INTERNATIONAL STANDARD

ISO/IEC 27011

Second edition
2016-12-01

Information technology — Security techniques — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications

Reference number
ISO/IEC 27011:2016(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
copyright@iso.org
Web www.iso.org

Published in Switzerland

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.

This second edition cancels and replaces firs edition of ISO/IEC 27011:2008 which has been technically revised.

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 Rec. ITU-T X.1051.

CONTENTS

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security controls in telecommunications organizations based on ISO/IEC 27002.

Telecommunications organizations provide telecommunications services by facilitating the communications of customers through their infrastructure. In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their services and facilities and/or use the services and facilities of other telecommunications organizations. Furthermore, the site location, such as radio sites, antenna locations, ground cables and utility provision (power, water), may be accessed not only by the organization's staff, but also by contractors and providers external to the organization.

Therefore, the management of information security in telecommunications organizations is complex, potentially:

- depending on external parties;
- having to cover all areas of network infrastructure, services applications and other facilities;
- including a range of telecommunications technologies (e.g., wired, wireless or broadband);
- supporting a wide range of operational scales, service areas and service types.

In addition to the application of security objectives and controls described in ISO/IEC 27002, telecommunications organizations may need to implement extra controls to ensure confidentiality, integrity, availability and any other security property of telecommunications in order to manage security risk in an adequate fashion.

1) *Confidentiality*

   Protecting confidentiality of information related to telecommunications 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. This includes ensuring that persons engaged by the telecommunications organization 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*

   Protecting the integrity of telecommunications information includes controlling the installation and use of telecommunications facilities to ensure the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other method.

3) *Availability*

   Availability of telecommunications information includes ensuring that access to facilities and the medium used for the provision of communication services is authorized, regardless of whether communications is provided by wire, radio or any other method. Typically, telecommunications organizations give priority to essential communications in case of emergencies, managing unavailability of less important communications in compliance with regulatory requirements.

Audience

The audience of this Recommendation | International Standard consists of telecommunications organizations and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers. This Recommendation | International Standard provides 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 – Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security controls 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 27000, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
- ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls.*

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Recommendation | International Standard, the definitions given in ISO/IEC 27000 and the following apply:

3.1.1 co-location: 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 disasters and for the maintenance of public order in adverse conditions.

3.1.4 non-disclosure of communications: Requirement not to disclose the existence, the content, the source, the destination and the date and time of communicated information.

3.1.5 priority call: Telecommunications made by specific terminals in the event of emergencies, which should be handled with priority by restricting public calls.

NOTE – The specific terminals may span different services (voice over Internet protocol (VoIP), public switched telephone network (PSTN) voice, Internet protocol (IP) data traffic, etc.) for wired and wireless networks.

3.1.6 telecommunications applications: Applications such as Voice over IP (VoIP) that are consumed by end-users and built upon the network based services.

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

3.1.8 telecommunications equipment room: A secure location or room within a general building where equipment for providing telecommunications business are sited.

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

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

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

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

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

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

3.1.15 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.

3.1.16 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:

CIA	Confidentiality, Integrity and Availability
CNI	Critical National Infrastructure
DDoS	Distributed Denial of Service
DNS	Domain Name System
DoS	Denial of Service
HVAC	Heating, Ventilation, and Air Conditioning
IP	Internet Protocol
IRC	Internet Relay Chat
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
NMS	Network Management System
OAM&P	Operations, Administration, Maintenance and Provisioning
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMS	Short Message Service
SOA	Statement of Applicability
URL	Uniform Resource Locator
VoIP	Voice over Internet Protocol

4 Overview

4.1 Structure of this Recommendation | International Standard

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. A telecommunications sector-specific set of control and implementation guidance is described in normative Annex A.

In cases where controls need additional guidance specific to telecommunications, the ISO/IEC 27002 control 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)

- Human resources security (clause 7)
- Asset management (clause 8)
- Access control (clause 9)
- Physical and environmental security (clause 11)
- Operations security (clause 12)
- Communications security (clause 13)
- Systems acquisition, development and maintenance (clause 14)
- Supplier relationships (clause 15)
- Information security incident management (clause 16)
- Information security aspects of business continuity management (clause 17)

4.2 Information security management systems in telecommunications organizations

4.2.1 Goal

Information is critical to every organization. In the case of telecommunications, information consists of data transmitted between any two points in an electronic formation as well as metadata of each transmission, e.g., positioning data of sender and receiver. Regardless of how the information is transmitted and whether it is cached or stored during transmission, information should always be appropriately protected.

Telecommunications organizations and their information systems and networks are exposed to security threats from a wide range of sources, including: wire-tapping; advanced persistent threats; terrorism; espionage; sabotage; vandalism; information leakage; errors; and force majeure events. These security threats may originate from inside or outside the telecommunications organization, resulting in damage to the organization.

Once information security is violated, e.g., by wire-tapping the telecommunications lines, the organization may suffer damage. Therefore, it is essential for an organization to ensure its information security by continual improvement of its information security management system (ISMS).

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 telecommunications facilities, services and applications. These activities will enable an organization to meet its security objectives and therefore business objectives.

Telecommunications organizations provide facilities to various user types to process, transmit and store information. This information could be personally identifiable information, or confidential private and business data. In all cases, information should be handled with the correct level of care and attention, and the appropriate levels of protection provided to ensure confidentiality, integrity and availability (CIA), with privacy and sensitivity being paramount.

