:2004]

2.4

information processing facilities
any information processing system, service or infrastructure, or the physical locations housing them

2.5

information security
preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved

2.6

information security event
an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant
[ISO/IEC TR 18044:2004]

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

2.7

information security incident
an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security
[ISO/IEC TR 18044:2004]

2.8

policy
overall intention and direction as formally expressed by management

2.9

risk
combination of the probability of an event and its consequence
[ISO/IEC Guide 73:2002]

2.10

risk analysis
systematic use of information to identify sources and to estimate the risk
[ISO/IEC Guide 73:2002]

2.11

risk assessment
overall process of risk analysis and risk evaluation
[ISO/IEC Guide 73:2002]

2.12

risk evaluation
process of comparing the estimated risk against given risk criteria to determine the significance of the risk
[ISO/IEC Guide 73:2002]

2.13

risk management
coordinated activities to direct and control an organization with regard to risk
NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.
[ISO/IEC Guide 73:2002]

2.14

risk treatment
process of selection and implementation of measures to modify risk
[ISO/IEC Guide 73:2002]

2.15

third party
that person or body that is recognized as being independent of the parties involved, as concerns the issue in question
[ISO/IEC Guide 2:1996]

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

2.16

threat
a potential cause of an unwanted incident, which may result in harm to a system or organization
[ISO/IEC 13335-1:2004]

2.17

vulnerability
a weakness of an asset or group of assets that can be exploited by one or more threats
[ISO/IEC 13335-1:2004]

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

3 Structure of this standard

This standard contains 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment.

3.1 Clauses

Each clause contains a number of main security categories. The eleven clauses (accompanied with the number of main security categories included within each clause) are:

a) Security Policy (1);

b) Organizing Information Security (2);

c) Asset Management (2);

d) Human Resources Security (3);

e) Physical and Environmental Security (2);

f) Communications and Operations Management (10);

g) Access Control (7);

h) Information Systems Acquisition, Development and Maintenance (6);

i) Information Security Incident Management (2);

j) Business Continuity Management (1);

k) Compliance (3).

Note: The order of the clauses in this standard does not imply their importance. Depending on the circumstances, all clauses could be important, therefore each organization applying this standard should identify applicable clauses, how important these are and their application to individual business processes. Also, all lists in this standard are not in priority order unless so noted.

3.2 Main security categories

Each main security category contains:

a) a control objective stating what is to be achieved; and

b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control

Defines the specific control statement to satisfy the control objective.

Implementation guidance

Provides more detailed information to support the implementation of the control and meeting the control objective. Some of this guidance may not be suitable in all cases and so other ways of implementing the control may be more appropriate.

Other information

Provides further information that may need to be considered, for example legal considerations and references to other standards.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

4 Risk assessment and treatment

4.1 Assessing security risks

Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The information security risk assessment should have a clearly defined scope in order to be effective and should include relationships with risk assessments in other areas, if appropriate.

The scope of a risk assessment can be either the whole organization, parts of the organization, an individual information system, specific system components, or services where this is practicable, realistic, and helpful. Examples of risk assessment methodologies are discussed in ISO/IEC TR 13335-3 (Guidelines for the Management of IT Security: Techniques for the Management of IT Security).

4.2 Treating security risks

Before considering the treatment of a risk, the organization should decide criteria for determining whether or not risks can be accepted. Risks may be accepted if, for example, it is assessed that the risk is low or that the cost of treatment is not cost-effective for the organization. Such decisions should be recorded.

For each of the risks identified following the risk assessment a risk treatment decision needs to be made. Possible options for risk treatment include:

a) applying appropriate controls to reduce the risks;
b) knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance;
c) avoiding risks by not allowing actions that would cause the risks to occur;
d) transferring the associated risks to other parties, e.g. insurers or suppliers.

