FINAL
DRAFT

INTERNATIONAL STANDARD

ISO/IEC FDIS 17799

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2005-02-11

Voting terminates on:
2005-04-11

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

Please see the administrative notes on page iii

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 17799:2005(E)

© ISO/IEC 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

Copyright notice

This ISO document is a Draft International Standard and is copyright-protected by ISO. Except as permitted under the applicable laws of the user's country, neither this ISO draft nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission being secured.

Requests for permission to reproduce should be addressed to either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

 © ISO/IEC 2005 – All rights reserved

In accordance with the provisions of Council Resolution 21/1986, this document is **circulated in the English language only**.

© ISO/IEC 2005 – All rights reserved

Contents

Page

FOREWORD ..... **VIII**

0 INTRODUCTION ..... **IX**

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

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 ORGANIZING 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*

© ISO/IEC 2005 – All rights reserved

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*

© ISO/IEC 2005 – All rights reserved

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*

 © ISO/IEC 2005 – All rights reserved

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

© ISO/IEC 2005 – All rights reserved

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 17799 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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

 © ISO/IEC 2005 – All rights reserved

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) safeguarding 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) 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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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]

© ISO/IEC 2005 – All rights reserved

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 Guide 73:2002]

2.10

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

2.11

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

2.14

risk treatment
process of selection and implementation of measures to modify risk
[ISO 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 Guide 2:1996]

© ISO/IEC 2005 – All rights reserved

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 a threat
[ISO/IEC 13335-1:2004]

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

6 Organizing 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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

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, see also section 14), 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;

© ISO/IEC 2005 – All rights reserved

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 interval, 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 to 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 review programme. Section 15.3 specifies controls relevant to the independent review on operational information system and the use of system audit tools.

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

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 contains 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.

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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).

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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.

© ISO/IEC 2005 – All rights reserved

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, 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;

© ISO/IEC 2005 – All rights reserved

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;

© ISO/IEC 2005 – All rights reserved

d) achieve a level of awareness on security relevant to their roles and responsibilities within the organization (see also 8.2.2);

e) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working;

f) continue to have the appropriate skills and qualifications.

Other Information
If employees, contractors and third party users are not made aware of their security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause less information security incidents.

Poor management may cause personnel to feel undervalued resulting in a negative security impact to the organization. For example, poor management may lead to security being neglected or potential misuse of the organization's assets.

8.2.2 Information security awareness, education, and training

Control
All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

Implementation guidance
Awareness training should commence with a formal induction process designed to introduce the organization's security policies and expectations before access to information or services is granted.

Ongoing training should include security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities e.g. log-on procedure, use of software packages and information on the disciplinary process (see 8.2.3).

Other Information
The security awareness, education, and training activities should be suitable and relevant to the person's role, responsibilities and skills, and should include information on known threats, who to contact for further security advice and the proper channels for reporting information security incidents (see also 13.1).

Training to enhance awareness is intended to allow individuals to recognize information security problems and incidents, and respond according to the needs of their work role.

8.2.3 Disciplinary process

Control
There should be a formal disciplinary process for employees who have committed a security breach.

Implementation guidance
The disciplinary process should not be commenced without prior verification that a security breach has occurred (see also 13.2.3 for collection of evidence).

The formal disciplinary process should ensure correct and fair treatment for employees who are suspected of committing breaches of security. The formal disciplinary process should provide for a graduated response that takes into consideration factors such as the nature and gravity of the breach and its impact on business, whether or not this is a first or repeat offence, whether or not the violator was properly trained, relevant legislation, business contracts and other factors as required. In serious cases of misconduct the process should allow for instant removal of duties, access rights and privileges, and for immediate escorting out of the site, if necessary.

© ISO/IEC 2005 – All rights reserved

Other Information
The disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches.

8.3 Termination or change of employment

Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from the organization is managed, and that the return of all equipment and the removal of all access rights are completed.

Change of responsibilities and employments within an organization should be managed as the termination of the respective responsibility or employment in line with this section, and any new employments should be managed as described in section 8.1.

8.3.1 Termination responsibilities

Control
Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

Implementation guidance
The communication of termination responsibilities should include ongoing security requirements and legal responsibilities and, where appropriate, responsibilities contained within any confidentiality agreement (see 6.1.5), and the terms and conditions of employment (see 8.1.3) continuing for a defined period after the end of the employee's, contractor's or third party user's employment.

Responsibilities and duties still valid after termination of employment should be contained in employee's, contractor's or third party user's contracts.

Changes of responsibility or employment should be managed as the termination of the respective responsibility or employment, and the new responsibility or employment should be controlled as described in clause 8.1.

Other Information
The Human Resources function is generally responsible for the overall termination process and works together with the supervising manager of the person leaving to manage the security aspects of the relevant procedures. In the case of a contractor, this termination responsibility process may be undertaken by an agency responsible for the contractor, and in case of an other user this might be handled by their organization.

It may be necessary to inform employees, customers, contractors, or third party users of changes to personnel and operating arrangements.

8.3.2 Return of assets

Control
All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
The termination process should be formalized to include the return of all previously issued software, corporate documents, and equipment. Other organizational assets such as mobile computing devices, credit cards, access cards, software, manuals, and information stored on electronic media also need to be returned.

In cases where an employee, contractor or third party user purchases the organization's equipment or uses their own personal equipment, procedures should be followed to ensure that all relevant information is transferred to the organization and securely erased from the equipment (see also 10.7.1).

In cases where an employee, contractor or third party user has knowledge that is important to ongoing operations, that information should be documented and transferred to the organization.

8.3.3 Removal of access rights

Control
The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

Implementation guidance
Upon termination, the access rights of an individual to assets associated with information systems and services should be reconsidered. This will determine whether it is necessary to remove access rights. Changes of an employment should be reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adapted include physical and logical access, keys, identification cards, information processing facilities (see also 11.2.4), subscriptions, and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor or third party user has known passwords for accounts remaining active, these should be changed upon termination or change of employment, contract or agreement.

Access rights for information assets and information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

a) whether the termination or change is initiated by the employee, contractor or third party user, or by management and the reason of termination;

b) the current responsibilities of the employee, contractor or any other user;

c) the value of the assets currently accessible.

Other Information
In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee, contractor or third party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees, contractors and third party users involved to no longer share this information with the person departing.

In cases of management-initiated termination, disgruntled employees, contractors or third party users may deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning, they may be tempted to collect information for future use.

© ISO/IEC 2005 – All rights reserved

9 Physical and environmental security

9.1 Secure areas

Objective: To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

Critical or sensitive information processing facilities should be housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.

The protection provided should be commensurate with the identified risks.

9.1.1 Physical security perimeter

Control

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

Implementation guidance

The following guidelines should be considered and implemented where appropriate for physical security perimeters:

a) security perimeters should be clearly defined, and the siting and strength of each of the perimeters should depend on the security requirements of the assets within the perimeter and the results of a risk assessment;

b) perimeters of a building or site containing information processing facilities should be physically sound (i.e. there should be no gaps in the perimeter or areas where a break-in could easily occur); the external walls of the site should be of solid construction and all external doors should be suitably protected against unauthorized access with control mechanisms, e.g. bars, alarms, locks etc; doors and windows should be locked when unattended and external protection should be considered for windows, particularly at ground level;

c) a manned reception area or other means to control physical access to the site or building should be in place; access to sites and buildings should be restricted to authorized personnel only;

d) physical barriers should, where applicable, be built to prevent unauthorized physical access and environmental contamination;

e) all fire doors on a security perimeter should be alarmed, monitored, and tested in conjunction with the walls to establish the required level of resistance in accordance to suitable regional, national, and international standards; they should operate in accordance with local fire code in a failsafe manner;

f) suitable intruder detection systems should be installed to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be alarmed at all times; cover should also be provided for other areas, e.g. computer room or communications rooms;

g) information processing facilities managed by the organization should be physically separated from those managed by third parties.

© ISO/IEC 2005 – All rights reserved

Other information
Physical protection can be achieved by creating one or more physical barriers around the organization's premises and information processing facilities. The use of multiple barriers gives additional protection, where the failure of a single barrier does not mean that security is immediately compromised.

A secure area may be a lockable office, or several rooms surrounded by a continuous internal physical security barrier. Additional barriers and perimeters to control physical access may be needed between areas with different security requirements inside the security perimeter.

Special consideration towards physical access security should be given to buildings where multiple organizations are housed.

9.1.2 Physical entry controls

Control
Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

Implementation guidance
The following guidelines should be considered:

a) the date and time of entry and departure of visitors should be recorded, and all visitors should be supervised unless their access has been previously approved; they should only be granted access for specific, authorized purposes and should be issued with instructions on the security requirements of the area and on emergency procedures.

b) access to areas where sensitive information is processed or stored should be controlled and restricted to authorized persons only; authentication controls, e.g. access control card plus PIN, should be used to authorize and validate all access; an audit trail of all access should be securely maintained;

c) all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification;

d) third party support service personnel should be granted restricted access to secure areas or sensitive information processing facilities only when required; this access should be authorized and monitored;

e) access rights to secure areas should be regularly reviewed and updated, and revoked when necessary (see 8.3.3).

9.1.3 Securing offices, rooms, and facilities

Control
Physical security for offices, rooms, and facilities should be designed and applied.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
The following guidelines should be considered to secure offices, rooms, and facilities:

a) account should be taken of relevant health and safety regulations and standards;

b) key facilities should be sited to avoid access by the public;

c) where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities;

d) directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public.

9.1.4 Protecting against external and environmental threats

Control
Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Implementation guidance
Consideration should be given to any security threats presented by neighboring premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street.

The following guidelines should be considered to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:

a) hazardous or combustible materials should be stored at a safe distance from a secure area. Bulk supplies such as stationery should not be stored within a secure area;

b) fallback equipment and back-up media should be sited at a safe distance to avoid damage from a disaster affecting the main site;

c) appropriate fire fighting equipment should be provided and suitably placed.

9.1.5 Working in secure areas

Control
Physical protection and guidelines for working in secure areas should be designed and applied.

Implementation guidance
The following guidelines should be considered:

a) personnel should only be aware of the existence of, or activities within, a secure area on a need to know basis;

b) unsupervised working in secure areas should be avoided both for safety reasons and to prevent opportunities for malicious activities;

c) vacant secure areas should be physically locked and periodically checked;

d) photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed, unless authorized;

The arrangements for working in secure areas include controls for the employees, contractors and third party users working in the secure area, as well as other third party activities taking place there.

© ISO/IEC 2005 – All rights reserved

9.1.6 Public access, delivery, and loading areas

Control

Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

Implementation guidance

The following guidelines should be considered:

a) access to a delivery and loading area from outside of the building should be restricted to identified and authorized personnel;

b) the delivery and loading area should be designed so that supplies can be unloaded without delivery personnel gaining access to other parts of the building;

c) the external doors of a delivery and loading area should be secured when the internal doors are opened;

d) incoming material should be inspected for potential threats (see 9.2.1d)) before this material is moved from the delivery and loading area to the point of use;

e) incoming material should be registered in accordance with asset management procedures (see also 7.1.1) on entry to the site;

f) incoming and outgoing shipments should be physically segregated, where possible.

9.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

Equipment should be protected from physical and environmental threats.

Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against physical threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

9.2.1 Equipment siting and protection

Control

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

Implementation guidance

The following guidelines should be considered to protect equipment:

a) equipment should be sited to minimize unnecessary access into work areas;

b) information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access;

c) items requiring special protection should be isolated to reduce the general level of protection required;

d) controls should be adopted to minimize the risk of potential physical threats, e.g. theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, and vandalism;

© ISO/IEC 2005 – All rights reserved

e) guidelines for eating, drinking, and smoking in proximity to information processing facilities should be established;

f) environmental conditions, such as temperature and humidity, should be monitored for conditions, which could adversely affect the operation of information processing facilities;

g) lightning protection should be applied to all buildings and lightning protection filters should be fitted to all incoming power and communications lines;

h) the use of special protection methods, such as keyboard membranes, should be considered for equipment in industrial environments;

i) equipment processing sensitive information should be protected to minimize the risk of information leakage due to emanation.

9.2.2 Supporting utilities

Control

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

Implementation guidance

All supporting utilities, such as electricity, water supply, sewage, heating/ventilation, and air conditioning should be adequate for the systems they are supporting. Support utilities should be regularly inspected and as appropriate tested to ensure their proper functioning and to reduce any risk from their malfunction or failure. A suitable electrical supply should be provided that conforms to the equipment manufacturer's specifications.

An uninterruptible power supply (UPS) to support orderly close down or continuous running is recommended for equipment supporting critical business operations. Power contingency plans should cover the action to be taken on failure of the UPS. A back-up generator should be considered if processing is required to continue in case of a prolonged power failure. An adequate supply of fuel should be available to ensure that the generator can perform for a prolonged period. UPS equipment and generators should be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations. In addition, consideration could be given to using multiple power sources or, if the site is large a separate power substation.

Emergency power off switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided in case of main power failure.

The water supply should be stable and adequate to supply air conditioning, humidification equipment and fire suppression systems (where used). Malfunctions in the water supply system may damage equipment or prevent fire suppression from acting effectively. An alarm system to detect malfunctions in the supporting utilities should be evaluated and installed if required.

Telecommunications equipment should be connected to the utility provider by at least two diverse routes to prevent failure in one connection path removing voice services. Voice services should be adequate to meet local legal requirements for emergency communications.

Other information

Options to achieve continuity of power supplies include multiple feeds to avoid a single point of failure in the power supply.

© ISO/IEC 2005 – All rights reserved

9.2.3 Cabling security

Control

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

Implementation guidance

The following guidelines for cabling security should be considered:

a) power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;

b) network cabling should be protected from unauthorized interception or damage, for example by using a conduit or by avoiding routes through public areas;

c) power cables should be segregated from communications cables to prevent interference;

d) clearly identifiable cable and equipment markings should be used to minimise handling errors, such as accidentally patching of wrong network cables;

e) a documented patch list should be used to reduce the possibility of errors;

f) for sensitive or critical systems further controls to consider include:

   1) installation of armoured conduit and locked rooms or boxes at inspection and termination points;

   2) use of alternative routings and/or transmission media providing appropriate security;

   3) use of fibre optic cabling;

   4) use of electromagnetic shielding to protect the cables;

   5) initiation of technical sweeps and physical inspections for unauthorized devices being attached to the cables;

   6) controlled access to patch panels and cable rooms;

9.2.4 Equipment maintenance

Control

Equipment should be correctly maintained to ensure its continued availability and integrity.

Implementation guidance

The following guidelines for equipment maintenance should be considered:

a) equipment should be maintained in accordance with the supplier's recommended service intervals and specifications;

b) only authorized maintenance personnel should carry out repairs and service equipment;

c) records should be kept of all suspected or actual faults, and all preventive and corrective maintenance;

d) appropriate controls should be implemented when equipment is scheduled for maintenance, taking into account whether this maintenance is performed by personnel on site or external to the organization; where necessary, sensitive information should be cleared from the equipment, or the maintenance personnel should be sufficiently cleared;

e) all requirements imposed by insurance policies should be complied with.

© ISO/IEC 2005 – All rights reserved

9.2.5 Security of equipment off-premises

Control

Security should be applied to off-site equipment taking into account the different risks working outside the organization's premises.

Implementation guidance

Regardless of ownership, the use of any information processing equipment outside the organization's premises should be authorized by management.

The following guidelines should be considered for the protection of off-site equipment:

a) equipment and media taken off the premises should not be left unattended in public places; portable computers should be carried as hand luggage and disguised where possible when travelling;

b) manufacturers' instructions for protecting equipment should be observed at all times, e.g. protection against exposure to strong electromagnetic fields;

c) home-working controls should be determined by a risk assessment and suitable controls applied as appropriate, e.g. lockable filing cabinets, clear desk policy, access controls for computers and secure communication with the office (see also ISO/IEC 18028 Network Security);

d) adequate insurance cover should be in place to protect equipment off-site.