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 a network management system (NMS). Therefore, telecommunications security incidents can occur to various equipment/facilities and the incidents can propagate rapidly through the network into other equipment/facilities.

b) In addition to telecommunications facilities, vulnerabilities in network protocols and topology can result in serious security incidents. In particular, convergence of wired and wireless networks 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, 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.

f) Telecommunications services can be disrupted by malware such as worms and viruses attacking end systems or communications infrastructure. DoS/DDoS is a major cause of incidents on communications and can be caused by various methods to interrupt or block communication signals, or sending data to one system or network from many hundreds of systems as the same time to overload it (see TEL 13.1.6).

For the purpose of protecting information assets in telecommunications originating from different sources in 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 confidence that the information security requirements of their interested parties (e.g., suppliers, customers, regulators) will be satisfied;

b) telecommunications organizations seeking a business advantage through the implementation of an ISMS;

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 ISMS 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 ISMS appropriate to that organization;

f) ensuring compliance with trans-border legal and regulatory requirements, and complying with statutory requirements in all countries of operation or transit.

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 clause 8.1.1.

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) Those 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, trans-border legal and regulatory compliance, and the socio-cultural environment. Examples of legislative requirements for telecommunications organizations are non-disclosure of communications (TEL.18.1.6 in Annex A) and ensuring essential communications (TEL.18.1.7 in Annex A). Examples of socio-cultural requirements are ensuring the integrity of telecommunications that are 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, objectives 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 and at least annually, 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 Recommendation | International Standard 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 Recommendation | International Standard 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; additionally, the selection should be subject to all relevant national and international legislation and regulations.

5 Information security policies

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

NOTE – It might be necessary to take account of telecommunications-specific legislation and regulatory requirements and associated requirements concerning how these are both met and evidenced.

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

Control

All information security responsibilities should be defined and allocated.

Implementation guidance

The implementation guidance from ISO/IEC 27002 6.1.1 applies.

Telecommunications-specific implementation guidance

There should be an appointment of an executive manager who is responsible for all risks to telecommunication infrastructure and is accountable for their management.

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 telecoms engineers and other staff should be notified of and formally agree to their assigned roles and responsibilities.

Where cryptography is used, there should be specific crypto-custodian roles and personnel in these positions should be properly trained in the management of cryptographic material and the use and protection of cryptographic systems.

Other information

The other information from ISO/IEC 27002 6.1.1 applies.

6.1.2 Segregation of duties

Control and the contents from ISO/IEC 27002 6.1.2 apply.

6.1.3 Contact with authorities

Control

Appropriate contacts with relevant authorities should be maintained.

Implementation guidance

The implementation guidance from ISO/IEC 27002 6.1.3 applies.

Telecommunications-specific implementation guidance

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

The applications and infrastructure of telecommunications organizations can be considered part of critical infrastructure and may be essential for the functioning of the community, society and economy as a whole. Operators of such systems should therefore maintain contact with all of the relevant authorities. Telecommunications organizations should therefore maintain contact with all of the relevant authorities.

Other information

The other information from ISO/IEC 27002 6.1.3 applies.

6.1.4 Contact with special interest groups

Control and the contents from ISO/IEC 27002 6.1.4 apply.

6.1.5 Information security in project management

Control and the contents from of ISO/IEC 27002 6.1.5 apply.

6.2 Mobile devices and teleworking

The control objectives and the contents from ISO/IEC 27002 6.2 apply.

7 Human resource security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 7.1.1 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations should consider detailed checks on candidates for job positions that give employees access to sensitive information. This should also apply to positions giving employees access to telecommunications equipment or to communications information as this could provide unrestricted access to data which can become sensitive as a result of aggregation.

NOTE – Any person who is involved with critical national infrastructure (CNI) aspects of communications systems should be subjected to formal screening and criminal records checks before being given access.

7.1.2 Terms and conditions of employment

Control

The contractual agreements with employees and contractors should state their and the organization's responsibilities for information security.

Implementation guidance

The implementation guidance from ISO/IEC 27002 7.1.2 applies.

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.

Telecommunications organizations should clarify and state the responsibilities for maintaining the communications service provided by telecommunications organizations in addition to the protection and non-disclosure of personally identifiable and other confidential information in the terms and conditions of employment.

Telecommunications organizations should make sure that any person engaged in their telecommunications services is aware and up-to date on:

a) their responsibilities for protecting the personal identifiable information and other confidential information of users of their service;

b) their responsibilities concerning the non-disclosure of privileged information obtained through their operational activities on telecommunications services.

Other information

The other information from ISO/IEC 27002 7.1.1 applies.

7.2 During employment

The control objectives and the contents from ISO/IEC 27002 7.2 apply.

7.3 Termination or change of employment

The control objectives and the contents from ISO/IEC 27002 7.3 apply.

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

Control

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

Implementation guidance

The implementation guidance from ISO/IEC 27002 8.1.1 applies.

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.

Other information

The other information from ISO/IEC 27002 8.1.1 applies.

8.1.2 Ownership of assets

Control and the contents from ISO/IEC 27002 8.1.2 apply.

8.1.3 Acceptable use of assets

Control and the contents from ISO/IEC 27002 8.1.3 apply.

8.1.4 Return of assets

Control and the contents from ISO/IEC 27002 8.1.4 apply.

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification guidelines

Control

Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

Implementation guidance

The implementation guidance from ISO/IEC 27002 8.2.1 applies.