For those risks where the risk treatment decision has been to apply appropriate controls, these controls should be selected and implemented to meet the requirements identified by a risk assessment. Controls should ensure that risks are reduced to an acceptable level taking into account:

a) requirements and constraints of national and international legislation and regulations;

b) organizational objectives;

c) operational requirements and constraints;

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

d) cost of implementation and operation in relation to the risks being reduced, and remaining proportional to the organization's requirements and constraints;

e) the need to balance the investment in implementation and operation of controls against the harm likely to result from security failures.

Controls can be selected from this standard or from other control sets, or new controls can be designed to meet the specific needs of the organization. It is necessary to recognize that some controls may not be applicable to every information system or environment, and might not be practicable for all organizations. As an example, 10.1.3 describes how duties may be segregated to prevent fraud and error. It may not be possible for smaller organizations to segregate all duties and other ways of achieving the same control objective may be necessary. As another example, 10.10 describes how system use can be monitored and evidence collected. The described controls e.g. event logging, might conflict with applicable legislation, such as privacy protection for customers or in the workplace.

Information security controls should be considered at the systems and projects requirements specification and design stage. Failure to do so can result in additional costs and less effective solutions, and maybe, in the worst case, inability to achieve adequate security.

It should be kept in mind that no set of controls can achieve complete security, and that additional management action should be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support the organization's aims.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

5 Security policy

5.1 Information security policy

Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 Information security policy document

Control

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

Implementation guidance

The information security policy document should state management commitment and set out the organization's approach to managing information security. The policy document should contain statements concerning:

a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing (see introduction);

b) a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives;

c) a framework for setting control objectives and controls, including the structure of risk assessment and risk management;

d) a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including:

   1) compliance with legislative, regulatory, and contractual requirements;

   2) security education, training, and awareness requirements;

   3) business continuity management;

   4) consequences of information security policy violations;

e) a definition of general and specific responsibilities for information security management, including reporting information security incidents;

f) references to documentation which may support the policy, e.g. more detailed security policies and procedures for specific information systems or security rules users should comply with.

This information security policy should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader.

Other information

The information security policy might be a part of a general policy document. If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information. Further information can be found in the ISO/IEC 13335-1:2004.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

5.1.2 Review of the information security policy

Control

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

Implementation guidance

The information security policy should have an owner who has approved management responsibility for the development, review, and evaluation of the security policy. The review should include assessing opportunities for improvement of the organization's information security policy and approach to managing information security in response to changes to the organizational environment, business circumstances, legal conditions, or technical environment.

The review of the information security policy should take account of the results of management reviews. There should be defined management review procedures, including a schedule or period of the review.

The input to the management review should include information on:

a) feedback from interested parties;

b) results of independent reviews (see 6.1.8);

c) status of preventive and corrective actions (see 6.1.8 and 15.2.1);

d) results of previous management reviews;

e) process performance and information security policy compliance;

f) changes that could affect the organization's approach to managing information security, including changes to the organizational environment, business circumstances, resource availability, contractual, regulatory, and legal conditions, or to the technical environment;

g) trends related to threats and vulnerabilities;

h) reported information security incidents (see 13.1);

i) recommendations provided by relevant authorities (see 6.1.6).

The output from the management review should include any decisions and actions related to:

a) improvement of the organization's approach to managing information security and its processes;

b) improvement of control objectives and controls;

c) improvement in the allocation of resources and/or responsibilities.

A record of the management review should be maintained.

Management approval for the revised policy should be obtained.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

6 Organization of information security

6.1 Internal organization

Objective: To manage information security within the organization.

A management framework should be established to initiate and control the implementation of information security within the organization.

Management should approve the information security policy, assign security roles and co-ordinate and review 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 or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

6.1.1 Management commitment to information security

Control

Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

Implementation guidance

Management should:

a) ensure that information security goals are identified, meet the organizational requirements, and are integrated in relevant processes;

b) formulate, review, and approve information security policy;

c) review the effectiveness of the implementation of the information security policy;

d) provide clear direction and visible management support for security initiatives;

e) provide the resources needed for information security;

f) approve assignment of specific roles and responsibilities for information security across the organization;

g) initiate plans and programs to maintain information security awareness;

h) ensure that the implementation of information security controls is co-ordinated across the organization (see 6.1.2).

