INTERNATIONAL STANDARD

ISO/IEC 27011

First edition
2008-12-15

Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

Technologies de l'information — Techniques de sécurité — Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002

Reference number
ISO/IEC 27011:2008(E)

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

Published by ISO in 2009

Published in Switzerland

CONTENTS

		Page
1	Scope	1
2	Normative references	1
3	Definitions and abbreviations	1
3.1	Definitions	1
3.2	Abbreviations	2
4	Overview	3
4.1	Structure of this guideline	3
4.2	Information security management systems in telecommunications business	3
5	Security policy	5
6	Organization of information security	5
6.1	Internal organization	5
6.2	External parties	7
7	Asset management	10
7.1	Responsibility for assets	10
7.2	Information classification	12
8	Human resources security	13
8.1	Prior to employment	13
8.2	During employment	15
8.3	Termination or change of employment	15
9	Physical and environmental security	15
9.1	Secure areas	15
9.2	Equipment security	17
10	Communications and operations management	19
10.1	Operational procedures and responsibilities	19
10.2	Third party service delivery management	21
10.3	System planning and acceptance	21
10.4	Protection against malicious and mobile code	22
10.5	Back-up	22
10.6	Network security management	22
10.7	Media handling	23
10.8	Exchange of information	23
10.9	Electronic commerce services	23
10.10	Monitoring	23
11	Access control	25
11.1	Business requirement for access control	25
11.2	User access management	26
11.3	User responsibilities	26
11.4	Network access control	26
11.5	Operating system access control	26
11.6	Application and information access control	26
11.7	Mobile computing and teleworking	26
12	Information systems acquisition, development and maintenance	26
12.1	Security requirements of information systems	26
12.2	Correct processing in applications	26
12.3	Cryptographic controls	26
12.4	Security of system files	26
12.5	Security in development and support processes	27
12.6	Technical vulnerability management	27
13	Information security incident management	28
13.1	Reporting information security events and weaknesses	28
13.2	Management of information security incidents and improvements	29

Page

14 Business continuity management 31
14.1 Information security aspects of business continuity management 31
15 Compliance 33
Annex A – Telecommunications extended control set 34
A.9 Physical and environmental security 34
A.10 Communications and operations management 37
A.11 Access control 39
A.15 Compliance 39
Annex B – Additional implementation guidance 42
B.1 Network security measures against cyber attacks 42
B.2 Network security measures for network congestion 42
Bibliography 44

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 27011 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques* in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.1051 (02/2008).

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security management in telecommunications organizations based on ISO/IEC 27002 (Code of practice for information security management). In addition to the application of security objectives and controls described in ISO/IEC 27002, telecommunications organizations have to take into account the following security features:

1) *Confidentiality*

   Information related to telecommunications organizations should be protected from unauthorized disclosure.

   This implies non-disclosure of communications in terms of the existence, the content, the source, the destination and the date and time of communicated information.

   It is critical that telecommunications organizations ensure that the non-disclosure of communications being handled by them is not breached. Persons engaged by the telecommunications organization should maintain the confidentiality of any information regarding others that may have come to be known during their work duties.

   NOTE – The term "secrecy of communications" is used in some countries in the context of "non-disclosure of communications".

2) *Integrity*

   The installation and use of telecommunications facilities should be controlled, ensuring the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other methods.

3) *Availability*

   Only authorized access should be provided when necessary to telecommunications information, facilities and the medium used for the provision of communication services whether it might be provided by wire, radio or any other methods. As an extension of the availability, telecommunications organizations should give priority to essential communications in case of emergency, and comply with regulatory requirements.

Information security management in telecommunications organizations is required regardless of the method, e.g., wired, wireless or broadband technologies. If information security management is not implemented properly, the extent of telecommunications risks regarding confidentiality, integrity and availability may be increased.

Telecommunications organizations are designated to provide telecommunications services by intermediating communications of others through facilities for the use of others communications. Therefore, it should be taken into account that information processing facilities within a telecommunication organization are accessed and utilized by not only its own employees and contractors, but also various users outside of the organization.

In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their telecommunications services and facilities, and/or use the telecommunications services and facilities of other telecommunications organizations. Therefore, the management of information security in telecommunications organizations is mutually dependent and may include any and all areas of network infrastructure, services applications and other facilities.

Regardless of operational scales, service areas or service types, telecommunications organizations should implement appropriate controls to ensure confidentiality, integrity, availability and any other security property of telecommunications.

Audience

This Recommendation | International Standard provides telecommunications organizations, and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers, with a common set of general security control objectives based on ISO/IEC 27002, telecommunications sector specific controls, and information security management guidelines allowing for the selection and implementation of such controls.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

1 Scope

The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security management in telecommunications organizations.

The adoption of this Recommendation | International Standard will allow telecommunications organizations to meet baseline information security management requirements of confidentiality, integrity, availability and any other relevant security property.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

- ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*
- ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management.*

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation | International Standard, the definitions given in ISO/IEC 27002 apply. Additionally, the following definitions apply:

3.1.1 collocation: Installation of telecommunications facilities on the premises of other telecommunications carriers.