Security risks, e.g. of damage, theft or eavesdropping, may vary considerably between locations and should be taken into account in determining the most appropriate controls.

Other information

Information storing and processing equipment includes all forms of personal computers, organizers, mobile phones, smart cards, paper or other form, which is held for home working or being transported away from the normal work location.

More information about other aspects of protecting mobile equipment can be found in 11.7.1.

9.2.6 Secure disposal or re-use of equipment

Control

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Implementation guidance

Devices containing sensitive information should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

Other information

Damaged devices containing sensitive data may require a risk assessment to determine whether the items should be physically destroyed rather than sent for repair or discarded.

Information can be compromised through careless disposal or re-use of equipment (see also 10.7.2).

© ISO/IEC 2005 – All rights reserved

9.2.7 Removal of property

Control

Equipment, information or software should not be taken off-site without prior authorization.

Implementation guidance

The following guidelines should be considered:

a) equipment, information or software should not be taken off-site without prior authorization;

b) employees, contractors and third party users who have authority to permit off-site removal of assets should be clearly identified;

c) time limits for equipment removal should be set and returns checked for compliance;

d) where necessary and appropriate, equipment should be recorded as being removed off-site and recorded when returned.

Other information

Spot checks, undertaken to detect unauthorized removal of property, may also be performed to detect unauthorized recording devices, weapons, etc., and prevent their entry into the site. Such spot checks should be carried out in accordance with relevant legislation and regulations. Individuals should be made aware is spot checks are carried out, and the checks should only be performed with authorization appropriate for the legal and regulatory requirements.

© ISO/IEC 2005 – All rights reserved

10 Communications and operations management

10.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.
Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.
Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.1.1 Documented operating procedures

Control

Operating procedures should be documented, maintained, and made available to all users who need them.

Implementation guidance

Documented procedures should be prepared for system activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, media handling, computer room and mail handling management, and safety.

The operating procedures should specify the instructions for the detailed execution of each job including:

a) processing and handling of information;

b) backup (see 10.5);

c) scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times;

d) instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities (see 11.5.4);

e) support contacts in the event of unexpected operational or technical difficulties;

f) special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs (see 10.7.2 and 10.7.3);

g) system restart and recovery procedures for use in the event of system failure;

h) the management of audit-trail and system log information (see 10.10).

Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorized by management. Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities.

10.1.2 Change management

Control

Changes to information processing facilities and systems should be controlled.

Implementation guidance

Operational systems and application software should be subject to strict change management control**.**

© ISO/IEC 2005 – All rights reserved

In particular, the following items should be considered:

a) identification and recording of significant changes;

b) planning and testing of changes;

c) assessment of the potential impacts, including security impacts, of such changes;

d) formal approval procedure for proposed changes;

e) communication of change details to all relevant persons;

f) fallback procedures, including procedures and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events.

Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures. When changes are made, an audit log containing all relevant information should be retained.

Other information

Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to operational stage, can impact on the reliability of applications (see also 12.5.1).

Changes to operational systems should only be made when there is a valid business reason to do so, such as an increase in the risk to the system. Updating systems with the latest versions of operating system or application is not always in the business interest as this could introduce more vulnerabilities and instability than the current version. There may also be a need for additional training, license costs, support, maintenance and administration overhead, and new hardware especially during migration.

10.1.3 Segregation of duties

Control

Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

Implementation guidance

Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

Small organizations may find segregation of duties difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security audit remains independent.

10.1.4 Separation of development, test, and operational facilities

Control

Development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.

Implementation guidance

The level of separation between operational, test, and development environments that is necessary to prevent operational problems should be identified and appropriate controls implemented.

© ISO/IEC 2005 – All rights reserved

The following items should be considered:

a) rules for the transfer of software from development to operational status should be defined and documented;

b) development and operational software should run on different systems or computer processors and in different domains or directories;

c) compilers, editors, and other development tools or system utilities should not be accessible from operational systems when not required;

d) the test system environment should emulate the operational system environment as closely as possible;

e) users should use different user profiles for operational and test systems, and menus should display appropriate identification messages to reduce the risk of error;

f) sensitive data should not be copied into the test system environment (see 12.4.2).

Other information

Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or system failure. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

Where development and test personnel have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code, which can cause serious operational problems.

Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software or information if they share the same computing environment. Separating development, test, and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business data (see also 12.4.2 for the protection of test data).

10.2 Third party service delivery management

Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.

The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

10.2.1 Service delivery

Control

It should be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

Implementation guidance

Service delivery by a third party should include the agreed security arrangements, service definitions, and aspects of service management. In case of outsourcing arrangements, the organization should plan the necessary transitions (of information, information processing facilities, and anything else that needs to be moved), and should ensure that security is maintained throughout the transition period.

The organization should ensure that the third party maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see 14.1).

© ISO/IEC 2005 – All rights reserved

10.2.2 Monitoring and review of third party services

Control

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

Implementation guidance

Monitoring and review of third party services should ensure that the information security terms and conditions of the agreements are being adhered to, and that information security incidents and problems are managed properly. This should involve a service management relationship and process between the organization and the third party to:

a) monitor service performance levels to check adherence to the agreements;

b) review service reports produced by the third party and arrange regular progress meetings as required by the agreements;

c) provide information about information security incidents and review of this information by the third party and the organization as required by the agreements and any supporting guidelines and procedures;

d) review third party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;

e) resolve and manage any identified problems.

The responsibility for managing the relationship with a third party should be assigned to a designated individual or service management team. In addition, the organization should ensure that the third party assigns responsibilities for checking for compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that requirements of the agreement (see 6.2.3), in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

The organization should maintain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a third party. The organization should ensure they retain visibility into security activities such as change management, identification of vulnerabilities, and information security incident reporting/response through a clearly defined reporting process, format and structure.

Other information

In case of outsourcing, the organization needs to be aware that the ultimate responsibility for information processed by an outsourcing party remains with the organization.

10.2.3 Managing changes to third party services

Control

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

Implementation guidance

The process of managing changes to a third party service needs to take account of:

a) changes made by the organization to implement:

   1) enhancements to the current services offered;

   2) development of any new applications and systems;

© ISO/IEC 2005 – All rights reserved

3) modifications or updates of the organization's policies and procedures;
4) new controls to resolve information security incidents and to improve security;

b) changes in third party services to implement:
1) changes and enhancement to networks;
2) use of new technologies;
3) adoption of new products or newer versions/releases;
4) new development tools and environments;
5) changes to physical location of service facilities;
6) change of vendors.

10.3 System planning and acceptance

Objective: To minimize the risk of systems failures.
Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.
Projections of future capacity requirements should be made, to reduce the risk of system overload.
The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

10.3.1 Capacity management

Control
The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

Implementation guidance
For each new and ongoing activity, capacity requirements should be identified. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Detective controls should be put in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilization of key system resources. They should identify trends in usage, particularly in relation to business applications or management information system tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

10.3.2 System acceptance

Control
Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.

Implementation guidance
Managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented, and tested. New information systems, upgrades, and new versions

© ISO/IEC 2005 – All rights reserved

should only be migrated into production after obtaining formal acceptance. The following items should be considered prior to formal acceptance being provided:

a) performance and computer capacity requirements;

b) error recovery and restart procedures, and contingency plans;

c) preparation and testing of routine operating procedures to defined standards;

d) agreed set of security controls in place;

e) effective manual procedures;

f) business continuity arrangements (see 14.1);

g) evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end;

h) evidence that consideration has been given to the effect the new system has on the overall security of the organization;

i) training in the operation or use of new systems;

j) ease of use, as this affects user performance and avoids human error.

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

Other information

Acceptance may include a formal certification and accreditation process to verify that the security requirements have been properly addressed.

10.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

10.4.1 Controls against malicious code

Control

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

Implementation guidance

Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls. The following guidance should be considered:

a) establishing a formal policy prohibiting the use of unauthorized software (see 15.1.2);

b) establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, indicating what protective measures should be taken (see also 11.5, especially 11.5.4 and 11.5.5);

© ISO/IEC 2005 – All rights reserved

c) conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;

d) installation and regular update of malicious code detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the checks carried out should include:

   1) checking any files on electronic or optical media, and files received over networks, for malicious code before use;

   2) checking electronic mail attachments and downloads for malicious code before use; this check should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;

   3) checking web pages for malicious code;

e) defining management procedures and responsibilities to deal with malicious code protection on systems, training in their use, reporting and recovering from malicious code attacks (see 13.1 and 13.2);

f) preparing appropriate business continuity plans for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements (see clause 14);

g) implementing procedures to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code;

h) implementing procedures to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, are used to differentiate between hoaxes and real malicious code; all users should be made aware of the problem of hoaxes and what to do on receipt of them.

Other information

The use of two or more software products protecting against malicious code across the information processing environment from different vendors can improve the effectiveness of malicious code protection.

Software to protect against malicious code can be installed to provide automatic updates of definition files and scanning engines to ensure the protection is up to date. In addition, this software can be installed on every desktop to carry out automatic checks.

Care should be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

10.4.2 Controls against mobile code

Control

Where the use of mobile code is authorized, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

Implementation guidance

The following actions should be considered to protect against mobile code performing unauthorized actions:

a) executing mobile code in a logically isolated environment;

b) blocking any use of mobile code;

© ISO/IEC 2005 – All rights reserved

c) blocking receipt of mobile code;

d) activating technical measures as available on a specific system to ensure mobile code is managed;

e) control the resources available to mobile code access;

f) cryptographic controls to uniquely authenticate mobile code.

Other information
Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is associated with a number of middleware services.

In addition to ensuring that mobile code does not contain malicious code, control of mobile code is essential to avoid unauthorised use or disruption of system, network, or application resources and other breaches of information security.

10.5 Back-up

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

Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration.

10.5.1 Information back-up

Control
Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

Implementation guidance
Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

The following items for information back up should be considered:

a) the necessary level of back-up information should be defined;

b) accurate and complete records of the back-up copies and documented restoration procedures should be produced;

c) the extent (e.g. full or differential backup) and frequency of backups should reflect the business requirements of the organization, the security requirements of the information involved, and the criticality of the information to the continued operation of the organization;

d) the back-ups should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site;

e) back-up information should be given an appropriate level of physical and environmental protection (see clause 9) consistent with the standards applied at the main site; the controls applied to media at the main site should be extended to cover the back-up site;

f) back-up media should be regularly tested to ensure that they can be relied upon for emergency use when necessary;

© ISO/IEC 2005 – All rights reserved

g) restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery;

h) in situations where confidentiality is of importance, back-ups should be protected by means of encryption.

Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans (see clause 14). For critical systems, the backup arrangements should cover all systems information, applications, and data necessary to recover the complete system in the event of a disaster.

The retention period for essential business information, and also any requirement for archive copies to be permanently retained should be determined (see 15.1.3).

Other information

Back up arrangements can be automated to ease the back-up and restore process. Such automated solutions should be sufficiently tested prior to implementation and at regular intervals.

10.6 Network security management

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

The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.

Additional controls may also be required to protect sensitive information passing over public networks.

10.6.1 Network controls

Control

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Implementation guidance

Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) operational responsibility for networks should be separated from computer operations where appropriate (see 10.1.3);

b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;

c) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications (see 11.4 and 12.3); special controls may also be required to maintain the availability of the network services and computers connected;

d) appropriate logging and monitoring should be applied to enable recording of security relevant actions;

e) management activities should be closely co-ordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.

© ISO/IEC 2005 – All rights reserved

Other information

Additional information on network security can be found in ISO/IEC 18028, *Information technology – Security techniques – IT network security*.

10.6.2 Security of network services

Control

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

Implementation guidance

The ability of the network service provider to manage agreed services in a secure way should be determined and regularly monitored, and the right to audit should be agreed.

The security arrangements necessary for particular services, such as security features, service levels, and management requirements, should be identified. The organization should ensure that network service providers implement these measures.

Other information

Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and intrusion detection systems. These services can range from simple unmanaged bandwidth to complex value-added offerings.

Security features of network services could be:

a) technology applied for security of network services, such as authentication, encryption, and network connection controls;

b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules;

c) procedures for the network service usage to restrict access to network services or applications, where necessary.

10.7 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

Media should be controlled and physically protected.

Appropriate operating procedures should be established to protect documents, computer media (e.g. tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

10.7.1 Management of removable media

Control

There should be procedures in place for the management of removable media.

Implementation guidance

The following guidelines for the management of removable media should be considered:

a) if no longer required, the contents of any re-usable media that are to be removed from the organization should be made unrecoverable;

© ISO/IEC 2005 – All rights reserved

b) where necessary and practical, authorization should be required for media removed from the organization and a record of such removals should be kept in order to maintain an audit trail;

c) all media should be stored in a safe, secure environment, in accordance with manufacturers' specifications;

d) information stored on media that needs to be available longer than the media lifetime (in accordance with manufacturers' specifications) should be also stored elsewhere to avoid information loss due to media degradation;

e) registration of removable media should be considered to limit the opportunity for data loss;

f) removable media drives should only be enabled if there is a business reason for doing so.

All procedures and authorization levels should be clearly documented.

Other information
Removable media include tapes, disks, flash disks, removable hard drives, CDs, DVDs, and printed media.

10.7.2 Disposal of media

Control
Media should be disposed of securely and safely when no longer required, using formal procedures.

Implementation guidance
Formal procedures for the secure disposal of media should minimize the risk of sensitive information leakage to unauthorised persons. The procedures for secure disposal of media containing sensitive information should be commensurate with the sensitivity of that information. The following items should be considered:

a) media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding, or erased of data for use by another application within the organization;

b) procedures should be in place to identify the items that might require secure disposal;

c) it may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items;

d) many organizations offer collection and disposal services for papers, equipment and media; care should be taken in selecting a suitable contractor with adequate controls and experience;

e) disposal of sensitive items should be logged where possible in order to maintain an audit trail.

When accumulating media for disposal, consideration should be given to the aggregation effect, which may cause a large quantity of non-sensitive information to become sensitive.

Other information
Sensitive information could be disclosed through careless disposal of media (see also 9.2.6 for information about disposal of equipment).

10.7.3 Information handling procedures

Control
Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
Procedures should be drawn up for handling; processing, storing, and communicating information consistent with its classification (see 7.2). The following items should be considered:

a) handling and labelling of all media to its indicated classification level;

b) access restrictions to prevent access from unauthorized personnel;

c) maintenance of a formal record of the authorized recipients of data;

d) ensuring that input data is complete, that processing is properly completed and that output validation is applied;

e) protection of spooled data awaiting output to a level consistent with its sensitivity;

f) storage of media in accordance with manufacturers' specifications;

g) keeping the distribution of data to a minimum;

h) clear marking of all copies of media for the attention of the authorized recipient;

i) review of distribution lists and lists of authorized recipients at regular intervals.

Other information
These procedures apply to information in documents, computing systems, networks, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities, use of facsimile machines and any other sensitive items, e.g. blank cheques, invoices.

10.7.4 Security of system documentation

Control
System documentation should be protected against unauthorized access.

Implementation guidance
To secure system documentation, the following items should be considered:

a) system documentation should be stored securely;

b) the access list for system documentation should be kept to a minimum and authorized by the application owner;

c) system documentation held on a public network, or supplied via a public network, should be appropriately protected.

Other information
System documentation may contain a range of sensitive information, e.g. descriptions of applications processes, procedures, data structures, authorization processes.

10.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation (see clause 15).

Procedures and standards should be established to protect information and physical media containing information in transit.