Management should identify the needs for internal or external specialist information security advice, and review and coordinate results of the advice throughout the organization.

Depending on the size of the organization, such responsibilities could be handled by a dedicated management forum or by an existing management body, such as the board of directors.

Other information

Further information is contained in ISO/IEC 13335-1:2004.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

6.1.2 Information security co-ordination

Control

Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

Implementation guidance

Typically, information security co-ordination should involve the co-operation and collaboration of managers, users, administrators, application designers, auditors and security personnel, and specialist skills in areas such as insurance, legal issues, human resources, IT or risk management. This activity should:

a) ensure that security activities are executed in compliance with the information security policy;

b) identify how to handle non-compliances;

c) approve methodologies and processes for information security, e.g. risk assessment, information classification;

d) identify significant threat changes and exposure of information and information processing facilities to threats;

e) assess the adequacy and co-ordinate the implementation of information security controls;

f) effectively promote information security education, training and awareness throughout the organization;

g) evaluate information received from the monitoring and reviewing of information security incidents, and recommend appropriate actions in response to identified information security incidents.

If the organization does not use a separate cross-functional group, e.g. because such a group is not appropriate for the organization's size, the actions described above should be undertaken by another suitable management body or individual manager.

6.1.3 Allocation of information security responsibilities

Control

All information security responsibilities should be clearly defined.

Implementation guidance

Allocation of information security responsibilities should be done in accordance with the information security policy (see clause 4). Responsibilities for the protection of individual assets and for carrying out specific security processes should be clearly identified. This responsibility should be supplemented, where necessary, with more detailed guidance for specific sites and information processing facilities. Local responsibilities for the protection of assets and for carrying out specific security processes, such as business continuity planning, should be clearly defined.

Individuals with allocated security responsibilities may delegate security tasks to others. Nevertheless they remain responsible and should determine that any delegated tasks have been correctly performed.

Areas for which individuals are responsible should be clearly stated; in particular the following should take place:

a) the assets and security processes associated with each particular system should be identified and clearly defined;

b) the entity responsible for each asset or security process should be assigned and the details of this responsibility should be documented (see also 7.1.2);

c) authorization levels should be clearly defined and documented.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Other information
In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.

However, responsibility for resourcing and implementing the controls will often remain with individual managers. One common practice is to appoint an owner for each asset who then becomes responsible for its day-to-day protection.

6.1.4 Authorization process for information processing facilities

Control
A management authorization process for new information processing facilities should be defined and implemented.

Implementation guidance
The following guidelines should be considered for the authorization process:

a) new facilities should have appropriate user management authorization, authorizing their purpose and use. Authorization should also be obtained from the manager responsible for maintaining the local information system security environment to ensure that all relevant security policies and requirements are met;

b) where necessary, hardware and software should be checked to ensure that they are compatible with other system components;

c) the use of personal or privately owned information processing facilities, e.g. laptops, home-computers or hand-held devices, for processing business information, may introduce new vulnerabilities and necessary controls should be identified and implemented.

6.1.5 Confidentiality agreements

Control
Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.

Implementation guidance
Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);

b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;

c) required actions when an agreement is terminated;

d) responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know');

e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;

f) the permitted use of confidential information, and rights of the signatory to use information;

g) the right to audit and monitor activities that involve confidential information;

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

h) process for notification and reporting of unauthorized disclosure or confidential information breaches;

i) terms for information to be returned or destroyed at agreement cessation; and

j) expected actions to be taken in case of a breach of this agreement.

Based on an organization's security requirements, other elements may be needed in a confidentiality or non-disclosure agreement.

Confidentiality and non-disclosure agreements should comply with all applicable laws and regulations for the jurisdiction to which it applies (see also 15.1.1).