3.1.2 communication centre: Building where facilities for providing telecommunications business are sited.

3.1.3 essential communications: Communications whose contents are necessary for the prevention of or relief from calamities, for maintaining transportation, communications or electric power supply, or for the maintenance of public order.

3.1.4 non-disclosure of communications: Properties of communications being handled by the persons engaged in the telecommunications organization should not be disclosed in terms of the existence, the content, the source, the destination and the date and time of communicated information.

3.1.5 personal information: Information about an individual which can be used to identify that individual. The specific information used for this identification will be that defined by national legislation.

3.1.6 priority call: Telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls. The specific terminals may span different services (VoIP, PSTN voice, IP data traffic, etc.) for wired and wireless networks.

3.1.7 telecommunications applications: Applications such as e-mail that are accessed by end-users and are built upon the network-based services.

3.1.8 telecommunications business: Business to provide telecommunications services in order to meet the demand of others.

3.1.9 telecommunications equipment room: A part of general building such as a room where equipment for providing telecommunications business are sited.

3.1.10 telecommunications facilities: Machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications.

3.1.11 telecommunications organizations: Business entities who provide telecommunications services in order to meet the demand of others.

3.1.12 telecommunication records: Information concerning the parties in a communication excluding the contents of the communication, and the time, and duration of the telecommunication took place.

3.1.13 telecommunications services: Communications using telecommunications facilities, or any other means of providing communications either between telecommunications service users or telecommunications service customers.

3.1.14 telecommunications service customer: Person or organization who enters into a contract with telecommunications organizations to be offered telecommunications services by them.

3.1.15 telecommunications service user: Person or organization who utilizes telecommunications services.

3.1.16 terminal facilities: Telecommunications facilities which are to be connected to one end of telecommunications circuit facilities and part of which is to be installed on the same premises (including the areas regarded as the same premises) or in the same building where any other part thereof is also to be installed.

3.1.17 user: Person or organization who utilizes information processing facilities or systems, e.g., employee, contractor or third party user.

3.2 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ADSL	Asymmetric Digital Subscriber Line
ASP	Application Service Provider
CATV	Community Antenna TeleVision
CERT	Computer Emergency Response Team
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
NGN	Next Generation Network
NMS	Network Management System
OAM&P	Operations, Administration, Maintenance and Provisioning
PIN	Personal Identification Number
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SOA	Statement of Applicability
UPS	Uninterruptible Power Supply
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol

4 Overview

4.1 Structure of this guideline

This Recommendation | International Standard has been structured in a format similar to ISO/IEC 27002. In cases where objectives and controls specified in ISO/IEC 27002 are applicable without a need for any additional information, only a reference is provided to ISO/IEC 27002. Telecommunications sector specific set of control and implementation guidance is described in Annex A (normative).

In cases where controls need additional guidance specific to telecommunications, the ISO/IEC 27002 control and implementation guidance is repeated without modification, followed by the specific telecommunications guidance related to this control. Telecommunications sector specific guidance and information is included in the following clauses:

- Organization of information security (clause 6)
- Asset management (clause 7)
- Human resources security (clause 8)
- Physical and environmental security (clause 9)
- Communications and operations management (clause 10)
- Access control (clause 11)
- Information systems acquisition, development and maintenance (clause 12)
- Information security incident management (clause 13)
- Business continuity management (clause 14)

4.2 Information security management systems in telecommunications business

4.2.1 Goal

Information, like other organization assets, is an essential contributor to an organization's business. Information can be printed or written on paper, stored electronically, transmitted by post, communicated electronically, shown on films, or spoken in conversation. Regardless of the form or functionality of the information, or the means by which the information is shared or stored, information should always be appropriately protected.

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, information leakage, earthquake, fire or flood. These security threats may originate from inside or outside the telecommunications organization resulting in damage to the organization.

Once information security is violated, for example by unauthorized access to an organization's information processing system, the organization may suffer damage. Therefore, it is essential for an organization to ensure its information security by continuously improving its ISMS in accordance with ISO/IEC 27001.

Effective information security is achieved by implementing a suitable set of controls based on those described in this Recommendation | International Standard. These controls need to be established, implemented, monitored, reviewed and improved in the telecommunications facilities, services and applications. The successful deployment of security controls will better enable meeting the security and business objectives of the organization to be met.

Telecommunications organizations whose facilities are used by various users to process information such as personal data, confidential data and business data should handle this information with great/due care and apply an appropriate level of protection.

In conclusion, telecommunications organizations need to establish and continuously improve an overall ISMS which ensures appropriate security controls are maintained.

4.2.2 Security considerations in telecommunications

The requirement for a generic security framework in telecommunications has originated from different sources:

a) Customers/subscribers needing confidence in the network and the services to be provided, including availability of services (especially emergency services) in case of major catastrophes;

b) Public authorities demanding security by directives, regulation and legislation, in order to ensure availability of services, fair competition and privacy protection;

c) Network operators and service providers themselves needing security to safeguard their operational and business interests, and to meet their obligations to their customers and the public.

