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.