Requirements for confidentiality and non-disclosure agreements should be reviewed periodically and when changes occur that influence these requirements.

Other Information
Confidentiality and non-disclosure agreements protect organisational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorised manner.

There may be a need for an organisation to use different forms of confidentiality or non-disclose agreements in different circumstances.

6.1.6 Contact with authorities

Control
Appropriate contacts with relevant authorities should be maintained.

Implementation guidance
Organizations should have procedures in place that specify when and by whom authorities (e.g. law enforcement, fire department, supervisory authorities) should be contacted, and how identified information security incidents should be reported in a timely manner if it is suspected that laws may have been broken.

Organizations under attack from the Internet may need external third parties (e.g. an Internet service provider or telecommunications operator) to take action against the attack source.

Other information
Maintaining such contacts may be a requirement to support information security incident management (Section 13.2) or the business continuity and contingency planning process (Section 14). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in law or regulations, which have to be followed by the organization. Contacts with other authorities include utilities, emergency services, and health and safety, e.g. fire departments (in connection with business continuity), telecommunication providers (in connection with line routing and availability), water suppliers (in connection with cooling facilities for equipment).

6.1.7 Contact with special interest groups

Control
Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

Implementation guidance
Membership in special interest groups or forums should be considered as a means to:

a) improve knowledge about best practices and staying up to date with relevant security information;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

b) ensure the understanding of the information security environment is current and complete;

c) receive early warnings of alerts, advisories, and patches pertaining to attacks and vulnerabilities;

d) gain access to specialist information security advice;

e) share and exchange information about new technologies, products, threats, or vulnerabilities;

f) provide suitable liaison points when dealing with information security incidents (see also 13.2.1).

Other information

Information sharing agreements can be established to improve cooperation and coordination of security issues. Such agreements should identify requirements for the protection of sensitive information.

6.1.8 Independent review of information security

Control

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

Implementation guidance

The independent review should be initiated by management. Such an independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.

Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or a third party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience.

The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.

If the independent review identifies that the organization's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document (see 5.1.1), management should consider corrective actions.

Other information

The area, which managers should regularly review (see 15.2.1), may also be reviewed independently. Review techniques may include interviews of management, checking records or review of security policy documents. ISO 19011:2002, Guidelines for quality and/or environmental management systems auditing, may also provide helpful guidance for carrying out the independent review, including establishment and implementation of a review programme. Section 15.3 specifies controls relevant to the independent review of operational information systems and the use of system audit tools.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

6.2 External parties

Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

The security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services.

Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled.

Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product and service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

6.2.1 Identification of risks related to external parties

Control

The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

Implementation guidance

Where there is a need to allow an external party access to the information processing facilities or information of an organization, a risk assessment (see also Section 4) should be carried out to identify any requirements for specific controls. The identification of risks related to external party access should take into account the following issues:

a) the information processing facilities an external party is required to access;

b) the type of access the external party will have to the information and information processing facilities, e.g.:

   1) physical access, e.g. to offices, computer rooms, filing cabinets;

   2) logical access, e.g. to an organization's databases, information systems;

   3) network connectivity between the organization's and the external party's network(s), e.g. permanent connection, remote access;

   4) whether the access is taking place on-site or off-site;

c) the value and sensitivity of the information involved, and its criticality for business operations;

d) the controls necessary to protect information that is not intended to be accessible by external parties;

e) the external party personnel involved in handling the organization's information;

f) how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;

g) the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;

h) the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;

i) practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

j) legal and regulatory requirements and other contractual obligations relevant to the external party that should be taken into account;

k) how the interests of any other stakeholders may be affected by the arrangements.

Access by external parties to the organization's information should not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. Generally, all security requirements resulting from work with external parties or internal controls should be reflected by the agreement with the external party (see also 6.2.2 and 6.2.3).

It should be ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information processing facilities.

Other information

Information might be put at risk by external parties with inadequate security management. Controls should be identified and applied to administer external party access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements might be used.