Furthermore, telecommunications organizations should consider the following environmental and operational security incidents:

a) Telecommunications services are heavily dependent on various interconnected facilities, such as routers, switches, domain name servers, transmission relay systems and NMS. Therefore, telecommunications security incidents can occur to various equipment/facilities and the incidents can propagate rapidly through network into other equipment/facilities;

b) In addition to telecommunications facilities, vulnerabilities in network protocols and topology can result in serious security incidents. Especially, convergence of wired and wireless networks into NGN can impose significant challenges for developing interoperable protocols;

c) A major concern of telecommunications organizations is the possibility of compromised security that causes network down-time. Such down-time can be extremely costly in terms of customer relations, lost revenue, and recovery costs. Deliberate attacks on the availability of the national telecommunications infrastructure can be viewed as a national security concern;

d) Telecommunications management networks and systems are susceptible to hacker penetrations. A common motivation for such penetrations is theft of telecommunications services. Such theft can be engineered in various ways, such as invoking diagnostic functions, manipulating accounting records, and altering provisioning databases, and eavesdropping on subscriber calls;

e) In addition to external penetrations, carriers are concerned about security compromises from internal sources, such as invalid changes to network management databases and configurations on the part of unauthorized personnel. Such occurrences may be accidental or deliberate.

For the purpose of protecting information assets in telecommunications originating from different sources under the various telecommunications environments, security guidelines for telecommunications are indispensable to support the implementation of information security management in telecommunications organizations.

The security guidelines should be applicable to the following:

a) Telecommunications organizations seeking a business advantage through the implementation of an information security management system;

b) Telecommunications organizations seeking confidence that the information security requirements of their interested parties (e.g., suppliers, customers, regulators) will be satisfied;

c) Users and suppliers of the information security related products and services for the telecommunications industry;

d) Those internal or external to the telecommunications organization who assess and audit the information security management system for conformity with the requirements of ISO/IEC 27001;

e) Those internal or external to the telecommunications organizations who give advice or training on the information security management system appropriate to that organization.

4.2.3 Information assets to be protected

In order to establish information security management, it is essential for an organization to clarify and identify all organizational assets. The clarification of attributes and importance of the assets makes it possible to implement appropriate controls.

Information assets which telecommunications organizations should protect can be found in 7.1.1, Inventory of assets.

4.2.4 Establishment of information security management

4.2.4.1 How to establish security requirements

It is essential for telecommunications organizations to identify their security requirements. There are three main sources of security requirements as follows:

a) What is derived from assessing risks to a telecommunications carrier, taking into account its overall business strategy and objectives. Through risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated;

b) The legal, statutory, regulatory, and contractual requirements that telecommunications organizations have to satisfy, and the socio-cultural environment. Examples of legislative requirements for telecommunications organizations are non-disclosure of communications (A.15.1.7) and ensuring essential communications (A.15.1.8). Examples of socio-cultural requirements are ensuring the integrity

of telecommunications, transmitted, relayed and received by any means, the availability of wired or wireless telecommunications facilities by authorized persons, and not harming other telecommunications facilities;

c) The particular set of principles, objective and business requirements for information processing that a telecommunications carrier has developed to support its operations.

4.2.4.2 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.

4.2.4.3 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.

This guideline provides additional guidance and telecommunications specific controls, in addition to general information security management, taking account of telecommunications specific requirements. Therefore, telecommunications organizations are recommended to select controls from this guideline and implement them. In addition, 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 telecommunications organizations, and should also be subject to all relevant national and international legislation and regulations.

4.2.4.4 Critical success factors

The contents from ISO/IEC 27002 clause 0.7 apply.

5 Security policy

The control objective and the contents from ISO/IEC 27002 clause 5 apply.

6 Organization of information security

6.1 Internal organization

Objective: To manage information security within the organization.

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

Management should approve the information security policy, assign security roles and coordinate 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 6.1.1 from ISO/IEC 27002 applies.

6.1.2 Information security coordination

Control 6.1.2 from ISO/IEC 27002 applies.

6.1.3 Allocation of information security responsibilities

Control 6.1.3 from ISO/IEC 27002 applies.

6.1.4 Authorization process for information processing facilities

Control 6.1.4 from ISO/IEC 27002 applies.

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;

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;

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 in ISO/IEC 27002).

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

Telecommunications-specific implementation guidance

To identify requirements for confidentiality or non-disclosure agreements, telecommunications organizations should consider the need to protect against non-disclosure of:

a) the existence;

b) the content;

c) the source;

d) the destination; and

e) the date and time;

in communicated information.

Other information

Confidentiality and non-disclosure agreements protect organizational information and inform signatories of their responsibility to protect, use, and disclose information in a responsible and authorized manner.