© ISO/IEC 2005 – All rights reserved

10.8.1 Information exchange policies and procedures

Control

Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

Implementation guidance

The procedures and controls to be followed when using electronic communication facilities for information exchange should consider the following items:

a) procedures designed to protect exchanged information from interception, copying, modification, mis-routing, and destruction;

b) procedures for the detection of and protection against malicious code that may be transmitted through the use of electronic communications (see Clause 10.4.1);

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

d) policy or guidelines outlining acceptable use of electronic communication facilities (see 7.1.3);

e) procedures for the use of wireless communications, taking into account the particular risks involved;

f) employee, contractor and any other user's responsibilities not to compromise the organization, e.g. through defamation, harassment, impersonation, forwarding of chain letters, unauthorized purchasing, etc.;

g) use of cryptographic techniques e.g. to protect the confidentiality, integrity and authenticity of information (see Clause 12.3);

h) retention and disposal guidelines for all business correspondence, including messages, in accordance with relevant national and local legislation and regulations;

i) not leaving sensitive or critical information on printing facilities, e.g. copiers, printers, and facsimile machines, as these may be accessed by unauthorized personnel;

j) controls and restrictions associated with the forwarding of communication facilities, e.g. automatic forwarding of electronic mail to external mail addresses;

k) reminding personnel that they should take appropriate precautions, e.g. not to reveal sensitive information to avoid being overheard or intercepted when making a phone call by:

   1) people in their immediate vicinity particularly when using mobile phones;

   2) wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers;

   3) people at the recipient's end;

l) not leaving messages containing sensitive information on answering machines since these may be replayed by unauthorized persons, stored on communal systems or stored incorrectly as a result of misdialling;

m) reminding personnel about the problems of using facsimile machines, namely:

   1) unauthorized access to built-in message stores to retrieve messages;

   2) deliberate or accidental programming of machines to send messages to specific numbers;

   3) sending documents and messages to the wrong number either by misdialling or using the wrong stored number;

© ISO/IEC 2005 – All rights reserved

n) reminding personnel not to register demographic data, such as the e-mail address or other personal information, in any software to avoid collection for unauthorized use;

o) reminding personnel that modern facsimile machines and photocopiers have page caches and store pages in case of a paper or transmission fault, which will be printed once the fault is cleared.

In addition, personnel should be reminded that they should not have confidential conversations in public places or open offices and meeting places with non-sound proofed-walls.

Information exchange facilities should comply with any relevant legal requirements (see clause 15).

Other Information

Information exchange may occur through the use of a number of different types of communication facilities, including electronic mail, voice, facsimile, and video.

Software exchange may occur through a number of different mediums, including downloading from the Internet and acquired from vendors selling off-the-shelf products.

The business, legal, and security implications associated with electronic data interchange, electronic commerce, and electronic communications and the requirements for controls should be considered.

Information could be compromised due to lack of awareness, policy or procedures on the use of information exchange facilities, e.g. being overheard on a mobile phone in a public place, misdirection of an electronic mail message, answering machines being overheard, unauthorised access to dial-in voice-mail systems or accidentally sending facsimiles to the wrong facsimile equipment.

Business operations could be disrupted and information could be compromised if communications facilities fail, are overloaded or interrupted (see 10.3 and clause 14). Information could be compromised if accessed by unauthorized users (see clause 11).

10.8.2 Exchange agreements

Control

Agreements should be established for the exchange of information and software between the organization and external parties.

Implementation guidance

Exchange agreements should consider the following security conditions:

a) management responsibilities for controlling and notifying transmission, dispatch, and receipt;

b) procedures for notifying sender of transmission, dispatch, and receipt;

c) procedures to ensure traceability and non-repudiation;

d) minimum technical standards for packaging and transmission;

e) escrow agreements;

f) courier identification standards;

g) responsibilities and liabilities in the event of information security incidents, such as loss of data;

h) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;

© ISO/IEC 2005 – All rights reserved

i) ownership and responsibilities for data protection, copyright, software license compliance and similar considerations (see 15.1.2 and 15.1.4);

j) technical standards for recording and reading information and software;

k) any special controls that may be required to protect sensitive items, such as cryptographic keys (see 12.3).

Policies, procedures, and standards should be established and maintained to protect information and physical media in transit (see also 10.8.3), and should be referenced in such exchange agreements.

The security content of any agreement should reflect the sensitivity of the business information involved.

Other Information

Agreements may be electronic or manual, and may take the form of formal contracts or conditions of employment. For sensitive information, the specific mechanisms used for the exchange of such information should be consistent for all organizations and types of agreements.

10.8.3 Physical media in transit

Control

Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

Implementation guidance

The following guidelines should be considered to protect information media being transported between sites:

a) reliable transport or couriers should be used;

b) a list of authorized couriers should be agreed with management;

c) procedures to check the identification of couriers should be developed;

d) packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications (e.g. for software), for example protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields;

e) controls should be adopted, where necessary, to protect sensitive information from unauthorized disclosure or modification; examples include:

   1) use of locked containers;

   2) delivery by hand;

   3) tamper-evident packaging (which reveals any attempt to gain access);

   4) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

Other Information

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier.

© ISO/IEC 2005 – All rights reserved

10.8.4 Electronic messaging

Control
Information involved in electronic messaging should be appropriately protected.

Implementation guidance
Security considerations for electronic messaging should include the following:

a) protecting messages from unauthorized access, modification or denial of service;

b) ensuring correct addressing and transportation of the message;

c) general reliability and availability of the service;

d) legal considerations, for example requirements for electronic signatures;

e) obtaining approval prior to using external public services such as instant messaging or file sharing;

f) stronger levels of authentication controlling access from publicly accessible networks.

Other Information
Electronic messaging such as email, Electronic Data Interchange (EDI), and instant messaging play an increasingly important role in business communications. Electronic messaging has different risks than paper based communications.

10.8.5 Business information systems

Control
Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.

Implementation guidance
Consideration given to the security and business implications of interconnecting such facilities should include:

a) known vulnerabilities in the administrative and accounting systems where information is shared between different parts of the organization;

b) vulnerabilities of information in business communication systems, e.g. recording phone calls or conference calls, confidentiality of calls, storage of facsimiles, opening mail, distribution of mail;

c) policy and appropriate controls to manage information sharing;

d) excluding categories of sensitive business information and classified documents if the system does not provide an appropriate level of protection (see 7.2);

e) restricting access to diary information relating to selected individuals, e.g. personnel working on sensitive projects;

f) categories of personnel, contractors or business partners allowed to use the system and the locations from which it may be accessed (see 6.2 and 6.3);

g) restricting selected facilities to specific categories of user;

h) identifying the status of users, e.g. employees of the organization or contractors in directories for the benefit of other users;

i) retention and back-up of information held on the system (see 10.5.1);

j) fallback requirements and arrangements (see 14).

© ISO/IEC 2005 – All rights reserved

Other Information
Office information systems are opportunities for faster dissemination and sharing of business information using a combination of: documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services/facilities and facsimile machines.

10.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should also be considered.

10.9.1 Electronic commerce

Control
Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

Implementation guidance
Security considerations for electronic commerce should include the following:

a) the level of confidence each party requires in each others claimed identity, e.g. through authentication;

b) authorization processes associated with who may set prices, issue or sign key trading documents;

c) ensuring that trading partners are fully informed of their authorisations;

d) determining and meeting requirements for confidentiality, integrity, proof of dispatch and receipt of key documents, and the non-repudiation of contracts, e.g. associated with tendering and contract processes;

e) the level of trust required in the integrity of advertised price lists;

f) the confidentiality of any sensitive data or information;

g) the confidentiality and integrity of any order transactions, payment information, delivery address details, and confirmation of receipts;

h) the degree of verification appropriate to check payment information supplied by a customer;

i) selecting the most appropriate settlement form of payment to guard against fraud;

j) the level of protection required to maintain the confidentiality and integrity of order information;

k) avoidance of loss or duplication of transaction information;

l) liability associated with any fraudulent transactions;

m) insurance requirements.

Many of the above considerations can be addressed by the application of cryptographic controls (see 12.3), taking into account compliance with legal requirements (see 15.1, especially 15.1.6 for cryptography legislation).

Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization (see b) above). Other agreements with information service and value added network providers may be necessary.

© ISO/IEC 2005 – All rights reserved

Public trading systems should publicize their terms of business to customers.

Consideration should be given to the resilience to attack of the host(s) used for electronic commerce, and the security implications of any network interconnection required for the implementation of electronic commerce services (see 11.4.6).

Other Information
Electronic commerce is vulnerable to a number of network threats that may result in fraudulent activity, contract dispute, and disclosure or modification of information.

Electronic commerce can make use of secure authentication methods, e.g. using public key cryptography and digital signatures (see also 12.3) to reduce the risks. Also, trusted third parties can be used, where such services are needed.

10.9.2 On-Line Transactions

Control
Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

Implementation guidance
Security considerations for on-line transactions should include the following:

a) the use of electronic signatures by each of the parties involved in the transaction;

b) all aspects of the transaction, i.e. ensuring that:

   1) user credentials of all parties are valid and verified;

   2) the transaction remains confidential; and

   3) privacy associated with all parties involved is retained;

c) communications path between all involved parties is encrypted;

d) protocols used to communicate between all involved parties is secured;

e) ensuring that the storage of the transaction details are located outside of any public accessible environment, e.g. on a storage platform existing on the organizational Intranet, and not retained and exposed on a storage medium directly accessible from the Internet;

f) where a trusted authority is used (e.g. for the purposes of issuing and maintaining digital signatures and/or digital certificates) security is integrated and embedded throughout the entire end-to-end certificate/signature management process.

Other Information
The extent of the controls adopted will need to be commensurate with the level of the risk associated with each form of on-line transaction.

Transactions may need to comply with laws, rules, and regulations in the jurisdiction in which the transaction is generated from, processed via, completed at, and/or stored.

There exist many forms of transactions that can be performed in an on-line manner e.g. contractual, financial etc.

© ISO/IEC 2005 – All rights reserved

10.9.3 Publicly available information

Control

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

Implementation guidance

Software, data, and other information requiring a high level of integrity, being made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures (see 12.3). The publicly accessible system should be tested against weaknesses and failures prior to information being made available.

There should be a formal approval process before information is made publicly available. In addition, all input provided from the outside to the system should be verified and approved.

Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:

a) information is obtained in compliance with any data protection legislation (see 15.1.4);

b) information input to, and processed by, the publishing system will be processed completely and accurately in a timely manner;

c) sensitive information will be protected during collection, processing, and storage;

d) access to the publishing system does not allow unintended access to networks to which the system is connected.

Other Information

Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules, and regulations in the jurisdiction in which the system is located, where trade is taking place or where the owner(s) reside. Unauthorized modification of published information may harm the reputation of the publishing organization.

10.10 Monitoring

Objective: To detect unauthorized information processing activities.
Systems should be monitored and information security events should be recorded. Operator logs and fault logging should be used to ensure information system problems are identified.
An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities.
System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

10.10.1 Audit logging

Control

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Implementation guidance

Audit logs should include, when relevant:

a) user IDs;

b) dates, times, and details of key events, e.g. log-on and log-off;

© ISO/IEC 2005 – All rights reserved

c) terminal identity or location if possible;

d) records of successful and rejected system access attempts;

e) records of successful and rejected data and other resource access attempts;

f) changes to system configuration;

g) use of privileges;

h) use of system utilities and applications;

i) files accessed and the kind of access;

j) network addresses and protocols;

k) alarms raised by the access control system;

l) activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

Other information

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (see also 15.1.4). Where possible, system administrators should not have permission to erase or de-activate logs of their own activities (see 10.1.3).

10.10.2 Monitoring system use

Control

Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

Implementation guidance

The level of monitoring required for individual facilities should be determined by a risk assessment. An organisation should comply with all relevant legal requirements applicable to its monitoring activities. Areas that should be considered include:

a) authorized access, including detail such as:
   1) the user ID;
   2) the date and time of key events;
   3) the types of events;
   4) the files accessed;
   5) the program/utilities used;

b) all privileged operations, such as:
   1) use of privileged accounts, e.g. supervisor, root, administrator;
   2) system start-up and stop;
   3) I/O device attachment/detachment;

c) unauthorized access attempts, such as:
   1) failed or rejected user actions;
   2) failed or rejected actions involving data and other resources;
   3) access policy violations and notifications for network gateways and firewalls;
   4) alerts from proprietary intrusion detection systems;

© ISO/IEC 2005 – All rights reserved

d) system alerts or failures such as:
   1) console alerts or messages;
   2) system log exceptions;
   3) network management alarms;
   4) alarms raised by the access control system;
e) changes to, or attempts to change, system security settings and controls.

How often the results of monitoring activities are reviewed should depend on the risks involved. Risk factors that should be considered include the:

a) criticality of the application processes;
b) value, sensitivity, and criticality of the information involved;
c) past experience of system infiltration and misuse, and the frequency of vulnerabilities being exploited;
d) extent of system interconnection (particularly public networks);
e) logging facility being de-activated.

Other information
Usage monitoring procedures are necessary to ensure that users are only performing activities that have been explicitly authorized.

A log review involves understanding the threats faced by the system and the manner in which these may arise. Examples of events that might require further investigation in case of information security incidents are given in 13.1.1.

10.10.3 Protection of log information

Control
Logging facilities and log information should be protected against tampering and unauthorized access.

Implementation guidance
Controls should aim to protect against unauthorized changes and operational problems with the logging facility including:

a) alterations to the message types that are recorded;
b) log files being edited or deleted;
c) storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence (see also 13.2.3).

Other information
System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalization should be considered.

System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

© ISO/IEC 2005 – All rights reserved

10.10.4 Administrator and operator logs

Control
System administrator and system operator activities should be logged.

Implementation guidance
Logs should include:

a) the time at which an event (success or failure) occurred;

b) information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken);

c) which account and which administrator or operator was involved;

d) which processes were involved.

System administrator and operator logs should be reviewed on a regular basis.

Other information
An intrusion detection system managed outside of the control of system and network administrators can be used to monitor system and network administration activities for compliance.

10.10.5 Fault logging

Control
Faults should be logged, analysed, and appropriate action taken.

Implementation guidance
Faults reported by users or by system programs related to problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

a) review of fault logs to ensure that faults have been satisfactorily resolved;

b) review of corrective measures to ensure that controls have not been compromised, and that the action taken is fully authorized.

It should be ensured that error logging is enabled, if this system function is available.

Other information
Logging of errors and faults can impact the performance of a system. Such logging should be enabled by competent personnel, and the level of logging required for individual systems should be determined by a risk assessment, taking performance degradation into account.

10.10.6 Clock synchronization

Control
The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

Implementation guidance
Where a computer or communications device has the capability to operate a real-time clock, this clock should be set to an agreed standard, e.g. Coordinated Universal Time (UTC) or local standard time. As some clocks are known to drift with time, there should be a procedure that checks for and corrects any significant variation.

The correct interpretation of the date/time format is important to ensure that the timestamp reflects the real date/time. Local specifics (e.g. daylight savings) should be taken into account.

© ISO/IEC 2005 – All rights reserved

Other information

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence. A clock linked to a radio time broadcast from a national atomic clock can be used as the master clock for logging systems. A network time protocol can be used to keep all of the servers in synchronisation with the master clock.

© ISO/IEC 2005 – All rights reserved

11 Access control

11.1 Business requirement for access control

Objective: To control access to information.

Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements.

Access control rules should take account of policies for information dissemination and authorization.

11.1.1 Access control policy

Control

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

Implementation guidance

Access control rules and rights for each user or group of users should be clearly stated in an access control policy. Access controls are both logical and physical (see also section 9) and these should be considered together. Users and service providers should be given a clear statement of the business requirements to be met by access controls.

