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);