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) situations where information may be subject to legally regulated disclosure requirements;

b) distinction between information relating to essential communications that need to be handled with priority in an emergency or possible emergency and non-essential communications (see TEL.18.1.7 in Annex A);

c) awareness of the effects of aggregation, where classified or sensitive information can be deduced by searching large amount of data.

Other information

The other information from ISO/IEC 27002 8.2.1 applies.

8.2.2 Labelling of information

Control and the contents from ISO/IEC 27002 8.2.2 apply.

8.2.3 Handling of assets

Control and the contents from ISO/IEC 27002 8.2.3 apply.

8.3 Media handling

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

9 Access control

9.1 Business requirement for access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 9.1.1 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations should implement role-based access controls, with a limited number of profiles and controlled sets of user access permissions as applicable.

As telecommunication companies are regularly exposed to different suppliers that may not support the same security features or standards, it is essential to ensure all access is tracked for amendments and timely removal.

Only the authorized users should have access to use the communications services, such as a particular phone number, voicemail or other data services that have been assigned to them.

Other information

The other information from ISO/IEC 27002 9.1.1 applies.

9.1.2 Access to networks and network services

Control and the contents from ISO/IEC 27002 9.1.2 apply.

9.2 User access management

The control objective and the contents from ISO/IEC 27002 9.2 apply.

9.3 User responsibilities

The control objective and the contents from ISO/IEC 27002 9.3 apply.

9.4 System and application access control

The control objective and the contents from ISO/IEC 27002 9.4 apply.

10 Cryptography

The control objectives and the contents from ISO/IEC 27002 clause 10 apply.

11 Physical and environmental security

11.1 Secure areas

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

11.1.1 Physical security perimeter

Control

Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.

Implementation guidance

The implementation guidance from ISO/IEC 27002 11.1.1 applies.

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

The other information from ISO/IEC 27002 11.1.1 applies.

11.1.2 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 implementation guidance from ISO/IEC 27002 11.1.2 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the following guidelines:

a) appropriate physical security controls should be applied to all Telecommunication operation rooms and control centres;

b) upon entry, relevant visitor data should be recorded and adequately protected from unauthorized disclosure;

c) visitor records should be physically and electronically protected to preserve the CIA of the information they contain.

11.1.3 Securing offices, rooms, and facilities

Control and the contents from ISO/IEC 27002 11.1.3 apply.

11.1.4 Protecting against external and environmental threats

Control and the contents from ISO/IEC 27002 11.1.4 apply.

11.1.5 Working in secure areas

Control and the contents from ISO/IEC 27002 11.1.5 apply.

11.1.6 Delivery and loading areas

Control and the contents from ISO/IEC 27002 11.1.6 apply.

11.2 Equipment

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

11.2.1 Equipment siting and protection

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 11.2.1 applies.

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 have additional security in place, e.g., by being located in a separate secured area.

11.2.2 Supporting utilities

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 11.2.2 applies.

Telecommunications-specific implementation guidance

In particular, power supply facilities in isolated areas, 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.

Any equipment room should have adequate heating, ventilation and air conditioning (HVAC) services to ensure external environmental conditions do not result in equipment operating outside manufacturers' guidelines.

Other information

The other information from ISO/IEC 27002 11.2.2 applies.

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.

11.2.3 Cabling security

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 11.2.3 applies.

Telecommunications-specific implementation guidance

Cabling should be implemented to ensure that wire-tapping and eavesdropping devices or any alteration to the cabling can be detected either using active means or regular audits of access points.

11.2.4 Equipment maintenance

Control and the contents from ISO/IEC 27002 11.2.4 apply.

11.2.5 Removal of assets

Control and the contents from ISO/IEC 27002 11.2.5 apply.

11.2.6 Security of equipment and assets off-premises

Control and the contents from ISO/IEC 27002 11.2.6 apply.

11.2.7 Secure disposal or re-use of equipment

Control and the contents from ISO/IEC 27002 11.2.7 apply.

11.2.8 Unattended user equipment

Control and the contents from ISO/IEC 27002 11.2.8 apply.

11.2.9 Clear desk and clear screen policy

Control and the contents from ISO/IEC 27002 11.2.9 apply.

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.1.1 applies.

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 16.1).

12.1.2 Change management

Control

Changes to the organization, business processes, information processing facilities and systems that affect information security should be controlled.

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.1.2 applies.

Telecommunications-specific implementation guidance

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

Changes to infrastructure, including both physical and logical modifications, should be subject to a change management process. When applicable, this process should seek approval from a designated risk owner. Output from the change process, including risk assessments, should be subject to regular security audits.

Other information

The other information from ISO/IEC 27002 12.1.2 applies.

12.1.3 Capacity management

Control and the contents from ISO/IEC 27002 12.1.3 apply.

12.1.4 Separation of development, testing and operational environments

Control

Development, testing and operational environments should be separated to reduce the risks of unauthorized access or changes to the operational environment.

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.1.4 applies.

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 include sensitive information (e.g., personally identifiable 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.

Wherever possible, non-operational data or anonymized data produced from operational data should be used for testing.

Development staff should only have access to operational passwords or other authentication tokens where controls are in place for temporary authorization used for the support of operational systems. Controls should ensure that such authorizations are revoked or authentication tokens are changed after use.

Other information

The other information from ISO/IEC 27002 12.1.4 applies.

12.2 Protection from malware

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

12.3 Backup

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

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

Control

Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.4.1 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations should set the appropriate retention time period for retaining telecommunications data (e.g., accounting, billing, attending to complaints, as well as protection from 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 other information from ISO/IEC 27002 12.4.1 applies.