The policy should take account of the following:

a) security requirements of individual business applications;

b) identification of all information related to the business applications and the risks the information is facing;

c) policies for information dissemination and authorization, e.g. the need to know principle and security levels and classification of information (see 7.2);

d) consistency between the access control and information classification policies of different systems and networks;

e) relevant legislation and any contractual obligations regarding protection of access to data or services (see 15.1);

f) standard user access profiles for common job roles in the organization;

g) management of access rights in a distributed and networked environment which recognizes all types of connections available;

h) segregation of access control roles, e.g. access request, access authorization, access administration;

i) requirements for formal authorization of access requests (see 11.2.1);

j) requirements for periodic review of access controls (see 11.2.4);

k) removal of access rights (see 8.3.3).

Other information

Care should be taken when specifying access control rules to consider:

a) differentiating between rules that must always be enforced and guidelines that are optional or conditional;

© ISO/IEC 2005 – All rights reserved

b) establishing rules based on the premise "Everything is generally forbidden unless expressly permitted" rather than the weaker rule "Everything is generally permitted unless expressly forbidden";

c) changes in information labels (see 7.2) that are initiated automatically by information processing facilities and those initiated at the discretion of a user;

d) changes in user permissions that are initiated automatically by the information system and those initiated by an administrator;

e) rules, which require specific approval before enactment and those, which do not.

Access control rules should be supported by formal procedures and clearly defined responsibilities (see, for example, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

Formal procedures should be in place to control the allocation of access rights to information systems and services.

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

11.2.1 User registration

Control

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

Implementation guidance

The access control procedure for user registration and de-registration should include:

a) using unique user IDs to enable users to be linked to and held responsible for their actions; the use of group IDs should only be permitted where they are necessary for business or operational reasons, and should be approved and documented;

b) checking that the user has authorization from the system owner for the use of the information system or service; separate approval for access rights from management may also be appropriate;

c) checking that the level of access granted is appropriate to the business purpose (see 11.1) and is consistent with organizational security policy, e.g. it does not compromise segregation of duties (see 10.1.3);

d) giving users a written statement of their access rights;

e) requiring users to sign statements indicating that they understand the conditions of access;

f) ensuring service providers do not provide access until authorization procedures have been completed;

g) maintaining a formal record of all persons registered to use the service;

h) immediately removing or blocking access rights of users who have changed roles or jobs or left the organization;

i) periodically checking for, and removing or blocking, redundant user IDs and accounts (see 11.2.4);

j) ensuring that redundant user IDs are not issued to other users.

© ISO/IEC 2005 – All rights reserved

Other information
Consideration should be given to establish user access roles based on business requirements that summarize a number of access rights into typical user access profiles. Access requests and reviews (see 11.2.4) are easier managed at the level of such roles than at the level of particular rights.

Consideration should be given to including clauses in personnel contracts and service contracts that specify sanctions if unauthorized access is attempted by personnel or service agents (see also 6.1.5, 8.1.3 and 8.2.3).

11.2.2 Privilege management

Control
The allocation and use of privileges should be restricted and controlled.

Implementation guidance
Multi-user systems that require protection against unauthorized access should have the allocation of privileges controlled through a formal authorization process. The following steps should be considered:

a) the access privileges associated with each system product, e.g. operating system, database management system and each application, and the users to which they need to be allocated should be identified;

b) privileges should be allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (11.1.1), i.e. the minimum requirement for their functional role only when needed;

c) an authorization process and a record of all privileges allocated should be maintained. Privileges should not be granted until the authorization process is complete;

d) the development and use of system routines should be promoted to avoid the need to grant privileges to users;

e) the development and use of programs, which avoid the need to run with privileges should be promoted;

f) privileges should be assigned to a different user ID from those used for normal business use.

Other information
Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) can be a major contributory factor to the failures or breaches of systems.

11.2.3 User password management

Control
The allocation of passwords should be controlled through a formal management process.

Implementation guidance
The process should include the following requirements:

a) users should be required to sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group; this signed statement could be included in the terms and conditions of employment (see 8.1.3);

© ISO/IEC 2005 – All rights reserved

b) when users are required to maintain their own passwords they should be provided initially with a secure temporary password (see 11.3.1), which they are forced to change immediately;

c) establish procedures to verify the identity of a user prior to providing a new, replacement or temporary password;

d) temporary passwords should be given to users in a secure manner; the use of third parties or unprotected (clear text) electronic mail messages should be avoided;

e) temporary passwords should be unique to an individual and should not be guessable;

f) users should acknowledge receipt of passwords;

g) passwords should never be stored on computer systems in an unprotected form;

h) default vendor passwords should be altered following installation of systems or software.

Other information

Passwords are a common means of verifying a user's identity before access is given to an information system or service according to the user's authorization. Other technologies for user identification and authentication, such as biometrics, e.g. finger-print verification, signature verification, and use of hardware tokens, e.g. smart cards, are available, and should be considered if appropriate.

11.2.4 Review of user access rights

Control

Management should review users' access rights at regular intervals using a formal process.

Implementation guidance

The review of access rights should consider the following guidelines:

a) users' access rights should be reviewed at regular intervals, e.g. a period of 6 months, and after any changes, such as promotion, demotion, or termination of employment (see 11.2.1);

b) user access rights should be reviewed and re-allocated when moving from one employment to another within the same organization;

c) authorizations for special privileged access rights (see 11.2.2) should be reviewed at more frequent intervals, e.g. at a period of 3 months;

d) privilege allocations should be checked at regular intervals to ensure that unauthorized privileges have not been obtained;

e) changes to privileged accounts should be logged for periodic review.

Other information

It is necessary to regularly review users' access rights to maintain effective control over access to data and information services.

11.3 User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

The co-operation of authorized users is essential for effective security.

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

© ISO/IEC 2005 – All rights reserved

11.3.1 Password use

Control
Users should be required to follow good security practices in the selection and use of passwords.

Implementation guidance
All users should be advised to:

a) keep passwords confidential;

b) avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved;

c) change passwords whenever there is any indication of possible system or password compromise;

d) select quality passwords with sufficient minimum length which are:

   1) easy to remember;

   2) not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.;

   3) not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries);

   4) free of consecutive identical, all-numeric or all-alphabetic characters.

e) change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid re-using or cycling old passwords;

f) change temporary passwords at the first log-on;

g) not include passwords in any automated log-on process, e.g. stored in a macro or function key;

h) not share individual user passwords;

i) not use the same password for business and non-business purposes.

If users need to access multiple services, systems or platforms, and are required to maintain multiple separate passwords, they should be advised that they may use a single, quality password (see d) above) for all services where the user is assured that a reasonable level of protection has been established for the storage of the password within each service, system or platform.

Other information
Management of the help desk system dealing with lost or forgotten passwords needs special care as this may also be a means of attack to the password system.

11.3.2 Unattended user equipment

Control
Users should ensure that unattended equipment has appropriate protection.

Implementation guidance
All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection. Users should be advised to:

a) terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, e.g. a password protected screen saver;

b) log-off mainframe computers, servers, and office PCs when the session is finished (i.e. not just switch off the PC screen or terminal);

© ISO/IEC 2005 – All rights reserved

c) secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use (see also 11.3.3).

Other information
Equipment installed in user areas, e.g. workstations or file servers, may require specific protection from unauthorized access when left unattended for an extended period.

11.3.3 Clear desk and clear screen policy

Control
A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

Implementation guidance
The clear desk and clear screen policy should take into account the information classifications (see 7.2), legal and contractual requirements (see 15.1), and the corresponding risks and cultural aspects of the organization. The following guidelines should be considered:

a) sensitive or critical business information, e.g. on paper or on electronic storage media, should be locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated;

b) computers and terminals should be left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism when unattended and should be protected by key locks, passwords or other controls when not in use;

c) incoming and outgoing mail points and unattended facsimile machines should be protected;

d) unauthorised use of photocopiers and other reproduction technology (e.g., scanners, digital cameras) should be prevented;

e) documents containing sensitive or classified information should be removed from printers immediately.

Other information
A clear desk/clear screen policy reduces the risks of unauthorized access, loss of, and damage to information during and outside normal working hours. Safes or other forms of secure storage facilities might also protect information stored therein against disasters such as a fire, earthquake, flood or explosion.

Consider the use of printers with pin code function, so the originators are the only ones who can get their print outs, and only when standing next to the printer.

11.4 Network access control

Objective: To prevent unauthorized access to networked services.

Access to both internal and external networked services should be controlled.

User access to networks and network services should not compromise the security of the network services by ensuring:

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

b) appropriate authentication mechanisms are applied for users and equipment;

c) control of user access to information services in enforced.

© ISO/IEC 2005 – All rights reserved

11.4.1 Policy on use of network services

Control

Users should only be provided with access to the services that they have been specifically authorized to use.

Implementation guidance

A policy should be formulated concerning the use of networks and network services. This policy should cover:

a) the networks and network services which are allowed to be accessed;

b) authorization procedures for determining who is allowed to access which networks and networked services;

c) management controls and procedures to protect access to network connections and network services;

d) the means used to access networks and network services (e.g. the conditions for allowing dial-up access to an Internet service provider or remote system).

The policy on the use of network services should be consistent with the business access control policy (see 11.1).

Other information

Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.

11.4.2 User authentication for external connections

Control

Appropriate authentication methods should be used to control access by remote users.

Implementation guidance

Authentication of remote users can be achieved using, for example, a cryptographic based technique, hardware tokens, or a challenge/response protocol. Possible implementations of such techniques can be found in various virtual private network (VPN) solutions. Dedicated private lines can also be used to provide assurance of the source of connections.

Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations. When using this control, an organization should not use network services, which include call forwarding, or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. The call back process should ensure that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that the call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

© ISO/IEC 2005 – All rights reserved

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility. Cryptographic techniques, e.g. based on machine certificates, can be used for node authentication. This is part of several VPN based solutions.

Additional authentication controls should be implemented to control access to wireless networks. In particular, special care is needed in the selection of controls for wireless networks due to the greater opportunities for undetected interception and insertion of network traffic.

Other information
External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. This is especially important if the connection uses a network that is outside the control of the organization's security management.

11.4.3 Equipment identification in networks

Control
Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

Implementation guidance
Equipment identification can be used if it is important that the communication can only be initiated from a specific location or equipment. An identifier in or attached to, the equipment can be used to indicate whether this equipment is permitted to connect to the network. These identifiers should clearly indicate to which network the equipment is permitted to connect, if more than one network exists and particularly if these networks are of differing sensitivity. It may be necessary to consider physical protection of the equipment to maintain the security of the equipment identifier.

Other information
This control can be complemented with other techniques to authenticate the equipment's user (see 11.4.2). Equipment identification can be applied additionally to user authentication.

11.4.4 Remote diagnostic and configuration port protection

Control
Physical and logical access to diagnostic and configuration ports should be controlled.

Implementation guidance
Potential controls for the access to diagnostic and configuration ports include the use of a key lock and supporting procedures to control physical access to the port. An example for such a supporting procedure is to ensure that diagnostic and configuration ports are only accessible by arrangement between the manager of the computer service and the hardware/software support personnel requiring access.

Ports, services, and similar facilities installed on a computer or network facility, which are not specifically required for business functionality, should be disabled or removed.

Other information
Many computer systems, network systems, and communication systems are installed with a remote diagnostic or configuration facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access.

© ISO/IEC 2005 – All rights reserved

11.4.5 Segregation in networks

Control

Groups of information services, users, and information systems should be segregated on networks.

Implementation guidance

One method of controlling the security of large networks is to divide them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. A graduated set of controls can be applied in different logical network domains to further segregate the network security environments, e.g. publicly accessible systems, internal networks, and critical assets. The domains should be defined based on a risk assessment and the different security requirements within each of the domains.

Such a network perimeter can be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains (see 11.4.6 and 11.4.7) and to block unauthorized access in accordance with the organization's access control policy (see 11.1). An example of this type of gateway is what is commonly referred to as a firewall. Another method of segregating separate logical domains is to restrict network access by using virtual private networks for user groups within the organization.

Networks can also be segregated using the network device functionality, e.g. IP switching. Separate domains can then be implemented by controlling the network data flows using the routing/switching capabilities, such as access control lists.

The criteria for segregation of networks into domains should be based on the access control policy and access requirements (see 10.1), and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology (see 11.4.6 and 11.4.7).

In addition, segregation of networks should be based on the value and classification of information stored or processed in the network, levels of trust, or lines of business, in order to reduce the total impact of a service disruption.

Consideration should be given to the segregation of wireless networks from internal and private networks. As the perimeters of wireless networks are not well defined, a risk assessment should be carried out in such cases to identify controls (e.g. strong authentication, cryptographic methods, and frequency selection) to maintain network segregation.

Other information

Networks are increasingly being extended beyond traditional organizational boundaries, as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions might increase the risk of unauthorized access to existing information systems that use the network, some of which may require protection from other network users because of their sensitivity or criticality.

11.4.6 Network connection control

Control

For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1).

Implementation guidance

The network access rights of users should be maintained and updated as required by the access control policy (see 11.1.1).

© ISO/IEC 2005 – All rights reserved

The connection capability of users can be restricted through network gateways that filter traffic by means of pre-defined tables or rules. Examples of applications to which restrictions should be applied are:

a) messaging, e.g. electronic mail;

b) file transfer;

c) interactive access;

d) application access.

Linking network access rights to certain times of day or dates should be considered.

Other information
The incorporation of controls to restrict the connection capability of the users may be required by the access control policy for shared networks, especially those extending across organizational boundaries.

11.4.7 Network routing control

Control
Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Implementation guidance
Routing controls should be based on positive source and destination address checking mechanisms.

Security gateways can be used to validate source and destination addresses at internal and external network control points if proxy and/or network address translation technologies are employed. Implementers should be aware of the strength and shortcomings of any mechanisms deployed. The requirements for network routing control should be based on the access control policy (see 11.1).

Other information
Shared networks, especially those extending across organizational boundaries, may require additional routing controls. This particularly applies where networks are shared with third party (non-organization) users.

11.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

Security facilities should be used to restrict access to operating systems to authorized users. The facilities should be capable of the following:

a) authenticating authorized users, in accordance with a defined access control policy;

b) recording successful and failed system authentication attempts;

c) recording the use of special system privileges;

d) issuing alarms when system security policies are breached;

e) providing appropriate means for authentication;

f) where appropriate, restricting the connection time of users.

11.5.1 Secure log-on procedures

Control
Access to operating systems should be controlled by a secure log-on procedure.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
The procedure for logging into an operating system should be designed to minimize the opportunity for unauthorized access. The log-on procedure should therefore disclose the minimum of information about the system, in order to avoid providing an unauthorized user with any unnecessary assistance. A good log-on procedure should:

a) not display system or application identifiers until the log-on process has been successfully completed;

b) display a general notice warning that the computer should only be accessed by authorized users;

c) not provide help messages during the log-on procedure that would aid an unauthorized user;

d) validate the log-on information only on completion of all input data. If an error condition arises, the system should not indicate which part of the data is correct or incorrect;

e) limit the number of unsuccessful log-on attempts allowed, e.g. to three attempts, and consider:

   1) recording unsuccessful and successful attempts;

   2) forcing a time delay before further log-on attempts are allowed or rejecting any further attempts without specific authorization;

   3) disconnecting data link connections;

   4) sending an alarm message to the system console if the maximum number of log-on attempts is reached;

   5) setting the number of password retries in conjunction with the minimum length of the password and the value of the system being protected;

f) limit the maximum and minimum time allowed for the log-on procedure. If exceeded, the system should terminate the log-on;

g) display the following information on completion of a successful log-on:

   1) date and time of the previous successful log-on;

   2) details of any unsuccessful log-on attempts since the last successful log-on;

h) not display the password being entered or consider hiding the password characters by symbols;

i) not transmit passwords in clear text over a network.

Other information
If passwords are transmitted in clear text during the log-on session over a network, they may be captured by a network 'sniffer' program on the network.