There may be a need for an organization to use different forms of confidentiality or non-disclosure 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.

Telecommunications-specific implementation guidance

When telecommunications organizations receive inquiries from law-enforcement agencies or investigative organizations, regarding information relating to telecommunications service users, these telecommunications organizations need to confirm that the inquiries have gone through legitimate processes and procedures, according to national laws and regulations.

Other information

Maintaining such contacts may be a requirement to support information security incident management (clause 13.2) or the business continuity and contingency planning process (clause 14). Contacts with regulatory bodies are also useful to anticipate and prepare for upcoming changes in laws or regulations, which have to be followed by the organization. Contacts with other authorities include utilities, emergency services, and health and safety telecommunications providers (in connection with line routing and availability).

6.1.7 Contact with special interest groups

Control 6.1.7 from ISO/IEC 27002 applies.

6.1.8 Independent review of information security

Control 6.1.8 from ISO/IEC 27002 applies.

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 6.2.1 from ISO/IEC 27002 applies.

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;
   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 authorized 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 cooperation with customers in other countries (see also 15.1 in ISO/IEC 27002);
k) intellectual property rights (IPRs) and copyright assignment (see 15.1.2 in ISO/IEC 27002) and protection of any collaborative work (see also 6.1.5).

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the following terms to address security prior to giving customers access to any of the organization's assets:

a) a clear agreement in which telecommunications service facilities or those of other connected telecommunications users connected are not damaged or impaired;
b) a clear demarcation of responsibilities between the telecommunications service facilities of telecommunications organizations and those of telecommunications service users;
c) a clear specification for possible suspension of telecommunications services, in case there may be a risk, for example the threat of spam, hindering the continuous provision of telecommunications services.

Other information

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

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

6.2.3 Addressing security in third-party agreements

Control

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

Implementation guidance

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

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 2.5 in ISO/IEC 27002) 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 authorized 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;

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 cooperation with customers in other countries (see also 15.1 in ISO/IEC 27002);

t) intellectual property rights (IPRs) and copyright assignment (see 15.1.2 in ISO/IEC 27002) 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.

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the following terms for inclusion in the agreement in order to satisfy the identified security requirements:

a) a clear statement regarding protection against damaged or impaired telecommunications service facilities or those of other telecommunications users connected to these facilities in relation to other telecommunications organizations;

b) a clear demarcation of responsibilities between the telecommunications organizations regarding their telecommunication service facilities and those of other organizations.

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.

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 27005).

Telecommunications-specific implementation guidance

When developing and maintaining the inventory of assets, clear responsibilities between the telecommunications facilities of the organization and those of other connected or related telecommunications organizations should be specified and clearly documented.

The list of assets should be comprehensive covering all telecommunications assets of value including information assets for network facilities, network services and applications.

Additional resources can be found in the Bibliography.

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 trials, 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.

Other information for telecommunications

Assets related to telecommunications organizations include many types of assets as follows:

a) information: communication data, routing information, subscriber information, blacklist information, registered service information, operational information, trouble information, configuration information, customer information, billing information, customer calling patterns, customer geographical locations, traffic statistical information, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, emergency plan fallback arrangements, audit trails, and archived information;

b) software assets: communication control software, operation management software, subscriber information management software, billing software, application software, system software, development tools, and utilities;

c) hardware assets: switches, cables, terminal equipment, computer equipment (e.g., server and personal computer/workstation), removable media, and other equipment;

d) services: fixed telephone service, mobile-phone service, optical subscriber line/ADSL service, leased line/data circuit service, internet connection service, data centre service, CATV service, content delivery service, ASP service and customer services including billing service, call centre service;

e) facility and supporting utility system: building, electrical equipment, air-conditioning equipment, fire extinguishing equipment;

f) people: customer service staff, telecommunications engineers, IT support staff and staff for third party service providers;

g) intangibles: organization control, know-how, reputation and image of the organization.

7.1.2 Ownership of assets

Control 7.1.2 from ISO/IEC 27002 applies.

7.1.3 Acceptable use of assets

Control 7.1.3 from ISO/IEC 27002 applies.

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 in ISO/IEC 27002.

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.

Telecommunications-specific implementation guidance

In classifying information, in addition to the general requirements for organizational sensitive and critical information, telecommunications organizations should also take into account the following:

a) the possible need to separately classify the information related to non-disclosure of communications in terms of the existence, the content, the source, the destination and the date and time of communicated information (see A.15.1.7);

b) distinction between the essential communications, which need to be handled with priority in an emergency or at a risk of emergency, and non-essential communications (see A.15.1.8).

Other information

The level of protection can be assessed by analysing 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 labelling and handling

Control 7.2.2 from ISO/IEC 27002 applies.

8 Human resources security

8.1 Prior to employment[1)]

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 in ISO/IEC 27002);

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.