Other information for telecommunications

Appropriate measures to ensure non-disclosure of communications should be taken (see TEL.18.1.6 in Annex A).

12.4.2 Protection of log information

Control and the contents from ISO/IEC 27002 12.4.2 apply.

12.4.3 Administrator and operator logs

Control and the contents from ISO/IEC 27002 12.4.3 apply.

12.4.4 Clock synchronization

Control and the contents from ISO/IEC 27002 12.4.4 apply.

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

Control

Procedures should be implemented to control the installation of software on operational systems.

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.5.1 applies.

Telecommunications-specific implementation guidance

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

a) changes to critical systems' applications or operating system software should be fully tested. Procedures for rolling back such an upgrade should be included;

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

c) regression test of any updates, patches and changes on a test system, and ensure they operate correctly before they are implemented in an operational environment.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

Control

Control and the contents from ISO/IEC 27002 12.6.1 apply.

12.6.2 Restrictions on software installation

Control

Rules governing the installation of software by users should be established and implemented.

Implementation guidance

The implementation guidance from ISO/IEC 27002 12.6.2 applies.

Telecommunications-specific implementation guidance

For sensitive systems such as network elements or operations systems, only verified and permitted software should be installed.

Only authorized maintenance personnel should be able to install software on sensitive systems. This restriction should also be applied on the terminals used to administer the sensitive systems.

Software that can adversely affect sensitive systems performance and/or security should be controlled and monitored.

12.7 Information systems audit considerations

The control objective and the contents from ISO/IEC 27002 12.7 apply.

13 Communications security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

Control and the contents from ISO/IEC 27002 13.1.1 apply.

13.1.2 Security of network services

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 13.1.2 applies.

Other information

The other information from ISO/IEC 27002 13.1.2 applies.

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 operations, administration, maintenance and provisioning (OAM&P) as well as configuration of network services;

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

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

13.1.3 Segregation in networks

Control

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

Implementation guidance

The implementation guidance from ISO/IEC 27002 13.1.3 applies.

Telecommunications-specific implementation guidance

Specific attention should be paid to adequate segregation of production and management networks.

Hosted customer networks and associated data require adequate segregation from other parts of operational networks and other data.

Other information

The other information from ISO/IEC 27002 13.1.3 applies.

13.2 Information transfer

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

13.2.1 Information transfer policies and procedures

Control and the contents from ISO/IEC 27002 13.2.1 apply.

13.2.2 Agreements on information transfer

Control and the contents from ISO/IEC 27002 13.2.2 apply.

13.2.3 Electronic messaging

Control and the contents from ISO/IEC 27002 13.2.3 apply.

13.2.4 Confidentiality or non-disclosure agreements

Control and the contents from ISO/IEC 27002 13.2.4 apply.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

The control objective and the contents from ISO/IEC 27002 14.1 apply.

14.2 Security in development and support processes

The control objective and the contents from ISO/IEC 27002 14.2 apply.

14.3 Test data

The control objective and the contents from ISO/IEC 27002 14.3 apply.

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

Control

Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance

The implementation guidance from ISO/IEC 27002 15.1.1 applies.

Telecommunications-specific implementation guidance

If supplier's access to sensitive information (e.g., personally identifiable information and telephone records) is to be granted, telecommunications organizations should:

- ensure that the supplier is capable of adequately protecting that information;
- include handling of such sensitive information in a confidentiality or non-disclosure agreement with the supplier (see 13.2.4 in ISO/IEC 27002);
- meet all legal and regulatory requirements including trans-border requirements.

15.1.2 Addressing security within supplier agreements

Control

All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate or provide IT infrastructure components for, the organization's information.

Implementation guidance

The implementation guidance from ISO/IEC 27002 15.1.2 applies.

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 other information from ISO/IEC 27002 15.1.2 applies.

15.1.3 Information and communication technology supply chain

Control

Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance

The implementation guidance from ISO/IEC 27002 15.1.3 applies.

Telecommunications-specific implementation guidance

Supplier agreements between a telecommunications organization and its customers should include appropriate controls to ensure the non-disclosure of sensitive customer data. For instance, if directory assistance services are provided by third parties, the suppliers agreements should include requirements concerning disclosure of customer data, such as their telephone numbers or IDs.

When essential communications together with other communications are provided by suppliers, the telecommunications organizations should ensure existing agreements are fulfilled regarding prioritization of essential communications throughout the supply chain.

In cases where components provided by the supply chain are integrated into a telecommunications network, the organization should ensure the integrity and communications functionality of sourced components. Particular attention should be paid to maintenance and "call home" or "trouble reporting" functionalities.

Where services provided by a supplier involve sensitive information, there should be supplier agreements in place. These should include terms prohibiting any sub-contract that allows access to information in scope of the agreement, without prior agreement of the data owner. When it is necessary for a supplier to sub-contract work, telecommunications organizations should ensure that the appropriate levels of protection for that sensitive information have been previously agreed and are maintained throughout the entire supply chain.

15.2 Supplier service delivery management

The control objective and the contents from ISO/IEC 27002 15.2 apply.

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

16.1.1 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

The implementation guidance from ISO/IEC 27002 16.1.1 applies.

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.

Incident response procedures should include criteria and timing requirements for providing information about information security incidents to customers.

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 service level agreement (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, in addition to actions proposed in ISO/IEC 27002 16.1.1 include the following:

a) report the incident to the appropriate internal personnel and external organizations, including regulators, emergency services and those involved in critical infrastructure, as required;

b) isolate the telecommunication system, if possible – 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;

c) 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

The other information from ISO/IEC 27002 16.1.1 applies.