11.5.2 User identification and authentication

Control
All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

Implementation guidance
This control should be applied for all types of users (including technical support personnel, operators, network administrators, system programmers, and database administrators).

© ISO/IEC 2005 – All rights reserved

User IDs should be used to trace activities to the responsible individual. Regular user activities should not be performed from privileged accounts.

In exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented for such cases. Additional controls may be required to maintain accountability.

Generic IDs for use by an individual should only be allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g. read only access), or where there are other controls in place (e.g. password for a generic ID only issued to one staff at a time and logging such instance).

Where strong authentication and identity verification is required, authentication methods alternative to passwords, such as cryptographic means, smart cards, tokens or biometric means, should be used.

Other information
Passwords (see also 11.3.1 and 11.5.3) are a very common way to provide identification and authentication based on a secret that only the user knows. The same can also be achieved with cryptographic means and authentication protocols. The strength of user identification and authentication should be suitable to the sensitivity of the information to be accessed.

Objects such as memory tokens or smart cards that users possess can also be used for identification and authentication. Biometric authentication technologies that use the unique characteristics or attributes of an individual can also be used to authenticate the person's identity. A combination of technologies and mechanisms securely linked will result in stronger authentication.

11.5.3 Password management system

Control
Systems for managing passwords should be interactive and should ensure quality passwords.

Implementation guidance
A password management system should:

a) enforce the use of individual user IDs and passwords to maintain accountability;

b) allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;

c) enforce a choice of quality passwords (see 11.3.1);

d) enforce password changes (see 11.3.1);

e) force users to change temporary passwords at the first log-on (see 11.2.3);

f) maintain a record of previous user passwords and prevent re-use;

g) not display passwords on the screen when being entered;

h) store password files separately from application system data;

i) store and transmit passwords in protected (e.g. encrypted or hashed) form.

Other information
Passwords are one of the principal means of validating a user's authority to access a computer service.

Some applications require user passwords to be assigned by an independent authority; in such cases, points b), d) and e) of the above guidance do not apply. In most cases the passwords are selected and maintained by users. See section 11.3.1 for guidance on the use of passwords.

© ISO/IEC 2005 – All rights reserved

11.5.4 Use of system utilities

Control

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

Implementation guidance

The following guidelines for the use of system utilities should be considered:

a) use of identification, authentication, and authorization procedures for system utilities;

b) segregation of system utilities from applications software;

c) limitation of the use of system utilities to the minimum practical number of trusted, authorized users (see also 11.2.2);

d) authorization for ad hoc use of systems utilities;

e) limitation of the availability of system utilities, e.g. for the duration of an authorized change;

f) logging of all use of system utilities;

g) defining and documenting of authorization levels for system utilities;

h) removal or disabling of all unnecessary software based utilities and system software;

i) not making system utilities available to users who have access to applications on systems where segregation of duties is required.

Other information

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls.

11.5.5 Session time-out

Control

Inactive sessions should shut down after a defined period of inactivity.

Implementation guidance

A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. The time-out delay should reflect the security risks of the area, the classification of the information being handled and the applications being used, and the risks related to the users of the equipment.

A limited form of time-out facility can be provided for some systems, which clears the screen and prevents unauthorized access but does not close down the application or network sessions.

Other information

This control is particularly important in high risk locations, which include public or external areas outside the organization's security management. The sessions should be shut down to prevent access by unauthorized persons and denial of service attacks.

11.5.6 Limitation of connection time

Control

Restrictions on connection times should be used to provide additional security for high-risk applications.

© ISO/IEC 2005 – All rights reserved

Implementation guidance

Connection time controls should be considered for sensitive computer applications, especially from high risk locations, e.g. public or external areas that are outside the organization's security management. Examples of such restrictions include:

a) using predetermined time slots, e.g. for batch file transmissions, or regular interactive sessions of short duration;

b) restricting connection times to normal office hours if there is no requirement for overtime or extended-hours operation;

c) considering re-authentication at timed intervals.

Other information

Limiting the period during which connections to computer services are allowed reduces the window of opportunity for unauthorized access. Limiting the duration of active sessions prevents users from holding sessions open to prevent re-authenticating.

11.6 Application and information access control

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

Security facilities should be used to restrict access to and within application systems.

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

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

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

c) not compromise other systems with which information resources are shared.

11.6.1 Information access restriction

Control

Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

Implementation guidance

Restrictions to access should be based on individual business application requirements. The access control policy should also be consistent with the organizational access policy (see section 11.1).

Applying the following guidelines should be considered in order to support access restriction requirements:

a) providing menus to control access to application system functions;

b) controlling the access rights of users, e.g. read, write, delete, and execute;

c) controlling access rights of other applications;

d) ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations; this should include periodic reviews of such outputs to ensure that redundant information is removed.

© ISO/IEC 2005 – All rights reserved

11.6.2 Sensitive system isolation

Control
Sensitive systems should have a dedicated (isolated) computing environment.

Implementation guidance
The following points should be considered for sensitive system isolation:

a) the sensitivity of an application system should be explicitly identified and documented by the application owner (see 7.1.2);

b) when a sensitive application is to run in a shared environment, the application systems with which it will share resources and the corresponding risks should be identified and accepted by the owner of the sensitive application.

Other information
Some application systems are sufficiently sensitive to potential loss that they require special handling. The sensitivity may indicate that the application system:

a) should run on a dedicated computer; or

b) should only share resources with trusted applications systems.

Isolation could be achieved using physical or logical methods (see also 11.4.5).

11.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.
The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

11.7.1 Mobile computing and communications

Control
A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

Implementation guidance
When using mobile computing and communicating facilities, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised. The mobile computing policy should take into account the risks of working with mobile computing equipment in unprotected environments.

The mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection. This policy should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques (see 12.3).

Users of mobile computing facilities in public places should take care to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date (see 10.4).

© ISO/IEC 2005 – All rights reserved

Back-ups of critical business information should be taken regularly. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks. Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication, and with suitable access control mechanisms in place (see 11.4).

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centres, and meeting places. A specific procedure taking into account legal, insurance and other security requirements of the organization should be established for cases of theft or loss of the mobile computing facilities. Equipment carrying important, sensitive, and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment (see 9.2.5).

Training should be arranged for personnel using mobile computing to raise their awareness on the additional risks resulting from this way of working and the controls that should be implemented.

Other information

Mobile network wireless connections are similar to other types of network connection, but have important differences that should be considered when identifying controls. Typical differences are 1) some wireless security protocols are immature and have known weaknesses and 2) information stored on mobile computers may not be backed-up because of limited network bandwidth and/or because mobile equipment may not be connected at the times when back-ups are scheduled.

11.7.2 Teleworking

Control

A policy, operational plans and procedures should be developed and implemented for teleworking activities.

Implementation guidance

Organizations should only authorize teleworking activities if they are satisfied that appropriate security arrangements and controls are in place, and that these comply with the organization's security policy.

Suitable protection of the teleworking site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. Teleworking activities should both be authorized and controlled by management, and it should be ensured that suitable arrangements are in place for this way of working.

The following matters should be considered:

a) the existing physical security of the teleworking site, taking into account the physical security of the building and the local environment;

b) the proposed physical teleworking environment;

c) the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system;

© ISO/IEC 2005 – All rights reserved

d) the threat of unauthorized access to information or resources from other persons using the accommodation, e.g. family and friends;

e) the use of home networks and requirements or restrictions on the configuration of wireless network services;

f) policies and procedures to prevent disputes concerning rights to intellectual property developed on privately owned equipment;

g) access to privately owned equipment (to check the security of the machine or during an investigation), which may be prevented by legislation;

h) software licensing agreements that are such that organizations may become liable for licensing for client software on workstations owned privately by employees, contractors or third party users;

i) anti-virus protection and firewall requirements.

The guidelines and arrangements to be considered should include:

a) the provision of suitable equipment and storage furniture for the teleworking activities, where the use of privately owned equipment that is not under the control of the organization is not allowed;

b) a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the teleworker is authorized to access;

c) the provision of suitable communication equipment, including methods for securing remote access;

d) physical security;

e) rules and guidance on family and visitor access to equipment and information;

f) the provision of hardware and software support and maintenance;

g) the provision of insurance;

h) the procedures for back-up and business continuity;

i) audit and security monitoring;

j) revocation of authority and access rights, and the return of equipment when the teleworking activities are terminated.

Other information

Teleworking uses communications technology to enable personnel to work remotely from a fixed location outside of their organization.

© ISO/IEC 2005 – All rights reserved

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.

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

12.1.1 Security requirements analysis and specification

Control

Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

Implementation guidance

Specifications for the requirements for controls should consider the automated controls to be incorporated in the information system, and the need for supporting manual controls. Similar considerations should be applied when evaluating software packages, developed or purchased, for business applications.

Security requirements and controls should reflect the business value of the information assets involved (see also 7.2), and the potential business damage, which might result from a failure or absence of security.

System requirements for information security and processes for implementing security should be integrated in the early stages of information system projects. Controls introduced at the design stage are significantly cheaper to implement and maintain than those included during or after implementation.

If products are purchased, a formal testing and acquisition process should be followed. Contracts with the supplier should address the identified security requirements. Where the security functionality in a proposed product does not satisfy the specified requirement then the risk introduced and associated controls should be reconsidered prior to purchasing the product. Where additional functionality is supplied and causes a security risk, this should be disabled or the proposed control structure should be reviewed to determine if advantage can be taken of the enhanced functionality available.

Other information

If considered appropriate, for example for cost reasons, management may wish to make use of independently evaluated and certified products. Further information about evaluation criteria for IT security products can be found in ISO/IEC 15408 or other evaluation or certification standards, as appropriate.

ISO/IEC TR 13335-3 provides guidance on the use of risk management processes to identify requirements for security controls.

© ISO/IEC 2005 – All rights reserved

12.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

12.2.1 Input data validation

Control

Data input to applications should be validated to ensure that this data is correct and appropriate.

Implementation guidance

Checks should be applied to the input of business transactions, standing data (e.g. names and addresses, credit limits, customer reference numbers), and parameter tables (e.g. sales prices, currency conversion rates, tax rates). The following guidelines should be considered:

a) dual input or other input checks, such as boundary checking or limiting fields to specific ranges of input data, to detect the following errors:
   1) out-of-range values;
   2) invalid characters in data fields;
   3) missing or incomplete data;
   4) exceeding upper and lower data volume limits;
   5) unauthorized or inconsistent control data;
b) periodic review of the content of key fields or data files to confirm their validity and integrity;
c) inspecting hard-copy input documents for any unauthorized changes (all changes to input documents should be authorized);
d) procedures for responding to validation errors;
e) procedures for testing the plausibility of the input data;
f) defining the responsibilities of all personnel involved in the data input process;
g) creating a log of the activities involved in the data input process (see 10.10.1).

Other information

Automatic examination and validation of input data can be considered, where applicable, to reduce the risk of errors and to prevent standard attacks including buffer overflow and code injection.

12.2.2 Control of internal processing

Control

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
The design and implementation of applications should ensure that the risks of processing failures leading to a loss of integrity are minimized. Specific areas to consider include:

a) the use of add, modify, and delete functions to implement changes to data;

b) the procedures to prevent programs running in the wrong order or running after failure of prior processing (see also 10.1.1);

c) the use of appropriate programs to recover from failures to ensure the correct processing of data;

d) protection against attacks using buffer overruns/overflows.

An appropriate checklist should be prepared, activities documented, and the results should be kept secure. Examples of checks that can be incorporated include the following:

a) session or batch controls, to reconcile data file balances after transaction updates;

b) balancing controls, to check opening balances against previous closing balances, namely:

   1) run-to-run controls;

   2) file update totals;

   3) program-to-program controls;

c) validation of system-generated input data (see 12.2.1);

d) checks on the integrity, authenticity or any other security feature of data or software downloaded, or uploaded, between central and remote computers;

e) hash totals of records and files;

f) checks to ensure that application programs are run at the correct time;

g) checks to ensure that programs are run in the correct order and terminate in case of a failure, and that further processing is halted until the problem is resolved;

h) creating a log of the activities involved in the processing (see 10.10.1).

Other information
Data that has been correctly entered can be corrupted by hardware errors, processing errors or through deliberate acts. The validation checks required will depend on the nature of the application and the business impact of any corruption of data.

12.2.3 Message integrity

Control
Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

Implementation guidance
An assessment of security risks should be carried out to determine if message integrity is required and to identify the most appropriate method of implementation.

Other information
Cryptographic techniques (see 12.3) can be used as an appropriate means of implementing message authentication.

12.2.4 Output data validation

Control
Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

© ISO/IEC 2005 – All rights reserved

Implementation guidance
Output validation may include:

a) plausibility checks to test whether the output data is reasonable;

b) reconciliation control counts to ensure processing of all data;

c) providing sufficient information for a reader or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information;

d) procedures for responding to output validation tests;

e) defining the responsibilities of all personnel involved in the data output process;

f) creating a log of activities in the data output validation process.

Other information
Typically, systems and applications are constructed on the assumption that having undertaken appropriate validation, verification, and testing, the output will always be correct. However, this assumption is not always valid; i.e. systems that have been tested may still produce incorrect output under some circumstances.

12.3 Cryptographic controls

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

A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

12.3.1 Policy on the use of cryptographic controls

Control
A policy on the use of cryptographic controls for protection of information should be developed and implemented.

Implementation guidance
When developing a cryptographic policy the following should be considered:

a) the management approach towards the use of cryptographic controls across the organization, including the general principles under which business information should be protected (see also 5.1.1);

b) based on a risk assessment, the required level of protection should be identified taking into account the type, strength, and quality of the encryption algorithm required;

c) the use of encryption for protection of sensitive information transported by mobile or removable media, devices or across communication lines;

d) the approach to key management, including methods to deal with the protection of cryptographic keys and the recovery of encrypted information in the case of lost, compromised or damaged keys;

e) roles and responsibilities, e.g. who is responsible for:

   1) the implementation of the policy;

   2) the key management, including key generation (see also 12.3.2);

© ISO/IEC 2005 – All rights reserved

f) the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes);

g) the impact of using encrypted information on controls that rely upon content inspection (e.g. virus detection).

When implementing the organization's cryptographic policy, consideration should be given to the regulations and national restrictions that might apply to the use of cryptographic techniques in different parts of the world and to the issues of trans-border flow of encrypted information (see also 15.1.6).

Cryptographic controls can be used to achieve different security objectives, e.g.:

a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;

b) integrity/authenticity: using digital signatures or message authentication codes to protect the authenticity and integrity of stored or transmitted sensitive or critical information;

c) non-repudiation: using cryptographic techniques to obtain proof of the occurrence or non-occurrence of an event or action.

Other information

Making a decision as to whether a cryptographic solution is appropriate should be seen as part of the wider process of risk assessment and selection of controls. This assessment can then be used to determine whether a cryptographic control is appropriate, what type of control should be applied and for what purpose and business processes.

A policy on the use of cryptographic controls is necessary to maximize the benefits and minimize the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. When using digital signatures, consideration should be given to any relevant legislation, in particular legislation describing the conditions under which a digital signature is legally binding (see 15.1).

Specialist advice should be sought to identify the appropriate level of protection and to define suitable specifications that will provide the required protection and support the implementation of a secure key management system (see also 12.3.2).

ISO/IEC JTC1 SC27 has developed several standards related to cryptographic controls. Further information can also be found in IEEE P1363 and the OECD Guidelines on Cryptography.

12.3.2 Key management

Control

Key management should be in place to support the organization's use of cryptographic techniques.

Implementation guidance

All cryptographic keys should be protected against modification, loss, and destruction. In addition, secret and private keys need protection against unauthorized disclosure. Equipment used to generate, store and archive keys should be physically protected.