Telecommunications-specific implementation guidance

Telecommunications organizations should appoint telecommunications engineers and other staff, who have the right credentials or appropriate knowledge and skills, to be in charge of the supervision of matters related to the installation, maintenance and operation of telecommunications facilities for the telecommunications business. The relevant telecommunications engineers and other staff should be notified of their assigned roles and responsibilities.

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.

---

1) 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.

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.

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.

Telecommunications-specific implementation guidance

Telecommunications organizations should also consider further more detailed checks for job positions giving staff access to systems critical to providing services, information related to lawful access and lawful interception as well as access, for example to customer information, customer call content.

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 sign a confidentiality or non-disclosure agreement prior to being given access to information processing facilities;

b) the employee's, contractor's and any other user's legal responsibilities and rights, e.g., regarding copyright laws or data protection legislation (see also 15.1.1 and 15.1.2 in ISO/IEC 27002);

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 in ISO/IEC 27002);

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

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 in ISO/IEC 27002);

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 in ISO/IEC 27002);

g) actions to be taken if the employee, contractor or third party user disregards the organization's security requirements (see also 8.2.3 in ISO/IEC 27002).

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).

Telecommunications-specific implementation guidance

The legal rights and responsibilities regarding non-disclosure of communications and essential communications, which telecommunications organizations should take into account, are included in the laws and regulations (see A.15.1.7 and A.15.1.8).

Telecommunications organizations should clarify and state the responsibilities for maintaining the communications service provided by telecommunications organizations in the terms and conditions of employment.

Telecommunications organizations should make sure that any person engaged in the telecommunications services should be aware and kept well informed about keeping other people's secrets which he/she could know through operations for telecommunications services during his/her career and maintaining the confidentiality even after his/her retirement.

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

The control objective and the contents from ISO/IEC 27002 clause 8.2 apply.

8.3 Termination or change of employment

The control objective and the contents from ISO/IEC 27002 clause 8.3 apply.

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 with 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 according to national, regional or international standards and regularly tested to cover all external doors and accessible windows; unoccupied areas should be equipped with alarm systems at all times; cover should also be provided for other areas, e.g., computer rooms or communications rooms;

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

Telecommunications-specific implementation guidance

Telecommunications organizations should consider and implement the following guidelines where appropriate for physical security perimeters:

a) telecommunications operations centres should be equipped with adequate physical intruder detection systems;

b) facilities for telecommunications services, e.g., transmission facilities, switching facilities and telecommunications infrastructure, should be physically separated and sited away from other facilities, e.g., customer facilities in managed data centres;

c) physical barriers should be effectively installed, with all local security policies rigorously enforced to ensure the protection of corporate assets at all times; if a physical barrier is malfunctioning or a policy is not followed, it is imperative that the issue be resolved immediately by management with the appropriate level of responsibility.

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 in ISO/IEC 27002).

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the following guidelines:

a) operation rooms and control centres to operate telecommunications facilities should be protected by adequate strong entry controls;

b) at the front desk, other visitor's information should be protected against unauthorized access or viewing, for example, the date and time of entry and departure record of the visitor; the receptionist should also check the visitor's belongings at the point of entry and departure in order to prevent him/her from bringing dangerous objects into the premises or taking out assets without authorization.

9.1.3 Securing offices, rooms, and facilities

Control 9.1.3 from ISO/IEC 27002 applies.

9.1.4 Protecting against external and environmental threats

Control 9.1.4 from ISO/IEC 27002 applies.

9.1.5 Working in secure areas

Control 9.1.5 from ISO/IEC 27002 applies.

9.1.6 Public access, delivery, and loading areas

Control 9.1.6 from ISO/IEC 27002 applies.

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;

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.

Telecommunications-specific implementation guidance

If the systems of several organizations are sited in the same data centre as telecommunications facilities, the telecommunications organization should implement appropriate measures to protect customers' information stored in their systems. Such systems should be placed physically separate on a site, for example, on a different floor or in a different room.

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.

Telecommunications-specific implementation guidance

In particular, power supply facilities in the isolated area such as mobile base stations should preferably provide an uninterruptible power supply with capacity for all loading and capable of withstanding primary power supply failures for the duration of likely outages. If that is impossible, a mechanism to provide uninterruptible power to critical equipment should be installed. Batteries may need to be augmented with a private electric generator, especially in isolated areas.

Other information

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

Other information for telecommunications

Telecommunications organizations should specify in the agreement that supporting utilities are properly maintained and continually provided in order to ensure the provision of telecommunications services without interruption.

9.2.3 Cabling security

Control 9.2.3 from ISO/IEC 27002 applies.

9.2.4 Equipment maintenance

Control 9.2.4 from ISO/IEC 27002 applies.

9.2.5 Security of equipment off-premises

Control 9.2.5 from ISO/IEC 27002 applies.

9.2.6 Secure disposal or reuse of equipment

Control 9.2.6 from ISO/IEC 27002 applies.

9.2.7 Removal of property

Control 9.2.7 from ISO/IEC 27002 applies.

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, backup, 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) back-up (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 in ISO/IEC 27002);

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 in ISO/IEC 27002);

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.