Other information for telecommunications

Telecommunications organizations should share information regarding information security incidents with the relevant organizations such as the Telecom Information Sharing and Analysis Centre (Telecom-ISAC).

16.1.2 Reporting information security events

Control and the contents from ISO/IEC 27002 16.1.2 apply.

16.1.3 Reporting security weaknesses

Control and the contents from ISO/IEC 27002 16.1.3 apply.

16.1.4 Assessment of and decision on information security events

Control

Information security events should be assessed and it should be decided if they are to be classified as information security incidents.

Implementation guidance

The implementation guidance from ISO/IEC 27002 16.1.4 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations should consider the impact on customers when classifying security events as incidents.

16.1.5 Response to information security incidents

Control

Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

The implementation guidance from ISO/IEC 27002 16.1.5 applies.

Telecommunications-specific implementation guidance

Telecommunications organizations, if necessary, should promptly report incidents to the related customers through appropriate communications channels or other forms of communication.

The need to inform customers will depend on the nature of the service provided.

16.1.6 Learning from information security incidents

Control

Knowledge gained from analysing and resolving information security incidents should be used to reduce the likelihood or impact of future incidents.

Implementation guidance

The implementation guidance from ISO/IEC 27002 16.1.6 applies.

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 and costs, and use it for improvement of the incident management scheme;

c) retain related evidence in consideration of prosecution, law/regulation and cost (see 16.1.7).

Other information

The other information from ISO/IEC 27002 16.1.6 applies.

16.1.7 Collection of evidence

Control and the contents from ISO/IEC 27002 16.1.7 apply.

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

Control and the contents from ISO/IEC 27002 17.1.1 applies.

17.1.2 Implementing information security continuity

Control

The organization should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.

Implementation guidance

The implementation guidance from ISO/IEC 27002 17.1.2 applies.

Telecommunications-specific implementation guidance

Plan for graceful degradation of service with priority given to emergency services and the least critical services being degraded or stopped in priority order.

The business continuity plan should contain provision for information security continuity to protect information in various forms. In developing and implementing the business continuity plan, telecommunications organizations should consider the inclusion of a disaster recovery plan for telecommunications services and ensuring essential communications of telecommunications service customers.

Telecommunications organizations should also consider when to dispatch their staff to telecommunication operating areas for disaster recovery.

Other information

The other information from ISO/IEC 27002 17.1.2 applies.

17.1.3 Verify, review and evaluate information security continuity

Control and the contents from ISO/IEC 27002 17.1.3 apply.

17.2 Redundancies

Objective: To ensure availability of information processing facilities.

17.2.1 Availability of information processing facilities

Control

Information processing facilities should be implemented with redundancy sufficient to meet availability requirements.

Implementation guidance

The implementation guidance from ISO/IEC 27002 17.2.1 applies.

Telecommunications-specific implementation guidance

Telecommunications facilities for providing essential communications and supporting national critical infrastructure (see TEL.18.1.7 in Annex A) should have sufficient redundancies to ensure that a loss of availability does not impact the provision of the service.

18 Compliance

The control objectives and the contents from ISO/IEC 27002 clause 18 apply.

Annex A

Telecommunications extended control set

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

This annex provides 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 that is intended to be conformant to ISO/IEC 27001 extend their statement of applicability (SOA) by the inclusion of the controls stated in this annex.

TEL.9 Access control

TEL.9.5 Network access control

Objective: To prevent unauthorized access to networked services.

TEL.9.5.1 Telecommunications carrier identification and authentication by users

Control

Telecommunications organizations should provide an appropriate control for users to be able to identify and authenticate telecommunications organizations.

Implementation guidance

Where telecommunications services are used by remote users or via mobile links, such use is subject to the possibility of breach of confidentiality. This could be caused by a person impersonating a legitimate user of the service or malware compromising the service. Therefore, appropriate controls should be in place for telecommunications users to mutually authenticate their communications with telecommunications organizations.

If telecommunications users cannot authenticate telecommunications organizations, the telecommunications organizations should remind users that the authentication function is unavailable together with the generally incurred possible risks.

Other information

There are several alternatives utilizing encryption technology for identification and authentication.

One of the possible threats if users cannot correctly identify and authenticate telecommunications organizations is man-in-the-middle attacks.

TEL.11 Physical and environmental security

TEL.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to an organization's information and information processing facilities.

TEL.11.1.7 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) communication centres should be on level ground away from causes of vibration or natural hazards such as land movement;

b) communication centres should be well above the water table and any flood plains;

c) communication centres should be clear of man-made hazards such as chemical plants;

d) a site whose environment is least susceptible to damage from the environment should be selected for communication centres – where a site is chosen that is vulnerable to environmental damage, appropriate measures should be taken against known hazards including: natural disasters [see e)] and temperature extremes;

e) a site whose environment is least susceptible to damage from strong electromagnetic fields 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;

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

g) communication centre buildings should be designed to minimize the impact of natural disasters and/or events including:
   - earthquakes;
   - fires;
   - lightning;
   - floods;
   - water leakage.

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

i) automatic fire alarms should be installed in communication centres;

j) HVAC controls should be deployed to ensure that all communications equipment is operated within manufacturers' guidelines.