A key management system should be based on an agreed set of standards, procedures, and secure methods for:

a) generating keys for different cryptographic systems and different applications;

b) generating and obtaining public key certificates;

© ISO/IEC 2005 – All rights reserved

c) distributing keys to intended users, including how keys should be activated when received;

d) storing keys, including how authorized users obtain access to keys;

e) changing or updating keys including rules on when keys should be changed and how this will be done;

f) dealing with compromised keys;

g) revoking keys including how keys should be withdrawn or deactivated, e.g. when keys have been compromised or when a user leaves an organization (in which case keys should also be archived);

h) recovering keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information;

i) archiving keys, e.g. for information archived or backed up;

j) destroying keys;

k) logging and auditing of key management related activities.

In order to reduce the likelihood of compromise, activation, and deactivation dates for keys should be defined so that the keys can only be used for a limited period of time. This period of time should be dependent on the circumstances under which the cryptographic control is being used, and the perceived risk.

In addition to securely managing secret and private keys, the authenticity of public keys should also be considered. This authentication process can be done using public key certificates which are normally issued by a certification authority, which should be a recognized organization with suitable controls and procedures in place to provide the required degree of trust.

The contents of service level agreements or contracts with external suppliers of cryptographic services, e.g. with a certification authority, should cover issues of liability, reliability of services and response times for the provision of services (see 6.2.3).

Other information

The management of cryptographic keys is essential to the effective use of cryptographic techniques. ISO/IEC 11770 provides further information on key management. The two types of cryptographic techniques are:

a) secret key techniques, where two or more parties share the same key and this key is used both to encrypt and decrypt information; this key has to be kept secret since anyone having access to the key is able to decrypt all information being encrypted with that key, or to introduce unauthorized information using the key;

b) public key techniques, where each user has a key pair, a public key (which can be revealed to anyone) and a private key (which has to be kept secret); public key techniques can be used for encryption and to produce digital signatures (see also ISO/IEC 9796 and ISO/IEC 14888).

There is a threat of forging a digital signature by replacing a user's public key with. This problem is addressed by the use of a public key certificate.

Cryptographic techniques can also be used to protect cryptographic keys. Procedures may need to be considered for handling legal requests for access to cryptographic keys, e.g. encrypted information may need to be made available in an unencrypted form as evidence in a court case.

© ISO/IEC 2005 – All rights reserved

12.4 Security of system files

Objective: To ensure the security of system files. Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

12.4.1 Control of operational software

Control

There should be procedures in place to control the installation of software on operational systems.

Implementation guidance

To minimize the risk of corruption to operational systems, the following guidelines should be considered to control changes:

a) the updating of the operational software, applications, and program libraries should only be performed by trained administrators upon appropriate management authorization (see 12.4.3);

b) operational systems should only hold approved executable code, and not development code or compilers;

c) applications and operating system software should only be implemented after extensive and successful testing; the tests should include tests on usability, security, effects on other systems and user-friendliness, and should be carried out on separate systems (see also 10.1.4); it should be ensured that all corresponding program source libraries have been updated;

d) a configuration control system should be used to keep control of all implemented software as well as the system documentation;

e) a rollback strategy should be in place before changes are implemented;

f) an audit log should be maintained of all updates to operational program libraries;

g) previous versions of application software should be retained as a contingency measure;

h) old versions of software should be archived, together with all required information and parameters, procedures, configuration details, and supporting software for as long as the data is retained in archive.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.

Any decision to upgrade to a new release should take into account the business requirements for the change, and the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses (see also 12.6.1).

Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities should be monitored.

Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

© ISO/IEC 2005 – All rights reserved

Other information
Operating systems should only be upgraded when there is a requirement to do so, for example, if the current version of the operating system no longer supports the business requirements. Upgrades should not take place just because a new version of the operating system is available. New versions of operating systems may be less secure, less stable, and less well understood than current systems.

12.4.2 Protection of system test data

Control
Test data should be selected carefully, and protected and controlled.

Implementation guidance
The use of operational databases containing personal information or any other sensitive information for testing purposes should be avoided. If personal or otherwise sensitive information is used for testing purposes, all sensitive details and content should be removed or modified beyond recognition before use. The following guidelines should be applied to protect operational data, when used for testing purposes:

a) the access control procedures, which apply to operational application systems, should also apply to test application systems;

b) there should be separate authorization each time operational information is copied to a test application system;

c) operational information should be erased from a test application system immediately after the testing is complete;

d) the copying and use of operational information should be logged to provide an audit trail.

Other information
System and acceptance testing usually requires substantial volumes of test data that are as close as possible to operational data.

12.4.3 Access control to program source code

Control
Access to program source code should be restricted.

Implementation guidance
Access to program source code and associated items (such as designs, specifications, verification plans and validation plans) should be strictly controlled, in order to prevent the introduction of unauthorized functionality and to avoid unintentional changes. For program source code, this can be achieved by controlled central storage of such code, preferably in program source libraries. The following guidelines should then be considered (see also 11) to control access to such program source libraries in order to reduce the potential for corruption of computer programs:

a) where possible, program source libraries should not be held in operational systems;

b) the program source code and the program source libraries should be managed according to established procedures;

c) support personnel should not have unrestricted access to program source libraries;

d) the updating of program source libraries and associated items, and the issuing of program sources to programmers should only be performed after appropriate authorization has been received;

e) program listings should be held in a secure environment (see 10.7.4);

© ISO/IEC 2005 – All rights reserved

f) an audit log should be maintained of all accesses to program source libraries;

g) maintenance and copying of program source libraries should be subject to strict change control procedures (see 12.5.1).

Other information
Program source code is code written by programmers, which is compiled (and linked) to create executables. Certain programming languages do not formally distinguish between source code and executables as the executables are created at the time they are activated.

The standards ISO 10007 and ISO/IEC 12207 provide further information about configuration management and the software lifecycle process.

12.5 Security in development and support processes

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

Project and support environments should be strictly controlled.

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

12.5.1 Change control procedures

Control
The implementation of changes should be controlled by the use of formal change control procedures.

Implementation guidance
Formal change control procedures should be documented and enforced in order to minimize the corruption of information systems. Introduction of new systems and major changes to existing systems should follow a formal process of documentation, specification, testing, quality control, and managed implementation.

This process should include a risk assessment, analysis of the impacts of changes, and specification of security controls needed. This process should also ensure that existing security and control procedures are not compromised, that support programmers are given access only to those parts of the system necessary for their work, and that formal agreement and approval for any change is obtained.

Wherever practicable, application and operational change control procedures should be integrated (see also 10.1.2). The change procedures should include:

a) maintaining a record of agreed authorization levels;

b) ensuring changes are submitted by authorized users;

c) reviewing controls and integrity procedures to ensure that they will not be compromised by the changes;

d) identifying all software, information, database entities, and hardware that require amendment;

e) obtaining formal approval for detailed proposals before work commences;

f) ensuring authorized users accept changes prior to implementation;

g) ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of;

h) maintaining a version control for all software updates;

i) maintaining an audit trail of all change requests;

© ISO/IEC 2005 – All rights reserved

j) ensuring that operating documentation (see 10.1.1) and user procedures are changed as necessary to remain appropriate;

k) ensuring that the implementation of changes takes place at the right time and does not disturb the business processes involved.

Other information
Changing software can impact the operational environment.

Good practice includes the testing of new software in an environment segregated from both the production and development environments (see also 10.1.4). This provides a means of having control over new software and allowing additional protection of operational information that is used for testing purposes. This should include patches, service packs, and other updates. Automated updates should not be used on critical systems as some updates may cause critical applications to fail (see 12.6).

12.5.2 Technical review of applications after operating system changes

Control
When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

Implementation guidance
This process should cover:

a) review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

b) ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes;

c) ensuring that notification of operating system changes is provided in time to allow appropriate tests and reviews to take place before implementation;

d) ensuring that appropriate changes are made to the business continuity plans (see clause 14).

A specific group or individual should be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes (see 12.6).

12.5.3 Restrictions on changes to software packages

Control
Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

Implementation guidance
As far as possible, and practicable, vendor-supplied software packages should be used without modification. Where a software package needs to be modified the following points should be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) whether the consent of the vendor should be obtained;

c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the organization becomes responsible for the future maintenance of the software as a result of changes.

© ISO/IEC 2005 – All rights reserved

If changes are necessary the original software should be retained and the changes applied to a clearly identified copy. A software update management process should be implemented to ensure the most up-to-date approved patches and application updates are installed for all authorized software (see 12.6). All changes should be fully tested and documented, so that they can be reapplied if necessary to future software upgrades. If required, the modifications should be tested and validated by an independent evaluation body.

12.5.4 Information leakage

Control
Opportunities for information leakage should be prevented.

Implementation guidance
The following should be considered to limit the risk of information leakage, e.g. through the use and exploitation of covert channels:

a) scanning of outbound media and communications for hidden information;

b) masking and modulating system and communications behaviour to reduce the likelihood of a third party being able to deduce information from such behaviour;

c) making use of systems and software that are considered to be of high integrity, e.g. using evaluated products (see ISO/IEC 15408);

d) regular monitoring of personnel and system activities, where permitted under existing legislation or regulation;

e) monitoring resource usage in computer systems.

Other information
Covert Channels are paths which are not intended to conduct information flows, but which may nevertheless exist in a system or network. For example, manipulating bits in communications protocol packets could be used as a hidden method of signaling. By their nature, preventing the existence of all possible covert channels would be difficult, if not impossible. However, the exploitation of such channels is often carried out by Trojan code (see also 10.4.1). Taking measures to protect against Trojan code therefore reduces the risk of covert channel exploitation.

Prevention of unauthorized network access (11.4), as well as policies and procedures to discourage misuse of information services by personnel (15.1.5), will help to protect against covert channels.

12.5.5 Outsourced software development

Control
Outsourced software development should be supervised and monitored by the organization.

Implementation guidance
Where software development is outsourced, the following points should be considered:

a) licensing arrangements, code ownership, and intellectual property rights (see 15.1.2);

b) certification of the quality and accuracy of the work carried out;

c) escrow arrangements in the event of failure of the third party;

d) rights of access for audit of the quality and accuracy of work done;

e) contractual requirements for quality and security functionality of code;

f) testing before installation to detect malicious and Trojan code.

© ISO/IEC 2005 – All rights reserved

12.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

12.6.1 Control of technical vulnerabilities

Control

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Implementation guidance

A current and complete inventory of assets (see 7.1) is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version numbers, current state of deployment (e.g. what software is installed on what systems), and the person(s) within the organization responsible for the software.

Appropriate, timely action should be taken in response to the identification of potential technical vulnerabilities. The following guidance should be followed to establish an effective management process for technical vulnerabilities:

a) the organization should define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required;

b) information resources that will be used to identify relevant technical vulnerabilities and to maintain awareness about them should be identified for software and other technology (based on the asset inventory list, see 7.1.1); these information resources should be updated based on changes in the inventory, or when other new or useful resources are found;

c) a timeline should be defined to react to notifications of potentially relevant technical vulnerabilities;

d) once a potential technical vulnerability has been identified, the organization should identify the associated risks and the actions to be taken; such action could involve patching of vulnerable systems and/or applying other controls;

e) depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management (see 12.5.1) or by following information security incident response procedures (see 13.2);

f) if a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch);

g) patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered, such as

   1) turning off services or capabilities related to the vulnerability;

   2) adapting or adding access controls, e.g. firewalls, at network borders (see 11.4.5);

   3) increased monitoring to detect or prevent actual attacks;

   4) raising awareness of the vulnerability;

© ISO/IEC 2005 – All rights reserved

h) an audit log should be kept for all procedures undertaken;

i) the technical vulnerability management process should be regularly monitored and evaluated in order to ensure its effectiveness and efficiency;

j) systems at high risk should be addressed first.

Other information

The correct functioning of an organization's technical vulnerability management process is critical to many organizations and should therefore be regularly monitored. An accurate inventory is essential to ensure that potentially relevant technical vulnerabilities are identified.

Technical vulnerability management can be viewed as a sub-function of change management and as such can take advantage of the change management processes and procedures (see 10.1.2 and 12.5.1).

Vendors are often under significant pressure to release patches as soon as possible. Therefore, a patch may not address the problem adequately and may have negative side effects. Also, in some cases, uninstalling a patch may not be easily achieved once the patch has been applied.

If adequate testing of the patches is not possible, e.g. because of costs or lack of resources, a delay in patching can be considered to evaluate the associated risks, based on the experience reported by other users.

© ISO/IEC 2005 – All rights reserved

13 Information security incident management

13.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

13.1.1 Reporting information security events

Control

Information security events should be reported through appropriate management channels as quickly as possible.

Implementation guidance

A formal information security event reporting procedure should be established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event. A point of contact should be established for the reporting of information security events. It should be ensured that this point of contact is known throughout the organization, is always available and is able to provide adequate and timely response.

All employees, contractors and third party users should be made aware of their responsibility to report any information security events as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact. The reporting procedures should include:

a) suitable feedback processes to ensure that those reporting information security events are notified of results after the issue has been dealt with and closed;

b) information security event reporting forms to support the reporting action, and to help the person reporting to remember all necessary actions in case of an information security event;

c) the correct behaviour to be undertaken in case of an information security event, i.e.

   1) noting all important details (e.g. type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour) immediately;

   2) not carrying out any own action, but immediately reporting to the point of contact;

d) reference to an established formal disciplinary process for dealing with employees, contractors or third party users who commit security breaches.

In high-risk environments, a duress alarm[4] may be provided whereby a person under duress can indicate such problems. The procedures for responding to duress alarms should reflect the high risk situation such alarms are indicating.

[4] A duress alarm is a method for secretly indicating that an action is taking place 'under duress.'

© ISO/IEC 2005 – All rights reserved

Other Information
Examples of information security events and incidents are:

a) loss of service, equipment or facilities,
b) system malfunctions or overloads,
c) human errors,
d) non-compliances with policies or guidelines,
e) breaches of physical security arrangements,
f) uncontrolled system changes,
g) malfunctions of software or hardware,
h) access violations.

With due care of confidentiality aspects, information security incidents can be used in user awareness training (see 8.2.2) as examples of what could happen, how to respond to such incidents, and how to avoid them in the future. To be able to address information security events and incidents properly it might be necessary to collect evidence as soon as possible after the occurrence (see 13.2.3).

Malfunctions or other anomalous system behavior may be an indicator of a security attack or actual security breach and should therefore always be reported as information security event.

More information about reporting of information security events and management of information security incidents can be found in ISO/IEC TR 18044.

13.1.2 Reporting security weaknesses

Control
All employees, contractors and third party users of information systems and services should be required to note and report any observed or suspected security weaknesses in systems or services.

Implementation guidance
All employees, contractors and third party users should report these matters either to their management or directly to their service provider as quickly as possible in order to prevent information security incidents. The reporting mechanism should be as easy, accessible, and available as possible. They should be informed that they should not, in any circumstances, attempt to prove a suspected weakness.

Other Information
Employees, contractors and third party users should be advised not to attempt to prove suspected security weaknesses. Testing weaknesses might be interpreted as a potential misuse of the system and could also cause damage to the information system or service and result in legal liability for the individual performing the testing.

13.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

Where evidence is required, it should be collected to ensure compliance with legal requirements.