Telecommunications-specific implementation guidance

In the operating procedures, telecommunications organizations should specify under which conditions the incident, emergency or crisis handling procedures are to be invoked (see 13.2).

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. 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 the relevant information should be retained.

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the procedures and records for installation, relocation and removal of facilities.

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 in ISO/IEC 27002).

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 10.1.3 from ISO/IEC 27002 applies.

10.1.4 Separation of development, test, and operational facilities

Control

Development, test, and operational facilities should be separated to reduce the risks of unauthorized 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.

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).

Telecommunications-specific implementation guidance

In telecommunications organizations, the content of the data used in test and development environments should be adequate to test the system and service in a real telecommunications context. When the test data includes sensitive information (e.g., personal information and telephone records), appropriate controls should be implemented in order to avoid unintended information leakage caused by program bugs or operational errors.

In addition, such test data should be managed appropriately, taking account of data life cycle such as collection of operation data including sensitive information, production of test data from operation data, and destruction of test data after the test.

Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

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

The control objective and the contents from ISO/IEC 27002 clause 10.2 apply.

10.3 System planning and acceptance

The control objective and the contents from ISO/IEC 27002 clause 10.3 apply.

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 10.4.1 from ISO/IEC 27002 applies.

10.4.2 Controls against mobile code

Control

Where the use of mobile code is authorized, the configuration should ensure that the authorized 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;

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 a 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 unauthorized use or disruption of system, network, or application resources and other breaches of information security.

Other information for telecommunications

Some of the examples of mobile code are embedded script, ActiveX® and Java™. Since mobile code is associated with a number of middleware services, controls for middleware may be considered in addition to general controls for malicious code.

10.5 Back-up

The control objective and the contents from ISO/IEC 27002 clause 10.5 apply.

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 data flow, 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 10.6.1 from ISO/IEC 27002 applies.

Further implementation guidance is in Annex B (informative).

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.

Other information for telecommunications

For telecommunications organizations, securing the services that are provided to the users of the network includes the following:

a) securing the OAM&P and configuration of network services;

b) securing the control and signalling information used by the network service (e.g., SIP for VoIP service);

c) securing the end user data and voice as it uses the network service (e.g., VoIP traffic).

10.7 Media handling

The control objective and the contents from ISO/IEC 27002 clause 10.7 apply.

10.8 Exchange of information

The control objective and the contents from ISO/IEC 27002 clause 10.8 apply.

10.9 Electronic commerce services

The control objective and the contents from ISO/IEC 27002 clause 10.9 apply.

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;
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 deactivation of protection systems, such as anti-virus systems and intrusion detection systems.

Telecommunications-specific implementation guidance

Telecommunications organizations should set the appropriate retention time period for retaining data of telecommunications data (e.g., accounting, billing, attending to complaints, and protection of abuse and lawful access by the authorities) and to delete the data at the end of the retention period or at the attainment of the purposes without any delay. This should be done in accordance with any business, legal and regulatory requirements that might apply.

Other information

The audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures should be taken (see also 15.1.4 in ISO/IEC 27002). Where possible, system administrators should not have permission to erase or deactivate logs of their own activities (see 10.1.3).

Other information for telecommunications

Appropriate measures to ensure non-disclosure of communications should be taken (see A.15.1.7).

10.10.2 Monitoring system use

Control 10.10.2 from ISO/IEC 27002 applies.

10.10.3 Protection of log information

Control 10.10.3 from ISO/IEC 27002 applies.

10.10.4 Administrator and operator logs

Control 10.10.4 from ISO/IEC 27002 applies.

10.10.5 Fault logging

Control 10.10.5 from ISO/IEC 27002 applies.

10.10.6 Clock synchronization

Control 10.10.6 from ISO/IEC 27002 applies.

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 clause 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 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 in ISO/IEC 27002);

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 in ISO/IEC 27002);

j) requirements for periodic review of access controls (see 11.2.4 in ISO/IEC 27002);

k) removal of access rights (see 8.3.3 in ISO/IEC 27002).

Telecommunications-specific implementation guidance

Telecommunications organizations should specify appropriate access control rules for equipment sited in user premises. Access should be based on information ownership not physical asset ownership. For example, only the user of telecommunications equipment should have access to the address book stored on a mobile phone but denied access to any system design related information such as terminal ID.

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;

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 in ISO/IEC 27002).

11.2 User access management

The control objective and the contents from ISO/IEC 27002 clause 11.2 apply.

11.3 User responsibilities

The control objective and the contents from ISO/IEC 27002 clause 11.3 apply.

11.4 Network access control

The control objective and the contents from ISO/IEC 27002 clause 11.4 apply.

11.5 Operating system access control

The control objective and the contents from ISO/IEC 27002 clause 11.5 apply.

11.6 Application and information access control

The control objective and the contents from ISO/IEC 27002 clause 11.6 apply.

11.7 Mobile computing and teleworking

The control objective and the contents from ISO/IEC 27002 clause 11.7 apply.