TEL.11.1.8 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

All telecommunications equipment rooms and facilities should be subject to the application of appropriate physical and environmental security controls, such as use of access control systems, CCTV, alarm systems, as well as protection against fire and adverse environmental conditions.

To protect a room in which facilities are located for providing telecommunications services (hereafter referred to as telecommunications equipment room), the following guidance 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 fields;

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

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

g) materials used for the floor, walls, ceiling etc. 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;

p) HVAC controls should be connected to an uninterruptable power supply to ensure loss of power does not impact the operating environment.

TEL.11.1.9 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 areas (e.g., mobile base stations) in which telecommunications facilities are located for providing telecommunications business (hereafter referred to as isolated operating areas), 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 etc.;

d) physically secure perimeters should be provided in a proper manner, e.g., 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.

TEL.11.3 Security under the control of other party

Objective: To protect equipment located outside telecommunications organizations' premises (e.g., co-locations) against physical and environmental threats.

TEL.11.3.1 Equipment sited in other carriers' premises

Control

When telecommunications organizations install equipment outside their own premises, the equipment should be sited in a protected area so that any risks from environmental threats or dangers and from the possibility of unauthorized access are reduced.

Implementation guidance

To protect the equipment of one telecommunications organization sited in the premises of another, the following controls should be considered:

a) the boundary and interface with the other telecommunications organization should be specified, and the equipment should be easily isolated from that of the other organization, if required;

b) an agreement for the supply of support utilities should be made with the other telecommunications organization;

c) management should confirm that the location where the equipment is to be installed is appropriate in order to ensure the desired level of security.

Other information

In order to make the security level of the other organization's premises consistent with that of the telecommunications organization's own premises, an agreement and rules for achieving the desired level of security with other

telecommunications organizations should be checked beforehand.

TEL.11.3.2 Equipment sited in user premises

Control

When telecommunications organizations install equipment within the telecommunications service customer premises in order to connect with the customer equipment, the organizations' equipment should be protected in order to reduce risk from environmental threats or dangers and from the risk of unauthorized access.

Implementation guidance

To protect equipment located at a telecommunications service customer site, the following controls should be considered:

a) the equipment, such as cabinet, installed at the customer site should be sturdy, and be adequately protected against unauthorized access;

b) modification or attempted modification of equipment should be detectable;

c) the boundary and interface with the customer should be specified, and the equipment should be easily isolated from the customer, if required;

d) it should be possible to remotely monitor the status of the equipment or to operate the equipment.

TEL.11.3.3 Interconnected telecommunications services

Control

In the provision of interconnected telecommunications services, the telecommunications organizations should specify a well-defined boundary and interface with other telecommunications organizations, so that each organization may be partitioned and isolated in a timely manner in order to evade an identified risk.

Implementation guidance

Appropriate controls should be in place to check whether the service of interconnected telecommunications organizations is in normal operation or not.

In order to diagnose problems and take corrective actions, the organizations should have means to isolate the facilities of the organization from those of other organizations and to re-connect to them at the point of interconnection.

The telecommunications organizations should consistently monitor the traffic conditions at the point of interconnection.

Telecommunications organizations should specify in an agreement or a contract that the provision of telecommunications services for the customers may be suspended, whose communications pose a problem for the smooth service provision of the interconnected telecommunications organizations.

TEL.13 Communications security

TEL.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

TEL.13.1.4 Security management of telecommunications services delivery

Control

Telecommunications organizations should set the security level for the various business propositions of telecommunications services provided, announce it to their customers prior to service delivery, and maintain and manage their telecommunications services properly.

Implementation guidance

Telecommunications organizations should conduct the following activities for telecommunications service customers:

a) specification of security features, service levels, and management requirements of telecommunications services, and provision of their clear statement;

b) awareness activities to protect communications service users from unsolicited communications, cybercrime, malware and similar.

Telecommunications organizations should also consider the following:

c) implementation of controls compliant with relevant laws and regulations, such as prevention of unauthorized interception and ensuring interconnection with other telecommunications service providers;

d) provision of communications required for special service levels, such as essential communications in emergency situations (see TEL.18.1.7);

e) implementation of security controls for each service provided like the following;

IP connecting services/Data centre services:

1) controls against unsolicited communications such as email, fax, short message service (SMS) deliveries and automated calls (see TEL.13.1.5);

2) control against DoS/DDoS attack (see TEL.13.1.6);

3) control for management of technical vulnerabilities (see 12.6.1 in ISO/IEC 27002);

Telephone services/mobile-phone services:

4) handling of essential communications;

5) ensuring priority calls in an emergency;

6) traffic congestion of telephone calls;

Managed services:

7) utilization of authentication/encryption;

8) deliberate handling of privileged mode;

f) implementation of security controls in order to strictly maintain the following items in the management of information on service delivery:

1) ensuring non-disclosure of communications, including telephone call details;

2) protection of personally identifiable information.

Telecommunications service delivery should include appropriate controls to prevent the display of corruptly modified uniform resource locators (URLs). Upon detection of such an attack, service delivery should be suspended to minimize the impact of the attack and the relevant customer advised.

In order to maintain the telecommunications services provided, telecommunications organizations should apply the following controls:

g) appropriate maintenance of transmission facilities such as transmission cables and prompt repair in emergency situations;

h) appropriate maintenance of switching facilities for telecommunications services, or constant monitoring of their traffic load; changeover to back-up facilities or other routes in order to avoid traffic congestion in emergency situations;

i) methods and procedures to maintain the functions of telecommunications facilities in the case of DoS attacks which may force the switching facilities like routers to process a larger amount of traffics compared with ordinary situation;

j) appropriate management of internet routing information and control information such as the domain name system (DNS).