Organizations may face risks associated with inter-organizational processes, management, and communication if a high degree of outsourcing is applied, or where there are several external parties involved.

The controls 6.2.2 and 6.2.3 cover different external party arrangements, e.g. including:

a) service providers, such as ISPs, network providers, telephone services, maintenance and support services;

b) managed security services;

c) customers;

d) outsourcing of facilities and/or operations, e.g. IT systems, data collection services, call centre operations;

e) management and business consultants, and auditors;

f) developers and suppliers, e.g. of software products and IT systems;

g) cleaning, catering, and other outsourced support services;

h) temporary personnel, student placement, and other casual short-term appointments.

Such agreements can help to reduce the risks associated with external parties.

6.2.2 Addressing security when dealing with customers

Control

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

Implementation guidance

The following terms should be considered to address security prior to giving customers access to any of the organization's assets (depending on the type and extent of access given, not all of them might apply):

a) asset protection, including:

1) procedures to protect the organization's assets, including information and software, and management of known vulnerabilities;

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

2) procedures to determine whether any compromise of the assets, e.g. loss or modification of data, has occurred;

3) integrity;

4) restrictions on copying and disclosing information;

b) description of the product or service to be provided;

c) the different reasons, requirements, and benefits for customer access;

d) access control policy, covering:

1) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;

2) an authorization process for user access and privileges;

3) a statement that all access that is not explicitly authorised is forbidden;

4) a process for revoking access rights or interrupting the connection between systems;

e) arrangements for reporting, notification, and investigation of information inaccuracies (e.g. of personal details), information security incidents and security breaches;

f) a description of each service to be made available;

g) the target level of service and unacceptable levels of service;

h) the right to monitor, and revoke, any activity related to the organization's assets;

i) the respective liabilities of the organization and the customer;

j) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with customers in other countries (see also 15.1);

k) intellectual property rights (IPRs) and copyright assignment (see 15.1.2) and protection of any collaborative work (see also 6.1.5).

Other information

The security requirements related to customers accessing organizational assets can vary considerably depending on the information processing facilities and information being accessed. These security requirements can be addressed using customer agreements, which contain all identified risks and security requirements (see 6.2.1).

Agreements with external parties may also involve other parties. Agreements granting external party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

6.2.3 Addressing security in third party agreements

Control

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

Implementation guidance

The agreement should ensure that there is no misunderstanding between the organization and the third party. Organizations should satisfy themselves as to the indemnity of the third party.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

The following terms should be considered for inclusion in the agreement in order to satisfy the identified security requirements (see 6.2.1):

a) the information security policy;

b) controls to ensure asset protection, including:

   1) procedures to protect organizational assets, including information, software and hardware;

   2) any required physical protection controls and mechanisms;

   3) controls to ensure protection against malicious software (see 10.4.1);

   4) procedures to determine whether any compromise of the assets, e.g. loss or modification of information, software and hardware, has occurred;

   5) controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement;

   6) confidentiality, integrity, availability, and any other relevant property (see 2.1.5) of the assets;

   7) restrictions on copying and disclosing information, and using confidentiality agreements (see 6.1.5);

c) user and administrator training in methods, procedures, and security;

d) ensuring user awareness for information security responsibilities and issues;

e) provision for the transfer of personnel, where appropriate;

f) responsibilities regarding hardware and software installation and maintenance;

g) a clear reporting structure and agreed reporting formats;

h) a clear and specified process of change management;

i) access control policy, covering:

   1) the different reasons, requirements, and benefits that make the access by the third party necessary;

   2) permitted access methods, and the control and use of unique identifiers such as user IDs and passwords;

   3) an authorization process for user access and privileges;

   4) a requirement to maintain a list of individuals authorized to use the services being made available, and what their rights and privileges are with respect to such use;

   5) a statement that all access that is not explicitly authorised is forbidden;