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

The control objective and the contents from ISO/IEC 27002 clause 12.1 apply.

12.2 Correct processing in applications

The control objective and the contents from ISO/IEC 27002 clause 12.2 apply.

12.3 Cryptographic controls

The control objective and the contents from ISO/IEC 27002 clause 12.3 apply.

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 in ISO/IEC 27002).

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.

Telecommunications-specific implementation guidance

Telecommunications organizations should minimize the risk of corruption to operational systems by considering the following guidelines to control changes:

a) If applications and operating system software are to be implemented to sensitive systems such as switching facility, the test should be carried out with a full coverage of path;

b) If application software is sensitive, then at least three generations of software should be retained.

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 12.4.2 from ISO/IEC 27002 applies.

12.4.3 Access control to program source code

Control 12.4.3 from ISO/IEC 27002 applies.

12.5 Security in development and support processes

The control objective and the contents from ISO/IEC 27002 clause 12.5 apply.

12.6 Technical vulnerability management

The control objective and the contents from ISO/IEC 27002 clause 12.6 apply.

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[2)] 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.

Telecommunications-specific implementation guidance

A point of contact trained for assessing, responding to and learning from security incidents should be in place to cooperate with the incident response team. This post may be formed virtually within telecommunications organizations. Such incident response team should be authorized to make immediate decisions on how to deal with an incident. In addition, relationships between the response team and external parties (e.g., CERT, law enforcement organizations, other emergency authorities, customers, and business partners) should be established.

If necessary, telecommunications organizations should promptly report the incidents to the related customers through direct e-mails and/or home-page provided by them.

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;

---

2) A duress alarm is a method for secretly indicating that an action is taking place 'under duress'.

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 in ISO/IEC 27002) 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 behaviour 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 13.1.2 from ISO/IEC 27002 applies.

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.

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 contingeny 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 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.

Telecommunications-specific implementation guidance

If the agreed service level is no longer met, telecommunications organizations should escalate any customer-initiated issues that affect both customer and employees regarding the operation of existing customer configurations such as hardware outages, network problems and the company configurations.

All customers should be made fully aware of problem escalation procedures and have the relevant documentation available to them.

For example, customer-initiated issues can be prioritized according to the criteria provided:

a) customer site is completely down or is failing to meet SLA requirements;

b) customer site is being significantly impacted by the outage; one or more systems down or significant packet loss and/or latency;

c) customer service degraded;

d) customer requests.

Telecommunications organizations, responsible for the provision of telecommunications services as an important utility, should establish mechanisms and/or procedures for containing, eradicating and recovering from information security incidents as well as those for detecting and analysing incidents in telecommunications systems accurately and in a timely manner.

Such mechanisms and/or procedures should include the following actions:

a) determine whether an incident has occurred by analysing indications and related information;

b) classify and prioritize the incident according to the incident management scheme;

c) report the incident to the appropriate internal personnel and external organizations;

d) acquire, preserve, secure, and document evidence;

e) isolate the telecommunication system, if possible, and use of it should be stopped; if the system is to be examined, it should be disconnected from any telecommunications operation networks before being re-powered;

f) eradicate the incident by identifying and mitigating all vulnerabilities that were exploited and remove malicious code, inappropriate materials, and other components;

g) recover from the incident with a confirmation that the affected systems are functioning normally; if necessary, implement additional monitoring to look for future related activity.

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.

Other information for telecommunications

Telecommunications organizations should share information regarding information security incidents with the relevant organizations such as Telecom-ISAC.

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.

Telecommunications-specific implementation guidance

Telecommunications organizations should establish mechanisms and/or procedures for sharing the lessons learnt and improving the incident management, taking account of the following actions:

a) hold a post-incident meeting, which includes on the agenda the lessons learned; this meeting should consider ways for improving security measures and the incident handling process itself;

b) collect incident data, such as number of incidents handled, total hours on involvement, costs and so on, and use it for improvement of incident management scheme;

c) retain related evidence in consideration with prosecution, law/regulation, and cost (see 13.2.3).

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 in ISO/IEC 27002).

13.2.3 Collection of evidence

Control 13.2.3 from ISO/IEC 27002 applies.

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 prioritization 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;

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).

Telecommunications-specific implementation guidance

Telecommunications organizations should ensure the safety of telecommunications facilities as one of the key elements of business continuity management.

14.1.2 Business continuity and risk assessment

Control 14.1.2 from ISO/IEC 27002 applies.

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;

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.

Telecommunications-specific implementation guidance

In developing and implementing the business continuity plan, telecommunications organizations should consider the inclusion of emergency rehabilitation plan of telecommunications services and ensuring essential communications of telecommunications service customers. If adjacent buildings or sites are damaged or requested for evacuation, telecommunications service facilities may become virtually out of control, even if the facilities themselves are not damaged. Telecommunications organizations should consider how to cope with such situations.

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 14.1.4 from ISO/IEC 27002 applies.

