International Standard

ISO/IEC 27011

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

*Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/IEC 27002*

Third edition
2024-03

Reference number
ISO/IEC 27011:2024(en)

© ISO/IEC 2024



## COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

# 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.

© ISO/IEC 2024 – All rights reserved

**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.



**History**[*]

| Edition | Recommendation | Approval | Study Group | Unique ID |
|---|---|---|---|---|
| 1.0 | ITU-T X.1051 | 2004-07-29 | 17 | 11.1002/1000/7286 |
| 2.0 | ITU-T X.1051 | 2008-02-13 | 17 | 11.1002/1000/9332 |
| 3.0 | ITU-T X.1051 | 2016-04-29 | 17 | 11.1002/1000/12845 |
| 3.1 | ITU-T X.1051 (2016) Cor. 1 | 2017-09-06 | 17 | 11.1002/1000/13407 |
| 4.0 | ITU-T X.1051 | 2023-06-13 | 17 | 11.1002/1000/15559 |

**Keywords**

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


[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

© ISO/IEC 2024 – All rights reserved

## FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

## NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

## INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.



© ISO/IEC 2024 – All rights reserved

## CONTENTS


| | | Page |
|---|---|---|
| 1 | Scope | 1 |
| 2 | Normative references | 1 |
| 3 | Definitions and abbreviations | 1 |
| | 3.1 Definitions | 1 |
| | 3.2 Abbreviations | 2 |
| 4 | Overview | 2 |
| | 4.1 Structure of this Recommendation \| International Standard | 2 |
| | 4.2 Information security management systems in telecommunications organizations | 3 |
| 5 | Organizational controls | 5 |
| | 5.1 Policies for information security | 5 |
| | 5.2 Information security roles and responsibilities | 5 |
| | 5.3 Segregation of duties | 6 |
| | 5.4 Management responsibilities | 6 |
| | 5.5 Contact with authorities | 6 |
| | 5.6 Contact with special interest groups | 6 |
| | 5.7 Threat intelligence | 6 |
| | 5.8 Information security in project management | 6 |
| | 5.9 Inventory of information and other associated assets | 6 |
| | 5.10 Acceptable use of information and other associated assets | 6 |
| | 5.11 Return of assets | 6 |
| | 5.12 Classification of information | 7 |
| | 5.13 Labelling of information | 7 |
| | 5.14 Information transfer | 7 |
| | 5.15 Access control | 7 |
| | 5.16 Identity management | 7 |
| | 5.17 Authentication information | 7 |
| | 5.18 Access rights | 7 |
| | 5.19 Information security in supplier relationships | 7 |
| | 5.20 Addressing information security within supplier agreements | 8 |
| | 5.21 Managing information security in the ICT supply chain | 8 |
| | 5.22 Monitoring, review and change management of supplier services | 8 |
| | 5.23 Information security for use of cloud services | 8 |
| | 5.24 Information security incident management planning and preparation | 8 |
| | 5.25 Assessment and decision on information security events | 9 |
| | 5.26 Response to information security incidents | 9 |
| | 5.27 Learning from information security incidents | 9 |
| | 5.28 Collection of evidence | 9 |
| | 5.29 Information security during disruption | 9 |
| | 5.30 ICT readiness for business continuity | 10 |
| | 5.31 Legal, statutory, regulatory and contractual requirements | 10 |
| | 5.32 Intellectual property rights | 10 |
| | 5.33 Protection of records | 10 |
| | 5.34 Privacy and protection of PII | 10 |
| | 5.35 Independent review of information security | 10 |


© ISO/IEC 2024 – All rights reserved

*Page*

5.36 Compliance with policies, rules and standards for information security ..... 10
5.37 Documented operating procedures ..... 10
5.38 TEL – Interconnected telecommunications services ..... 10
5.39 TEL – Security management of telecommunications services delivery ..... 11
5.40 TEL – Response to spam ..... 12
5.41 TEL – Response to DoS/DDoS attacks ..... 12
5.42 TEL – Non-disclosure of communications ..... 13
5.43 TEL – Essential communications ..... 14
5.44 TEL – Legality of emergency actions ..... 15
5.45 TEL – Coordination for information security incident management ..... 15
6 People controls ..... 16
6.1 Screening ..... 16
6.2 Terms and conditions of employment ..... 16
6.3 Information security awareness, education and training ..... 16
6.4 Disciplinary process ..... 16
6.5 Responsibilities after termination or change of employment ..... 16
6.6 Confidentiality or non-disclosure agreements ..... 16
6.7 Remote working ..... 17
6.8 Information security event reporting ..... 17
7 Physical controls ..... 17
7.1 Physical security perimeter ..... 17
7.2 Physical entry ..... 17
7.3 Securing offices, rooms and facilities ..... 17
7.4 Physical security monitoring ..... 17
7.5 Protecting against physical and environmental threats ..... 17
7.6 Working in secure areas ..... 17
7.7 Clear desk and clear screen ..... 17
7.8 Equipment siting and protection ..... 18
7.9 Security of assets off-premises ..... 18
7.10 Storage media ..... 18
7.11 Supporting utilities ..... 18
7.12 Cabling security ..... 18
7.13 Equipment maintenance ..... 18
7.14 Secure disposal or re-use of equipment ..... 18
7.15 TEL – Securing communication centres ..... 18
7.16 TEL – Securing telecommunications equipment room ..... 19
7.17 TEL – Securing physically isolated operation areas ..... 20
7.18 TEL – Equipment sited in other carriers' premises ..... 21
7.19 TEL – Equipment sited in user premises ..... 21
8 Technological controls ..... 22
8.1 User endpoint devices ..... 22
8.2 Privileged access rights ..... 22
8.3 Information access restriction ..... 22
8.4 Access to source code ..... 22
8.5 Secure authentication ..... 22


© ISO/IEC 2024 – All rights reserved

*Page*

8.6 Capacity management ..... 22
8.7 Protection against malware ..... 22
8.8 Management of technical vulnerabilities ..... 22
8.9 Configuration management ..... 22
8.10 Information deletion ..... 22
8.11 Data masking ..... 22
8.12 Data leakage prevention ..... 22
8.13 Information backup ..... 22
8.14 Redundancy of information processing facilities ..... 22
8.15 Logging ..... 23
8.16 Monitoring activities ..... 23
8.17 Clock synchronization ..... 23
8.18 Use of privileged utility programs ..... 23
8.19 Installation of software on operational systems ..... 23
8.20 Network security ..... 23
8.21 Security of network services ..... 23
8.22 Segregation of networks ..... 24
8.23 Web filtering ..... 24
8.24 Use of cryptography ..... 24
8.25 Secure development lifecycle ..... 24
8.26 Application security requirements ..... 24
8.27 Secure system architecture and engineering principles ..... 24
8.28 Secure coding ..... 24
8.29 Security testing in development and acceptance ..... 24
8.30 Outsourced development ..... 24
8.31 Separation of development, test and production environments ..... 24
8.32 Change management ..... 24
8.33 Test information ..... 25
8.34 Protection of information systems during audit testing ..... 25
8.35 TEL – Telecommunications carrier identification and authentication by users ..... 25

Annex A Additional guidance for network security ..... 26
A.1 Security measures against network attacks ..... 26
A.2 Network security measures for network congestion ..... 27

Bibliography ..... 28

© ISO/IEC 2024 – All rights reserved

**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.


© ISO/IEC 2024 – All rights reserved

**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 – 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 – 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.

© ISO/IEC 2024 – All rights reserved