   6) a process for revoking access rights or interrupting the connection between systems;

j) arrangements for reporting, notification, and investigation of information security incidents and security breaches, as well as violations of the requirements stated in the agreement;

k) a description of the product or service to be provided, and a description of the information to be made available along with its security classification (see 7.2.1);

l) the target level of service and unacceptable levels of service;

m) the definition of verifiable performance criteria, their monitoring and reporting;

n) the right to monitor, and revoke, any activity related to the organization's assets;

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

o) the right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;

p) the establishment of an escalation process for problem resolution;

q) service continuity requirements, including measures for availability and reliability, in accordance with an organization's business priorities;

r) the respective liabilities of the parties to the agreement;

s) responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organizations in other countries (see also 15.1);

t) intellectual property rights (IPRs) and copyright assignment (see 15.1.2) and protection of any collaborative work (see also 6.1.5);

u) involvement of the third party with subcontractors, and the security controls these subcontractors need to implement;

v) conditions for renegotiation/termination of agreements:

   1) a contingency plan should be in place in case either party wishes to terminate the relation before the end of the agreements;

   2) renegotiation of agreements if the security requirements of the organization change;

   3) current documentation of asset lists, licences, agreements or rights relating to them.

Other information

The agreements can vary considerably for different organizations and among the different types of third parties. Therefore, care should be taken to include all identified risks and security requirements (see also 6.2.1) in the agreements. Where necessary, the required controls and procedures can be expanded in a security management plan.

If information security management is outsourced, the agreements should address how the third party will guarantee that adequate security, as defined by the risk assessment, will be maintained, and how security will be adapted to identify and deal with changes to risks.

Some of the differences between outsourcing and the other forms of third party service provision include the question of liability, planning the transition period and potential disruption of operations during this period, contingency planning arrangements and due diligence reviews, and collection and management of information on security incidents. Therefore, it is important that the organization plans and manages the transition to an outsourced arrangement and has suitable processes in place to manage changes and the renegotiation/termination of agreements.

The procedures for continuing processing in the event that the third party becomes unable to supply its services need to be considered in the agreement to avoid any delay in arranging replacement services.

Agreements with third parties may also involve other parties. Agreements granting third party access should include allowance for designation of other eligible parties and conditions for their access and involvement.

Generally agreements are primarily developed by the organization. There may be occasions in some circumstances where an agreement may be developed and imposed upon an organization by a third party. The organization needs to ensure that its own security is not unnecessarily impacted by third party requirements stipulated in imposed agreements.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

7 Asset management

7.1 Responsibility for assets

Objective: To achieve and maintain appropriate protection of organizational assets.

All assets should be accounted for and have a nominated owner.

Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

7.1.1 Inventory of assets

Control

All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

Implementation guidance

An organization should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value. The inventory should not duplicate other inventories unnecessarily, but it should be ensured that the content is aligned.

In addition, ownership (see 7.1.2) and information classification (see 7.2) should be agreed and documented for each of the assets. Based on the importance of the asset, its business value and its security classification, levels of protection commensurate with the importance of the assets should be identified (more information on how to value assets to represent their importance can be found in ISO/IEC TR 13335-3).

Other information

There are many types of assets, including:

a) information: databases and data files, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, fallback arrangements, audit trails, and archived information;

b) software assets: application software, system software, development tools, and utilities;

c) physical assets: computer equipment, communications equipment, removable media, and other equipment;

d) services: computing and communications services, general utilities, e.g. heating, lighting, power, and air-conditioning;

e) people, and their qualifications, skills, and experience;

f) intangibles, such as reputation and image of the organization.

Inventories of assets help to ensure that effective asset protection takes place, and may also be required for other business purposes, such as health and safety, insurance or financial (asset management) reasons. The process of compiling an inventory of assets is an important prerequisite of risk management (see also Section 4).

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

7.1.2 Ownership of assets

Control

All information and assets associated with information processing facilities should be owned[2] by a designated part of the organization.