14.1.5 Testing, maintaining and re-assessing business continuity plans

Control 14.1.5 from ISO/IEC 27002 applies.

15 Compliance

The control objectives and the contents from ISO/IEC 27002 clause 15 apply.

Annex A

Telecommunications extended control set

(This annex forms an integral part of this Recommendation | International Standard)

This annex provides definitions for new objectives, new controls and new implementation guidance, as a telecommunications extended control set. ISO/IEC 27002 control objectives related to the new controls are repeated without any modifications. It is recommended that any organization implementing these controls in the context of an ISMS which is intended to be conformant to ISO/IEC 27001 extend their SOA by the inclusion of the controls stated in this annex.

A.9 Physical and environmental security

A.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.

A.9.1.7 Securing communication centres

Control

Physical security of communication centres, where telecommunications facilities such as switching facilities for providing telecommunications business are housed, should be designed, developed and applied.

Implementation guidance

To protect telecommunications facilities such as switching facilities for providing telecommunications business (hereafter referred to as communication centres), the following should take place:

a) a site on rigid ground should be selected for communication centres; when appropriate, less than rigid ground may be selected provided adequate measures are taken to prevent uneven settlement;

b) a site whose environment is least susceptible to damage from wind and water, etc., should be selected for communication centres; where a site is chosen that is vulnerable to environmental damage, appropriate measures should be taken against wind and water hazards;

c) a site whose environment is least susceptible to damage from strong electromagnetic field should be selected for communication centres; where a site is chosen that is exposed to strong electromagnetic fields, appropriate measures should be taken to protect telecommunications equipment rooms with electromagnetic shields;

d) communication centres should not be located at sites adjacent to facilities used for storing dangerous articles that pose the danger of explosion or combustion;

e) communication centre buildings should be of earthquake-proof construction;

f) communication centre buildings should be of fire-proof or fire-resistant construction;

g) communication centre buildings should have adequate structural stability to meet the necessary floor load;

h) automatic fire alarms should be installed in communication centres.

A.9.1.8 Securing telecommunications equipment room

Control

Physical security of equipment room, where telecommunications facilities are set for providing telecommunications business, should be designed, developed and applied.

Implementation guidance

To protect a room in which facilities are located for providing telecommunications services (hereafter referred to as telecommunications equipment room), the following controls should be considered:

a) the telecommunications equipment room should be located where it is least susceptible to external effects such as natural disasters;

b) the telecommunications equipment room should be located where it is least susceptible to intrusion by unauthorized personnel; adequate measures should be taken to prevent such intrusions;

c) the telecommunications equipment room should be located where it is least susceptible to flooding; if the room needs to be located where it is susceptible to flooding, then necessary measures should be taken such as raising the floor level, installing a water blockade, and installing special water drainage facilities;

d) the telecommunications equipment room should be located where it is least susceptible to damage from strong electromagnetic fields; if the room needs to be located where it is susceptible to strong electromagnetic fields, it should be protected by electromagnetic shields or some other measures; especially, if power supply facilities are installed within the telecommunications equipment room, measures should be appropriately taken to prevent interference from electromagnetic field;

e) important facilities should be placed in an exclusive telecommunications equipment room appropriate physical protection;

f) measures should be taken to prevent the materials used for the floor, walls, ceiling and so on from collapsing and falling, for example, due to earthquakes of a normally predictable magnitude;

g) materials used for the floor, walls, ceiling and so on should be non-combustible or fire-resistant;

h) measures should be taken to deal with static electricity;

i) ducts connecting telecommunications equipment rooms should be designed to slow down or prevent the spread of fire;

j) if necessary, measures should be taken to protect the data storage room and data safe from electromagnetic interference;

k) fire-proofing measures should be taken for the data storage room and dedicated data warehouses as needed;

l) automatic fire alarms should be installed in the telecommunications equipment room and the air-conditioning facility room;

m) fire extinguishers should be installed in the telecommunications equipment room and the air-conditioning facility room;

n) the telecommunications equipment room should be air-conditioned;

o) air-conditioning of telecommunications equipment room housing important facilities should be provided by a separate system from that for offices and other rooms.

A.9.1.9 Securing physically isolated operation areas

Control

For physically isolated operating areas, where telecommunications facilities are located for providing telecommunications business, physical security controls should be designed, developed and implemented.

Implementation guidance

To protect physically isolated operating area (e.g., mobile base station) in which telecommunications facilities are located for providing telecommunications business (hereafter referred to as isolated operating area), the following controls should be considered:

a) isolated operating areas should be earthquake-proof to meet the mandated national or regional standards;

b) isolated operating areas should be equipped with automatic fire control equipment;

c) isolated operating areas should be monitored by a remote office for the purpose of detecting facility failures, power failures, fire, humidity and temperature and so on;

d) physically secure perimeters should be provided in a proper manner, for example, using secure fencing to cover the isolated operating area; since it is normally operated in an unmanned way, it should be equipped with an automatic alert function to the operation centre in the event of incident.