© ISO/IEC 2005 – All rights reserved

13.2.1 Responsibilities and procedures

Control

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

Implementation guidance

In addition to reporting of information security events and weaknesses (see also 13.1), the monitoring of systems, alerts, and vulnerabilities (10.10.2) should be used to detect information security incidents. The following guidelines for information security incident management procedures should be considered:

a) procedures should be established to handle different types of information security incident, including:
   1) information system failures and loss of service;
   2) malicious code (see 10.4.1);
   3) denial of service;
   4) errors resulting from incomplete or inaccurate business data;
   5) breaches of confidentiality and integrity;
   6) misuse of information systems.

b) in addition to normal contingency plans (see 14.1.3), the procedures should also cover (see also 13.2.2):
   1) analysis and identification of the cause of the incident;
   2) containment;
   3) planning and implementation of corrective action to prevent recurrence, if necessary;
   4) communication with those affected by or involved with recovery from the incident;
   5) reporting the action to the appropriate authority;

c) audit trails and similar evidence should be collected (see 13.2.3) and secured, as appropriate, for:
   1) internal problem analysis;
   2) use as forensic evidence in relation to a potential breach of contract breach or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
   3) negotiating for compensation from software and service suppliers;

d) action to recover from security breaches and correct system failures should be carefully and formally controlled; the procedures should ensure that:
   1) only clearly identified and authorized personnel are allowed access to live systems and data (see also 6.2 for external access);
   2) all emergency actions taken are documented in detail;
   3) emergency action is reported to management and reviewed in an orderly manner;
   4) the integrity of business systems and controls is confirmed with minimal delay.

The objectives for information security incident management should be agreed with management, and it should be ensured that those responsible for information security incident management understand the organization's priorities for handling information security incidents.

© ISO/IEC 2005 – All rights reserved

Other information
Information security incidents might transcend organizational and national boundaries. To respond to such incidents there is an increasing need to coordinate response and share information about these incidents with external organizations as appropriate.

13.2.2 Learning from information security incidents

Control
There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

Implementation guidance
The information gained from the evaluation of information security incidents should be used to identify recurring or high impact incidents.

Other Information
The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process (see 5.1.2).

13.2.3 Collection of evidence

Control
Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal) evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Implementation guidance
Internal procedures should be developed and followed when collecting and presenting evidence for the purposes of disciplinary action handled within an organization.

In general, the rules for evidence cover:

a) admissibility of evidence: whether or not the evidence can be used in court;

b) weight of evidence: the quality and completeness of the evidence.

To achieve admissibility of the evidence, the organization should ensure that their information systems comply with any published standard or code of practice for the production of admissible evidence.

The weight of evidence provided should comply with any applicable requirements. To achieve weight of evidence, the quality and completeness of the controls used to correctly and consistently protect the evidence (i.e. process control evidence); throughout the period that the evidence to be recovered was stored and processed should be demonstrated by a strong evidence trail. In general, such a strong trail can be established under the following conditions:

a) for paper documents: the original is kept securely with a record of the individual who found the document, where the document was found, when the document was found and who witnessed the discovery; any investigation should ensure that originals are not tampered with;

b) for information on computer media: mirror images or copies (depending on applicable requirements) of any removable media, information on hard disks or in memory should be taken to ensure availability; the log of all actions during the copying process should be kept and the process should be witnessed; the original media and the log (if this is not possible, at least one mirror image or copy) should be kept securely and untouched.

© ISO/IEC 2005 – All rights reserved

Any forensics work should only be performed on copies of the evidential material. The integrity of all evidential material should be protected. Copying of evidential material should be supervised by trustworthy personnel and information on when and where the copying process was executed, who performed the copying activities and which tools and programs have been utilized should be logged.

Other information

When an information security event is first detected, it may not be obvious whether or not the event will result in court action. Therefore, the danger exists that necessary evidence is destroyed intentionally or accidentally before the seriousness of the incident is realized. It is advisable to involve a lawyer or the police early in any contemplated legal action and take advice on the evidence required.

Evidence may transcend organizational and/or jurisdictional boundaries. In such cases, it should be ensured that the organization is entitled to collect the required information as evidence. The requirements of different jurisdictions should also be considered to maximize chances of admission across the relevant jurisdictions.

© ISO/IEC 2005 – All rights reserved

14 Business continuity management

14.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.

The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization.

Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

14.1.1 Including information security in the business continuity management process

Control

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

Implementation guidance

The process should bring together the following key elements of business continuity management:

a) understanding the risks the organization is facing in terms of likelihood and impact in time, including an identification and prioritisation of critical business processes (see 14.1.2);

b) identifying all the assets involved in critical business processes (see 7.1.1);

c) understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities;

d) considering the purchase of suitable insurance which may form part of the overall business continuity process, as well as being part of operational risk management;

e) identifying and considering the implementation of additional preventive and mitigating controls;

f) identifying sufficient financial, organizational, technical, and environmental resources to address the identified information security requirements;

g) ensuring the safety of personnel and the protection of information processing facilities and organizational property;

© ISO/IEC 2005 – All rights reserved

h) formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy (see 14.1.3);

i) regular testing and updating of the plans and processes put in place (see 14.1.5);

j) ensuring that the management of business continuity is incorporated in the organization's processes and structure; responsibility for the business continuity management process should be assigned at an appropriate level within the organization (see 6.1.1).

14.1.2 Business continuity and risk assessment

Control

Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

Implementation guidance

Information security aspects of business continuity should be based on identifying events (or sequence of events) that can cause interruptions to the organizations business processes, e.g. equipment failure, human errors, theft, fire, natural disasters and acts of terrorism. This should be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period.

Business continuity risk assessments should be carried out with full involvement from owners of business resources and processes. This assessment should consider all business processes and should not be limited to the information processing facilities, but should include the results specific to information security. It is important to link the different risk aspects together, to obtain a complete picture of the business continuity requirements of the organization. The assessment should identify, quantify, and prioritise risks against criteria and objectives relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

Depending on the results of the risk assessment, a business continuity strategy should be developed to determine the overall approach to business continuity. Once this strategy has been created, endorsement should be provided by management, and a plan created and endorsed to implement this strategy.

14.1.3 Developing and implementing continuity plans including information security

Control

Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

Implementation guidance

The business continuity planning process should consider the following:

a) identification and agreement of all responsibilities and business continuity procedures;

b) identification of the acceptable loss of information and services;

c) implementation of the procedures to allow recovery and restoration of business operations and availability of information in required time-scales; particular attention needs to be given to the assessment of internal and external business dependencies and the contracts in place;

d) operational procedures to follow pending completion of recovery and restoration;

e) documentation of agreed procedures and processes;

© ISO/IEC 2005 – All rights reserved

f) appropriate education of staff in the agreed procedures and processes, including crisis management;

g) testing and updating of the plans.

The planning process should focus on the required business objectives, e.g. restoring of specific communication services to customers in an acceptable amount of time. The services and resources facilitating this should be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services.

Business continuity plans should address organizational vulnerabilities and therefore may contain sensitive information that needs to be appropriately protected. Copies of business continuity plans should be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Management should ensure copies of the business continuity plans are up-to-date and protected with the same level of security as applied at the main site. Other material necessary to execute the continuity plans should also be stored at the remote location.

If alternative temporary locations are used, the level of implemented security controls at these locations should be equivalent to the main site.

Other information

It should be noted that crisis management plans and activities (see 14.1.3 f)) may be different from business continuity management; i.e. a crisis may occur that can be accommodated by normal management procedures.

14.1.4 Business continuity planning framework

Control

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

Implementation guidance

Each business continuity plan should describe the approach for continuity, for example the approach to ensure information or information system availability and security. Each plan should also specify the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures, e.g. evacuation plans or fallback arrangements, should be amended as appropriate. Procedures should be included within the organization's change management programme to ensure that business continuity matters are always addressed appropriately.

Each plan should have a specific owner. Emergency procedures, manual fallback plans, and resumption plans should be within the responsibility of the owners of the appropriate business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, should usually be the responsibility of the service providers.

A business continuity planning framework should address the identified information security requirements and consider the following:

a) the conditions for activating the plans which describe the process to be followed (e.g. how to assess the situation, who is to be involved) before each plan is activated;

© ISO/IEC 2005 – All rights reserved

b) emergency procedures, which describe the actions to be taken following an incident, which jeopardizes business operations;

c) fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales;

d) temporary operational procedures to follow pending completion of recovery and restoration;

e) resumption procedures which describe the actions to be taken to return to normal business operations;

f) a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan;

g) awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective;

h) the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required;

i) the critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

14.1.5 Testing, maintaining and re-assessing business continuity plans

Control

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

Implementation guidance

Business continuity plan tests should ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) should indicate how and when each element of the plan should be tested. Each element of the plan(s) should be tested frequently.

A variety of techniques should be used in order to provide assurance that the plan(s) will operate in real life. These should include:

a) table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);

b) simulations (particularly for training people in their post-incident/crisis management roles);

c) technical recovery testing (ensuring information systems can be restored effectively);

d) testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);

e) tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);

f) complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions).

© ISO/IEC 2005 – All rights reserved

These techniques can be used by any organization. They should be applied in a way that is relevant to the specific recovery plan. The results of tests should be recorded and actions taken to improve the plans, where necessary.

Responsibility should be assigned for regular reviews of each business continuity plan. The identification of changes in business arrangements not yet reflected in the business continuity plans should be followed by an appropriate update of the plan. This formal change control process should ensure that the updated plans are distributed and reinforced by regular reviews of the complete plan.

Examples of changes where updating of business continuity plans should be considered are acquisition of new equipment, upgrading of systems and changes in:

a) personnel;

b) addresses or telephone numbers;

c) business strategy;

d) location, facilities, and resources;

e) legislation;

f) contractors, suppliers, and key customers;

g) processes, or new or withdrawn ones;

h) risk (operational and financial).

© ISO/IEC 2005 – All rights reserved

15 Compliance

15.1 Compliance with legal requirements

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

The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.

Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

15.1.1 Identification of applicable legislation

Control

All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.

Implementation guidance

The specific controls and individual responsibilities to meet these requirements should be similarly defined and documented.

15.1.2 Intellectual property rights (IPR)

Control

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

Implementation guidance

The following guidelines should be considered to protect any material that may be considered intellectual property:

a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;

b) acquiring software only through known and reputable sources, to ensure that copyright is not violated;

c) maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against personnel breaching them;

d) maintaining appropriate asset registers, and identifying all assets with requirements to protect intellectual property rights;

e) maintaining proof and evidence of ownership of licenses, master disks, manuals, etc;

f) implementing controls to ensure that any maximum number of users permitted is not exceeded;

g) carrying out checks that only authorized software and licensed products are installed;

h) providing a policy for maintaining appropriate licence conditions;

i) providing a policy for disposing or transferring software to others;

© ISO/IEC 2005 – All rights reserved

j) using appropriate audit tools;

k) complying with terms and conditions for software and information obtained from public networks;

l) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law;

m) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Other information

Intellectual property rights include software or document copyright, design rights, trademarks, patents, and source code licenses.

Proprietary software products are usually supplied under a license agreement that specifies license terms and conditions, for example, limiting the use of the products to specified machines or limiting copying to the creation of back-up copies only. The IPR situation of software developed by the organization requires to be clarified with the staff.

Legislative, regulatory, and contractual requirements may place restrictions on the copying of proprietary material. In particular, they may require that only material that is developed by the organization, or that is licensed or provided by the developer to the organization, can be used. Copyright infringement can lead to legal action, which may involve criminal proceedings.

15.1.3 Protection of organizational records

Control

Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

Implementation guidance

Records should be categorized into record types, e.g. accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures (see 12.3), should also be stored to enable decryption of the records for the length of time the records are retained.

Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with manufacturer's recommendations. For long term storage, the use of paper and microfiche should be considered.

Where electronic storage media are chosen, procedures to ensure the ability to access data (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure clear identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these record safeguarding objectives, the following steps should be taken within an organization:

a) guidelines should be issued on the retention, storage, handling, and disposal of records and information;

© ISO/IEC 2005 – All rights reserved

b) a retention schedule should be drawn up identifying records and the period of time for which they should be retained;

c) an inventory of sources of key information should be maintained;

d) appropriate controls should be implemented to protect records and information from loss, destruction, and falsification;

Other information

Some records may need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organization operates within statutory or regulatory rules, to ensure adequate defense against potential civil or criminal action, or to confirm the financial status of an organization with respect to shareholders, external parties, and auditors. The time period and data content for information retention may be set by national law or regulation.

Further information about managing organizational records can be found in ISO 15489-1.

15.1.4 Data protection and privacy of personal information

Control

Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

Implementation guidance

An organizational data protection and privacy policy should be developed and implemented. This policy should be communicated to all persons involved in the processing of personal information.

Compliance with this policy and all relevant data protection legislation and regulations requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a data protection officer, who should provide guidance to managers, users, and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personal information and ensuring awareness of the data protection principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personal information should be implemented.

Other information

A number of countries have introduced legislation placing controls on the collection, processing, and transmission of personal data (generally information on living individuals who can be identified from that information). Depending on the respective national legislation, such controls may impose duties on those collecting, processing, and disseminating personal information, and may restrict the ability to transfer that data to other countries.

15.1.5 Prevention of misuse of information processing facilities

Control

Users should be deterred from using information processing facilities for unauthorized purposes.

Implementation guidance

Management should approve the use of information processing facilities. Any use of these facilities for non-business purposes without management approval (see 6.1.4), or for any unauthorized purposes, should be regarded as improper use of the facilities. If any unauthorized activity is identified by monitoring or other means, this activity should be brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

Legal advice should be taken before implementing monitoring procedures.

© ISO/IEC 2005 – All rights reserved

All users should be aware of the precise scope of their permitted access and of the monitoring in place to detect unauthorized use. This can be achieved by giving users written authorization, a copy of which should be signed by the user and securely retained by the organization. Employees of an organization, contractors, and third party users should be advised that no access will be permitted except that which is authorized.

At log-on, a warning message should be presented to indicate that the information processing facility being entered is owned by the organization and that unauthorized access is not permitted. The user has to acknowledge and react appropriately to the message on the screen to continue with the log-on process (see 11.5.1).

Other information
The information processing facilities of an organization are intended primarily or exclusively for business purposes.

Intrusion detection, content inspection, and other monitoring tools may help prevent and detect misuse of information processing facilities.

Many countries have legislation to protect against computer misuse. It may be a criminal offence to use a computer for unauthorized purposes.

The legality of monitoring the usage varies from country to country and may require management to advise all users of such monitoring and/or to obtain their agreement. Where the system being entered is used for public access (e.g., a public web server) and is subject to security monitoring, a message should be displayed saying so.

15.1.6 Regulation of cryptographic controls

Control
Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

Implementation guidance
The following items should be considered for compliance with the relevant agreements, laws, and regulations:

a) restrictions on import and/or export of computer hardware and software for performing cryptographic functions;

b) restrictions on import and/or export of computer hardware and software which is designed to have cryptographic functions added to it;

c) restrictions on the usage of encryption;

d) mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.

Legal advice should be sought to ensure compliance with national laws and regulations. Before encrypted information or cryptographic controls are moved to another country, legal advice should also be taken.

15.2 Compliance with security policies and standards and technical compliance

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

The security of information systems should be regularly reviewed.
Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

© ISO/IEC 2005 – All rights reserved

15.2.1 Compliance with security policies and standards

Control

Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

Implementation guidance

Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

If any non-compliance is found as a result of the review, managers should:

a) determine the causes of the non-compliance;

b) evaluate the need for actions to ensure that non-compliance do not recur;

c) determine and implement appropriate corrective action;

d) review the corrective action taken.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out the independent reviews (see 6.1.8), when the independent review takes place in the area of their responsibility.

Other information

Operational monitoring of system use is covered in 10.10.

15.2.2 Technical compliance checking

Control

Information systems should be regularly checked for compliance with security implementation standards.

Implementation guidance

Technical compliance checking should be performed either manually (supported by appropriate software tools, if necessary) by an experienced system engineer, and/or with the assistance of automated tools, which generate a technical report for subsequent interpretation by a technical specialist.

If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.

Any technical compliance check should only be carried out by competent, authorized persons, or under the supervision of such persons.

Other information

Technical compliance checking involves the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance checking requires specialist technical expertise.

© ISO/IEC 2005 – All rights reserved

Compliance checking also covers, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for checking how effective the controls are in preventing unauthorized access due to these vulnerabilities.

Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s). Penetration testing and vulnerability assessments are not a substitute for risk assessment.

15.3 Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.
There should be controls to safeguard operational systems and audit tools during information systems audits.
Protection is also required to safeguard the integrity and prevent misuse of audit tools.

15.3.1 Information systems audit controls

Control

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.

Implementation guidance

The following guidelines should be observed:

a) audit requirements should be agreed with appropriate management;

b) the scope of the checks should be agreed and controlled;

c) the checks should be limited to read-only access to software and data;

d) access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements;

e) resources for performing the checks should be explicitly identified and made available;

f) requirements for special or additional processing should be identified and agreed;

g) all access should be monitored and logged to produce a reference trail; the use of time-stamped reference trails should be considered for critical data or systems;

h) all procedures, requirements, and responsibilities should be documented;

i) the person(s) carrying out the audit should be independent of the activities audited.

15.3.2 Protection of information systems audit tools

Control

Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

Implementation guidance

Information systems audit tools, e.g. software or data files, should be separated from development and operational systems and not held in tape libraries or user areas, unless given an appropriate level of additional protection.

© ISO/IEC 2005 – All rights reserved

Other information

If third parties are involved in an audit, there might be a risk of misuse of audit tools by these third parties, and information being accessed by this third party organization. Controls such as 6.2.1 (to assess the risks) and 9.1.2 (to restrict physical access) can be considered to address this risk, and any consequences, such as immediately changing passwords disclosed to the auditors, should be taken.

© ISO/IEC 2005 – All rights reserved

Bibliography

ISO/IEC Guide 2:1996, Standardization and related activities – General vocabulary

ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards

ISO/IEC 13335-1:2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management

ISO/IEC TR 13335-3:1998, Information technology – Guidelines for the Management of IT Security – Part 3: Techniques for the management of IT Security

ISO/IEC 13888-1: 1997, Information technology – Security techniques – Non-repudiation – Part 1: General

ISO/IEC 11770-1:1996 Information technology – Security techniques – Key management – Part 1: Framework

ISO/IEC 9796-2:2002 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

ISO/IEC 9796-3:2000 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

ISO/IEC 14888-1:1998 Information technology – Security techniques – Digital signatures with appendix – Part 1: General

ISO/IEC 15408-1:1999 Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model

ISO/IEC 14516:2002 Information technology – Security techniques – Guidelines for the use and management of Trusted Third Party services

ISO 15489-1:2001 Information and documentation – Records management – Part 1: General

ISO 10007:2003 Quality management systems – Guidelines for configuration management

ISO/IEC 12207:1995 Information technology – Software life cycle processes

ISO 19011:2002 Guidelines for quality and /or environmental management systems auditing

OECD Guidelines for the Security of Information Systems and Networks: 'Towards a Culture of Security', 2002

OECD Guidelines for Cryptography Policy, 1997

IEEE P1363-2000: Standard Specifications for Public-Key Cryptography

ISO/IEC 18028-4 Information technology – Security techniques – IT Network security – Part 4: Securing remote access

ISO/IEC TR 18044 Information technology – Security techniques – Information security incident management

© ISO/IEC 2005 – All rights reserved

Index

A

access control 11
- for application systems 11.6
- business requirements for 11.1
- for information 11.6, 11.6.1
- for networks 11.4
- for operating systems 11.5
- policy for 11.1.1
- to program source code 12.4.3

access rights
- removal of 8.3.3
- review of 11.2.4

acceptable use of assets 7.1.3
accountability 2.5
acquisition, development and maintenance of information systems 12
agreements
- addressing security in third party 6.2.3
- for exchange 10.8.2

allocation of information security responsibilities 6.1.3
application
- system access control 11.6
- correct processing in applications 12.2
- review of, after operating system changes 12.5.2

asset 2.1
- acceptable use of 7.1.3
- inventory of 7.1.1
- management 7
- ownership of 7.1.2
- responsibility for 7.1
- return of 8.3.2

audit
- considerations for information systems 15.3
- controls for information systems 15.3.1
- logging 10.10.1
- tools, protection of 12.3.2

authentication
- of users 11.5.2
- of users for external connections 11.4.3

authenticity 2.5
authorities, contact with 6.1.6
authorization process 6.1.4
availability 2.5
awareness, education and training in information security 8.2.2

B

back-up 10.5
- of information 10.5.1

business continuity 14
- management of 14
- management of information security aspects of 14.1
- management process to include information security in 14.1.1
- planning, framework for 14.1.4
- plans, development and implementation 14.1.3
- and risk assessment 14.1.2
- testing, maintaining and re-assessing plans for 14.1.5

business information systems 10.8.5

© ISO/IEC 2005 – All rights reserved

C
cabling security 9.2.3
capacity management 10.3.1
change
control, procedures for 12.5.1
of employment 8.3
management 10.2.1
of operating systems, review of 12.5.2
restriction of changes to software packages 12.5.3
changes to third party services, management of 10.2.3
classification
guidelines 7.2.1
of information 7.2
clear desk and clear screen policy 11.3.3
clock synchronization 10.10.6
collection of evidence 13.2.3
communications and operations management 10
compliance 15
with legal requirements 15.1
with security policies and standards 15.2, 15.2.1
technical compliance checking15.2.2
confidentiality 2.5
confidentiality agreements 6.1.5
configuration port protection, remote 11.4.4
connection control of networks 11.4.6
connection time, limitation of 11.5.6
contact
with authorities 6.1.6
with specialist interest groups 6.1.7
control 2.2, 3.2
against malicious code 10.4.1
against mobile code 10.4.2
of internal processing 12.2.2
of operational software 12.4.1
copyright
IPR 15.1.2
software 15.1.2
correct processing in applications 12.2
cryptographic controls 12.3
policy on the use of 12.3.1
regulation of 15.1.6
customers, addressing security when dealing with 6.2.2

D
data protection and privacy of personal information 15.1.4
delivery area 9.1.6
development
and acquisition and maintenance of information systems 12
and test and operational facilities, separation of 8.1.5
of software, outsourced 12.5.5
and support processes, security in 12.5
diagnostic port protection, remote 11.4.4
disciplinary process 8.2.3
disposal
of equipment 9.2.6
of media 10.7.2
documentation, security of system 10.7.4
documented operating procedures 10.1.1
during employment 8.2
duties, segregation of 10.1.3

© ISO/IEC 2005 – All rights reserved

E
education, awareness and training in information security 8.2.2
electronic
commerce 10.9.1
commerce services 10.9
messaging 10.8.4
employment
during 8.2
prior to 8.1
termination or change of 8.3
entry controls 9.1.2
environmental and external threats 9.1.4
environmental and physical security 9
equipment
identification in networks 11.4.3
maintenance 9.2.4
security 9.2
security off-premises 9.2.5
secure disposal or re-use of 9.2.6
siting and protection of 9.2.1
unattended 11.3.2
evidence, collection of 13.2.3
exchange
agreements 10.8.2
of information 10.8
of information, policies and procedures for 10.8.1
external parties 6.2
identification of risks related to 6.2.1
external and environmental threats 9.1.4

F
fault logging 10.10.5
framework for business continuity plans 14.1.4

G
guideline 2.3

H
human resources security 8
home working
security of equipment 9.2.5
security of teleworking 11.7.2

I
identification of applicable legislation 15.1.1
identification
of equipment in networks 11.4.3
of users 11.5.2
independent review of information security 6.1.8
information
access, restrictions on 11.6.1
back-up of 10.5.1
classification 7.2
exchange of 10.8
exchange of, policies and procedures for 10.8.1
handling procedures for 10.7.3
labeling and handling 7.2.2
leakage 12.5.4
made publicly available 10.9.3

© ISO/IEC 2005 – All rights reserved

processing facilities 2.4
processing facilities and misuse of them 15.1.5
system acquisition, development and maintenance 12
system audit controls 15.3.1
system audit tools, protection of 15.3.2
systems for business 10.8.5
information security 2.5
awareness, education and training in 8.2.2
co-ordination of 6.1.2
event 2.6, 13.1
event, reporting of 13.1.1
incident 2.7, 13.2
incident, learning from 13.2.2
inclusion in the business continuity management process 14.1.1
inclusion in the development and implementation of business continuity plans 14.1.3
organizing 6
policy for 5.1
policy document for 5.1.1
input data validation 12.2.1
integrity 2.5
of messages 12.2.3
intellectual property rights 15.1.2
internal organization 6.1
internal processing, control of 12.2.2
inventory of assets 7.1.1
implementation guidance 3.2
isolation of sensitive systems 11.6.2

K
key management 12.3.2

L
labeling and handling of information 7.2.2
leakage of information 12.5.4
learning from information security incidents 13.2.2
legal requirements, compliance with 15.1
legislation, identification of applicable 15.1.1
limitation of connection time11.5.6
loading area 9.1.6
logs
administrator and operator logs 10.10.4
audit logging 10.10.1
fault logging 10.10.5
protection of log information 10.10.3
log-on procedures 11.5.1

M
maintenance
of equipment 9.2.4
and acquisition and development of information systems 12
malicious code
controls against 10.4.1
protection against 10.4
management
of assets 7
of business continuity 14
of capacity 10.3.1
of changes 10.1.2
of changes to third party services 10.2.3
commitment to information security 6.1.1

© ISO/IEC 2005 – All rights reserved

of communications and operations 10
of cryptographic keys 12.3.2
of information security aspects of business continuity 14.1
of information security incidents 13, 13.2
of network security 10.6
of privileges 11.2.2
of removable computer media 10.7.1
responsibilities 8.2.1
system for passwords 11.5.3
of technical vulnerabilities 12.6
of user access 11.2
of user passwords 11.2.3
media
disposal of 10.7.2
handling 10.7
in transit 10.8.3
removable10.7.1
message integrity 12.2.3
messaging, electronic 10.8.4
misuse of information processing facilities, prevention of 15.1.5
mobile code
controls against 10.4.2
protection against 10.4
mobile computing 11.7
mobile computing and communications 11.7.1
monitoring 10.10
and review, of third party services 10.2.2
system use 10.10.2

N
network
access control of 11.4
connection control of 11.4.6
controls 10.6.1
equipment identification in 11.4.3
routing control of 11.4.7
security, management of 10.6
segregation in 11.4.5
services, policy on their use 11.4.1
services, security of 10.6.2
non-repudiation 2.5
services 12.3.1

O
offices, rooms and facilities, securing 9.1.3
on-line transactions 10.9.2
operating
procedures, documented 10.1.1
system access control 11.5
system changes, technical review of 12.5.2
operational
procedures and responsibilities 10.1
software, control of 12.4.1
operations and communications management 10
operator logs 10.10.4
organizational records, protection of 15.1.3
other information 3.2
output data validation 12.2.4
outsourced software development 12.5.5
ownership of assets 7.1.2

© ISO/IEC 2005 – All rights reserved

P
passwords
management of, user 11.2.3
management system for 11.5.3
use of 11.3.1
personal information, privacy of 15.1.4
physical
and environmental security 9
entry controls 9.1.2
media in transit 10.8.3
security perimeter 9.1.1
plans for business continuity
developing and implementing them 14.1.3
testing, maintaining and re-assessing them 14.1.5
policy 2.8
on access control 11.1
on clear desk and clear screen 11.3.2
on information exchange 10.8.1
on information security 5.1
on the use of cryptographic controls 12.3.1
on use of network services 11.4.1
security 5
prevention of misuse of information processing facilities 15.1.5
prior to employment 8.1
privilege management 11.2.2
procedures
on change control 12.5.1
on information exchange 10.8.1
for information handling 10.7.3
for log-on 11.5.3
operational 10.1, 10.1.1
and responsibilities for incident management 13.2.1
program source code, access control to 12.4.3
property, removal of 9.2.7
property rights, intellectual 15.1.2
protection
of log information 10.10.3
against malicious and mobile code 10.4
of organizational records 14.1.3
of information system audit tools 15.3.2
of system test data 12.4.2
public access, delivery and loading area 9.1.6
publicly available information 10.9.3

R
regulation of cryptographic controls 15.1.6
reliability 2.5
remote diagnostic and configuration port protection 11.4.5
removable media, management of 10.7.1
removal
of access rights 8.3.3
of property 9.2.7
reporting
information security events 13.1, 13.1.1
security weaknesses 13.1, 13.1.2
responsibilities
allocation of information security 6.1.3
and roles 8.1.1
for termination 8.3.1

© ISO/IEC 2005 – All rights reserved

of management 8.2.1
operational 10.1
and procedures for incident management 13.2.1
user 11.3
restrictions of changes to software packages 12.5.3
return of assets 8.3.2
re-use of equipment 9.2.6
review
of information security 6.1.8
of information security policy 5.1.2
and monitoring, of third party services
of user access rights 11.2.4
risk 2.9
analysis 2.10
assessment 2.11, 4.1
assessment and business continuity 14.1.2
evaluation 2.12
management 2.13
treatment 2.14, 4.2
risks related to external parties 6.2.1
roles and responsibilities 8.1.1
rooms, offices and facilities, securing 9.1.3
routing control in networks 11.4.7

S
screening 8.1.2
secure areas 9.1
working in 9.1.5
securing offices, rooms and facilities 9.1.3
security
in development and support processes 12.5
of human resources 8
of equipment 9.2
of equipment off-premises 9.2.5
of network services 10.6.2
policy 5
policy, compliance with 15.2.1
requirements analysis and specification 12.1.1
of system documentation 10.7.4
of system files 12.4
weaknesses, reporting of 13.1.2
segregation of duties 10.1.3
in networks 11.4.5
sensitive system isolation 11.6.2
separation of development, test and operational facilities 10.1.4
service delivery 10.2.1
management, of third parties 10.2
services, for electronic commerce 10.9
session time-out 11.5.5
siting of equipment 9.2.1
software
development, outsourced 12.5.5
operational, control of 12.4.1
packages, restrictions on changes 12.5.3
source code, access control to 12.4.3
standards and security policies, compliance with 15.2, 15.2.1
support and development processes, security in 12.5
system
acceptance 10.3.2
acquisition, development and maintenance 12

© ISO/IEC 2005 – All rights reserved

audit considerations 15.3
audit controls 15.3.1
audit tools, protection of 15.3.2
documentation, security of 10.7.4
files, security of 12.4
planning and acceptance 10.3
sensitive, isolation of 11.6.2
test data, protection of 12.4.2
use, monitoring of 10.10.2
utilities, use of 11.5.4

T
technical
compliance checking 15.2.2
review of applications after operating system changes 10.5.2
vulnerabilities, control of 12.6.1
vulnerability management 12.6
teleworking 11.7, 11.7.2
termination of employment 8.3
termination responsibilities 8.3.1
terms and conditions of employment 8.1.3
test
data, protection of 12.4.2
and development and operational facilities, separation of 10.1.4
testing, maintaining and re-assessing business continuity plans 11.1.5.
third party 2.15
addressing security in agreements 6.2.3
service delivery management 10.2
services, managing changes to 10.2.3
services, monitoring and review 10.2.2
threat 2.16
training, awareness and education in information security 8.2.2
transactions, on-line 10.9.2

U
unattended user equipment 11.3.2
user
access management 11.2
access rights, review of 11.2.4
authentication for external connections 11.4.2
identification and authentication 11.5.2
password management 11.2.3
registration 11.2.1
responsibilities 11.3
unattended user equipment 11.3.2
utilities
supporting 9.2.2
system 11.5.4

V
validation
of input data 12.2.1
of output data 12.2.3
virus protection 10.4
vulnerability 2.17
technical vulnerability management 12.6
control of technical vulnerabilities 12.6.1

W
working in secure areas 9.1.5

© ISO/IEC 2005 – All rights reserved

ICS 35.040

Price based on 115 pages

© ISO/IEC 2005 – All rights reserved