TEL.13.1.5 Response to spam

Control

Telecommunications organizations should stipulate the policies for responding to spam and implement appropriate controls in order to establish a favourable and desirable environment for e-mail communications.

Implementation guidance

When telecommunications organizations recognize spam from a telecommunications service user's complaint and the relevant spammer is their own customer, telecommunications organizations should request the relevant customer to stop the sending of spam.

In the case of a determined spammer attack, telecommunications organizations should suspend their services to the relevant customer, in order to minimize the impact of the attack.

When spam is sent out from the network of other telecommunications organizations with which telecommunications organizations interconnect its telecommunications facilities, the organization should request the relevant organization to take necessary measures in order to block spam, and the relevant organization should take appropriate actions, responding to such a request.

In order to take effective measures against spam, telecommunications organizations should work in close cooperation with other telecommunications organizations and spam-fighting organizations at home and abroad.

Telecommunications organizations should develop and implement their policies against spam in line with national law and regulations and make them available to the public.

TEL.13.1.6 Response to DoS/DDoS attacks

Control

Telecommunications organizations should stipulate the policies for responding to DoS/DDoS attacks and implement appropriate controls in order to prepare a favourable and desirable environment for telecommunications services.

Implementation guidance

When telecommunications organizations recognize the incidence of DoS/DDoS attacks e.g. detection of abnormal traffic patterns or unstable operation status of telecommunications facilities, telecommunications organizations should take appropriate countermeasures in order to ensure the ongoing stable operation of telecommunications facilities.

Although specific measures required depend upon the type of DoS/DDoS attacks, telecommunications organizations should take account of the following countermeasures:

a) filtering of packets heading for the target site under attacks;

b) restriction of communication port used for DoS/DDoS attacks;

c) reduction or suspension of operation of target telecommunications facilities.

When the DoS/DDoS attacker is their own customer, telecommunications organizations should suspend telecommunications services to the relevant customer in order to block DoS/DDoS attacks to telecommunications facilities.

When DoS/DDoS attacks comes from the network of other telecommunications organizations with which telecommunications organizations interconnect its telecommunications facilities, the organization should request the relevant organization to take necessary measures in order to stop DoS/DDoS attacks, and the relevant organization should take appropriate actions to respond to such requests.

In order to take effective measures against DoS/DDoS attacks, telecommunications organizations should work in close cooperation with other telecommunications organizations and anti-cyber terrorism organizations at home and abroad.

TEL.18 Compliance

TEL.18.1 Compliance with legal and contractual requirements

Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

TEL.18.1.6 Non-disclosure of communications

Control

Non-disclosure of communications being handled by telecommunications organizations should be ensured.

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;

e) the date and time;

in communicated information.

Telecommunications organizations should take account of the following guidelines:

a) maintaining telecommunications facilities properly to ensure non-disclosure of communications;

b) taking necessary measures to prevent unintended disclosure of other communications during normal use at the point of connection between telecommunications service users' terminal facilities and telecommunication circuits;

c) taking necessary measures to prevent unauthorized access, destruction or falsification of records and data of telecommunications service users stored in telecommunications facilities;

d) prohibiting the unauthorized or unlawful utilization by staff of the telecommunications organization of any information related to customer communication;

e) setting the appropriate retention period of telecommunications data, which is within the time period required for carrying out the purposes for retaining data, and delete them at the end of retention period or at the attainment of the purposes without any delay;

f) prohibiting provision of any secrets in communications to third parties, without legal enforcement or the consent of telecommunications service users themselves;

g) offering the functionality in which telecommunications service users can decide on a case-by-case basis whether they send their caller ID in the provision of caller ID services;

h) prohibiting the provision of caller ID to third parties, without legal enforcement or the consent of telecommunications service users themselves;

i) offering telecommunications service customers a choice as to whether to list their telephone numbers or ID related to other services, in the provision of directory assistance services – when users request their numbers to be unlisted, telecommunications organizations should exclude their information from directory assistance services without any delay;

j) when telecommunications organizations are requested to submit information related to telecommunications service users including non-disclosure of communications, they need to confirm that the request from law-enforcement agencies or other investigative bodies has gone through a legitimate procedure in accordance with the applicable national laws and regulations.

TEL.18.1.7 Essential communications

Control

Telecommunications organizations should, when a natural disaster, accident or any other emergency occurs, or at a risk of occurrence thereof, give priority to essential communications whose contents are necessary for the prevention of or relief or recovery from such incidents and for the maintenance of public order.

Implementation guidance

Telecommunications organizations should take account of suspending or restricting part of their telecommunications activities implementing graceful failure in order of importance or priority, in order to ensure that essential communications can be carried out by, for example, the following organizations and/or in agreement with national law and regulations:

a) meteorological organizations;

b) flood prevention organizations;

c) fire and rescue service organizations;

d) disaster relief organizations;

e) organizations directly associated with preservation of public order;

f) organizations directly associated with defence;

g) organizations directly associated with maritime safety;

h) organizations directly associated with ensuring transportation;

i) organizations directly associated with communications services;

j) organizations directly associated with electric power supply;

k) organizations directly associated with water supply;

l) organizations directly associated with gas supply;

m) election administration organizations;

n) journalistic organizations;

o) financial institutions;

p) medical institutions;

q) organizations directly associated with the food supply chain;

r) government agencies that provide essential services;

s) other national or local organizations that handle essential communications;

t) any other essential communications as defined by national laws, regulations or other requirements.