Implementation guidance

The asset owner should be responsible for:

a) ensuring that information and assets associated with information processing facilities are appropriately classified;

b) defining and periodically reviewing access restrictions and classifications, taking into account applicable access control policies.

Ownership may be allocated to:

a) a business process;

b) a defined set of activities;

c) an application; or

d) a defined set of data.

Other information

Routine tasks may be delegated, e.g. to a custodian looking after the asset on a daily basis, but the responsibility remains with the owner.

In complex information systems it may be useful to designate groups of assets, which act together to provide a particular function as 'services'. In this case the service owner is responsible for the delivery of the service, including the functioning of the assets, which provide it.

7.1.3 Acceptable use of assets

Control

Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

Implementation guidance

All employees, contractors and third party users should follow rules for the acceptable use of information and assets associated with information processing facilities, including:

a) rules for electronic mail and Internet usages (see 10.8);

b) guidelines for the use of mobile devices, especially for the use outside the premises of the organization (see 11.7.1);

Specific rules or guidance should be provided by the relevant management. Employees, contractors and third party users using or having access to the organization's assets should be aware of the limits existing for their use of organization's information and assets associated with information processing facilities, and resources. They should be responsible for their use of any information processing resources, and of any such use carried out under their responsibility.

---

[2] The term 'owner' identifies an individual or entity that has approved management responsibility for controlling the production, development, maintenance, use and security of the assets. The term 'owner' does not mean that the person actually has any property rights to the asset.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

7.2 Information classification

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

Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.

Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

7.2.1 Classification guidelines

Control

Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

Implementation guidance

Classifications and associated protective controls for information should take account of business needs for sharing or restricting information and the business impacts associated with such needs.

Classification guidelines should include conventions for initial classification and reclassification over time; in accordance with some predetermined access control policy (see 11.1.1).

It should be the responsibility of the asset owner (see 7.1.2) to define the classification of an asset, periodically review it, and ensure it is kept up to date and at the appropriate level. The classification should take account of the aggregation effect mentioned in 10.7.2.

Consideration should be given to the number of classification categories and the benefits to be gained from their use. Overly complex schemes may become cumbersome and uneconomic to use or prove impractical. Care should be taken in interpreting classification labels on documents from other organizations, which may have different definitions for the same or similarly named labels.

Other Information

The level of protection can be assessed by analyzing confidentiality, integrity and availability and any other requirements for the information considered.

Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. These aspects should be taken into account, as over-classification can lead to the implementation of unnecessary controls resulting in additional expense.

Considering documents with similar security requirements together when assigning classification levels might help to simplify the classification task.

In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected.

7.2.2 Information labeling and handling

Control

An appropriate set of procedures for information labeling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.

Implementation guidance

Procedures for information labeling need to cover information assets in physical and electronic formats.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Output from systems containing information that is classified as being sensitive or critical should carry an appropriate classification label (in the output). The labeling should reflect the classification according to the rules established in 7.2.1. Items for consideration include printed reports, screen displays, recorded media (e.g. tapes, disks, CDs), electronic messages, and file transfers.

For each classification level, handling procedures including the secure processing, storage, transmission, declassification, and destruction should be defined. This should also include the procedures for chain of custody and logging of any security relevant event.

Agreements with other organizations that include information sharing should include procedures to identify the classification of that information and to interpret the classification labels from other organizations.

Other Information

Labeling and secure handling of classified information is a key requirement for information sharing arrangements. Physical labels are a common form of labeling. However, some information assets, such as documents in electronic form, cannot be physically labeled and electronic means of labeling need to be used. For example, notification labeling may appear on the screen or display. Where labeling is not feasible, other means of designating the classification of information may be applied, e.g. via procedures or meta-data.

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

8 Human resources security

8.1 Prior to employment[3]

Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.

Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.

Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

8.1.1 Roles and responsibilities

Control

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

Implementation guidance

Security roles and responsibilities should include the requirement to:

a) implement and act in accordance with the organization's information security policies (see 5.1);

b) protect assets from unauthorized access, disclosure, modification, destruction or interference;

c) execute particular security processes or activities;

d) ensure responsibility is assigned to the individual for actions taken;

e) report security events or potential events or other security risks to the organization.

Security roles and responsibilities should be defined and clearly communicated to job candidates during the pre-employment process.

Other Information

Job descriptions can be used to document security roles and responsibilities. Security roles and responsibilities for individuals not engaged via the organization's employment process, e.g. engaged via a third party organization, should also be clearly defined and communicated.

8.1.2 Screening

Control

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

[3] Explanation: The word 'employment' is meant here to cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005

Implementation guidance
Verification checks should take into account all relevant privacy, protection of personal data and/or employment based legislation, and should, where permitted, include the following:

a) availability of satisfactory character references, e.g. one business and one personal;

b) a check (for completeness and accuracy) of the applicant's curriculum vitae;

c) confirmation of claimed academic and professional qualifications;

d) independent identity check (passport or similar document);

e) more detailed checks, such as credit checks or checks of criminal records.

Where a job, either on initial appointment or on promotion, involves the person having access to information processing facilities, and in particular if these are handling sensitive information, e.g. financial information or highly confidential information, the organization should also consider further, more detailed checks.

Procedures should define criteria and limitations for verification checks, e.g. who is eligible to screen people, and how, when and why verification checks are carried out.

A screening process should also be carried out for contractors, and third party users. Where contractors are provided through an agency the contract with the agency should clearly specify the agency's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern. In the same way, the agreement with the third party (see also 6.2.3) should clearly specify all responsibilities and notification procedures for screening.

Information on all candidates being considered for positions within the organization should be collected and handled in accordance with any appropriate legislation existing in the relevant jurisdiction. Depending on applicable legislation, the candidates should be informed beforehand about the screening activities.

8.1.3 Terms and conditions of employment

Control
As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

Implementation guidance
The terms and conditions of employment should reflect the organization's security policy in addition to clarifying and stating:

a) that all employees, contractors and third party users who are given access to sensitive information should sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;

b) the employee's, contractor's and any other user's legal responsibilities and rights, e.g. regarding copyright laws or data protection legislation (see also 15.1.1 and 15.1.2);

c) responsibilities for the classification of information and management of organizational assets associated with information systems and services handled by the employee, contractor or third party user (see also 7.2.1 and 10.7.3);

d) responsibilities of the employee, contractor or third party user for the handling of information received from other companies or external parties;

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27002:2005

e) responsibilities of the organization for the handling of personal information, including personal information created as a result of, or in the course of, employment with the organization (see also 15.1.4);

f) responsibilities that are extended outside the organization's premises and outside normal working hours, e.g. in the case of home-working (see also 9.2.5 and 11.7.1);

g) actions to be taken if the employee, contractor or third party user disregards the organization's security requirements (see also 8.2.3).

The organization should ensure that employees, contractors and third party users agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organization's assets associated with information systems and services.

Where appropriate, responsibilities contained within the terms and conditions of employment should continue for a defined period after the end of the employment (see also 8.3).

Other Information
A code of conduct may be used to cover the employee's, contractor's or third party user's responsibilities regarding confidentiality, data protection, ethics, appropriate use of the organization's equipment and facilities, as well as reputable practices expected by the organization. The contractor or third party users may be associated with an external organization that may in turn be required to enter in contractual arrangements on behalf of the contracted individual.

8.2 During employment

Objective: To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization.

An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimize possible security risks. A formal disciplinary process for handling security breaches should be established.

8.2.1 Management responsibilities

Control
Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization.

Implementation guidance
Management responsibilities should include ensuring that employees, contractors and third party users:

a) are properly briefed on their information security roles and responsibilities prior to being granted access to sensitive information or information systems;

b) are provided with guidelines to state security expectations of their role within the organization;

c) are motivated to fulfil the security policies of the organization;

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27002:2005