FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/IEC
FDIS
27011

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-11-13

Voting terminates on:
2024-01-08

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

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

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

Reference number
ISO/IEC FDIS 27011:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

INTERNATIONAL STANDARD ISO/IEC 27011

RECOMMENDATION ITU-T X.1051

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

Summary

This Recommendation | International Standard:

a) establishes guidelines and general principles for initiating, implementing, maintaining and improving information security controls in telecommunications organizations based on ISO/IEC 27002;

b) provides an implementation baseline of information security controls within telecommunications organizations to ensure the confidentiality, integrity and availability of telecommunications facilities, services and information handled, processed or stored by the facilities and services.

As a result of implementing this Recommendation | International Standard, telecommunications organizations, both within and between jurisdictions, will:

a) be able to ensure the confidentiality, integrity and availability of global telecommunications facilities, services and the information handled, processed or stored within global facilities and services;

b) have adopted secure collaborative processes and controls ensuring the lowering of risks in the delivery of telecommunications services;

c) be able to deliver information security in an effective and efficient manner;

d) have adopted a consistent holistic approach to information security;

e) be able to improve the security culture of organizations, raise staff awareness and increase public trust.

Keywords

information security controls and telecommunications extended controls, information security management, ISO/IEC 27002, information security risk assessment, information security risk treatment.

CONTENTS

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by ITU-T (as ITU-T Recommendation X.1051) and drafted in accordance with its editorial rules, in collaboration with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27011-1:2016), which has been technically revised. It also incorporates the Technical Corrigendum ISO/IEC 27011-1:2016/Cor 1:2018.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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), can 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 information security controls described in ISO/IEC 27002, telecommunications organizations can implement extra information security controls to ensure confidentiality, integrity, availability and any other information security property of telecommunications in order to manage information security risk in an adequate fashion. The security properties specialized for telecommunications can be described below (in no order of priority).

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 in the telecommunications organization maintain the confidentiality of any information regarding others that can 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 statutory and 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 information security controls based on ISO/IEC 27002, telecommunications sector-specific information security controls and information security management guidelines allowing for the selection and implementation of such controls.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

Information security, cybersecurity and privacy protection — Information security controls based on ISO/IEC 27002 for telecommunications organizations

1 Scope

The scope of this Recommendation | International Standard is to provide 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 information 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*

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.

Note 1 to entry: Communication information can include both data in motion and data at rest.

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 1 to entry: The specific terminals can 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 **resilience:** ability to absorb and adapt in a changing environment.

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

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

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

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

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

3.1.12 telecommunication records: information concerning the parties in a communication including the metadata such as the time, and duration of the telecommunication that took place but excluding the contents of the communication.

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

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

Note 1 to entry: A telecommunication service customer is a contractor with telecommunication organization and can be a telecommunication service user.

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

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

3.2 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
DNSSEC	domain name system security extensions
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
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 27002:2022. In cases where the information security control, attribute table, purpose, guidance and other information specified in ISO/IEC 27002:2022 are applicable without a need for any additional information, only a reference is provided to ISO/IEC 27002.

The following clauses include telecommunication sector specific information according to the control layout from ISO/IEC 27002:2022.

- Organizational controls (Clause 5)
- People controls (Clause 6)
- Physical controls (Clause 7)
- Technological controls (Clause 8)

Annex A provides additional guidance for network security

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 form as well as metadata of each transmission, e.g., positioning data of sender and receiver. Information in telecommunications organizations includes that information necessary for the organization to operate as well as information associated with telecommunications services. 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 information 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 can originate from inside or outside the telecommunications organization, resulting in damage to the organization and can also affect their customers.

Once information security is violated, e.g., by wire-tapping the telecommunications lines, the organization can 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 information security 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 information 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 Telecommunications Organizations

“Telecommunications Organizations” has evolved extensively to provide communication infrastructure and/or communication services. The following telecommunication organizations can be identified for providing communication infrastructure and/or services which can be forms of various businesses for telecommunications organizations.

A. Telecommunication organizations providing network facilities and the related services (Network facility service providers) - are the owners/providers of network facilities, namely infrastructure such as, cables, towers, satellite earth stations, broadband fibre optic cables, telecommunications lines and exchanges, radiocommunications transmission equipment, mobile communications base stations and broadcasting transmission towers and equipment. These represent the fundamental building blocks of the convergence model upon which network, applications and content services are provided.

B. Telecommunication organizations providing network services (Network service providers) – provide the basic connectivity and bandwidth to support a variety of network services. Network services enable connectivity or transport between different networks. A network service provider usually owns/deploys the network facilities or use the network facilities owned by another licensee providing connectivity services. [e.g., message communication service]

C. Telecommunication organizations providing applications services (Application service providers) – provide particular functions such as voice services, data services, Internet access and electronic commerce. Applications services are essentially the functions or capabilities, which are delivered to end-users. They do not install transmission line equipment by themselves and use the network facilities owned by another licensee providing connectivity services. [e.g., ISP service, MVNO service, CDN service]

D. Telecommunication organizations providing content applications (Content application service providers) – represent a special subset of applications service providers such as television and radio broadcast services, and