Telecommunications organizations should, in the case where they interconnect their telecommunications facilities with other telecommunications organizations, take the necessary measures to conclude an agreement for preferential treatment of essential communications in order to ensure their smooth and continuous operation.

TEL.18.1.8 Legality of emergency actions

Control

All measures that telecommunications organizations take in emergency situations should be confined only to those necessary and sufficient measures for legitimate self-defence or emergency evacuation. Such measures should be appropriate and not be excessive.

Implementation guidance

Telecommunications organizations should institute procedures in advance for contingency, including information security incidents, and get advice and guidance from legal experts whether the defined emergency measures are not excessive and that they are necessary and sufficient for legitimate self-defence or emergency evacuation.

Telecommunications organizations should make aware and advise their telecommunications service customers that they may need to take the necessary action, such as suspension of telecommunications services to respond to incidents where, for example, the connection with telecommunications service customers' facilities interfere with the functioning of telecommunications organizations facilities or other telecommunications service customers' facilities or other building sites and that might have an impact on human security and safety.

Annex B

Additional guidance for network security

(This annex does not form an integral part of this Recommendation | International Standard.)

B.1 Security measures against network attacks

B.1.1 Protection against network attack

a) Protection of network facilities

Telecommunications facilities should be appropriately protected in order to avoid significant interference to telecommunications services delivery caused by unexpected behaviour that is unintentionally provoked by malware delivered from telecommunications service users or telecommunications facilities of other organizations.

In order to protect IP network facilities, such as servers and routers, from attacks (e.g., DDoS attack), telecommunications organizations should have mechanisms to filter communications or limit communication bands in IP addresses, communication ports and application protocols. Depending on telecommunications services, such mechanisms of communications filters should be implemented associated with signal processing control, user authentication and access controls.

b) Measures against source impersonation

Telecommunications organizations should implement measures to protect against impersonation of IP addresses (IP spoofing).

In order to prevent source impersonation by means of a stepping stone, appropriate security controls against unauthorized access should be implemented at the systems providing user authentication by introducing strict password controls and/or strong authentication functions, e.g., mandatory use of unpredictable passwords above a certain length, and introduction of one-time-password and strong token authentication.

Telecommunications facilities dealing with essential communications should implement mechanisms to prevent source (caller) ID impersonation. For example, it is recommended that terminals based on hard-coding ID or mechanisms to verify caller ID in telecommunications network facilities by using a registered password at the time of registration and connection request be introduced.

c) Measures against malformed communication signal

Telecommunications organizations should implement measures to protect against malformed communication signals (e.g., illegally long packet).

For example, since malformed packets (that are often produced by network attacks) may cause IP network facilities failure, telecommunication organizations should drop such packets in order to protect telecommunications service or facilities.

B.1.2 Drawing attention of users

a) Drawing the attention of telecommunications services users

In order to deter unintended attacks from infected PCs of telecommunications service users or to promptly and properly respond to network attacks, telecommunications organizations should clearly specify in the terms and conditions of service delivery that the use of telecommunications services may be restricted in the case where telecommunications facilities are overloaded.

Telecommunications organizations should draw the attention of telecommunications service users to such threats (e.g., viruses and botnets) that may lead to network attacks and encourage them to take the necessary measures by themselves.

NOTE – The term "botnet" is generally used to refer to a group of compromised computers (called zombie computers) running programs, usually referred to as worms, Trojan horses or backdoors, under a common command and control infrastructure. A botnet's originator ("bot herder") can control the group remotely, usually through means, such as internet relay chat (IRC), and usually for nefarious purposes.

B.2 Network security measures for network congestion

B.2.1 Gathering information

a) Collection in advance of information that may cause congestion

Operating rules to collect information concerning disaster and planned events that may cause network congestion should be stipulated by telecommunications organizations, e.g., the establishment of a framework to collect weather information and planned events information. Mechanisms and procedures to report the collected information should be set up, and the information should keep relevant personnel informed.

b) Advance gathering of information that may trigger malfunction

Since disaster, accidents and social phenomena tend to be the cause of telecommunications facilities failures and network congestions, telecommunications organizations should consider measures in advance by gathering the relevant information and accumulating the know-how on a regular basis.

B.2.2 Measures against network congestion

a) Mechanisms of detecting and restricting network congestion

Telecommunications facilities should have mechanisms to detect network congestion and avoid concentration of communications in case of network congestion.

Telecommunications systems dealing with essential communications should have performance resilience to ensure that congestion control processes such as filtering do not adversely affect the provision of those essential services.

Telecommunications organizations should recognize the performance limits of the relevant communication facilities and implement mechanisms to control a number of communications requests before reaching the limits. Furthermore, traffic should be processed by distributed facilities, if possible.

b) Measures to improve temporary throughput

Taking account of the scale of potential disruption and disaster, the use of distributed processing centres and implementation of supplementary facilities, as well as adaptive configuration changes, should be considered, where necessary.

Bibliography

– ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*

– ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

– ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

– ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security.*

– ISO/IEC 27033-3:2010, *Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues.*

– ISO/IEC 27033-4:2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

– ISO/IEC 27033-5:2013, *Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs).*

– ISO/IEC 27035-1:2016, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management.*

– ISO/IEC 27035-2:2016, *Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

– ISO/IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*.

– ISO/IEC 27036-2:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements.*

– ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.*

– ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

ICS 35.040

Price based on 31 pages