

# American National Standard

INCITS/ISO/IEC 27011:2016 (2019)

(ISO/IEC 27011:2016, IDT)

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

**Developed by**



*Where IT all begins*



## INCITS/ISO/IEC 27011:2016 (2019)

### PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

**Adopted by INCITS (InterNational Committee for Information Technology Standards) as an American National Standard.**

Date of ANSI Approval: 11/22/2019

Published by American National Standards Institute,  
25 West 43rd Street, New York, New York 10036

Copyright 2019 by Information Technology Industry Council  
(ITI). All rights reserved.

These materials are subject to copyright claims of International Standardization Organization (ISO), International Electrotechnical Commission (IEC), American National Standards Institute (ANSI), and Information Technology Industry Council (ITI). Not for resale. No part of this publication may be reproduced in any form, including an electronic retrieval system, without the prior written permission of ITI. All requests pertaining to this standard should be submitted to ITI, 1101 K Street NW, Suite 610, Washington DC 20005.

Printed in the United States of America

This is a preview of "INCITS/ISO/IEC 27011...". [Click here to purchase the full version from the ANSI store.](#)

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)



This is a preview of "INCITS/ISO/IEC 27011...". Click [here](#) to purchase the full version from the ANSI store.



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2016

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of "INCITS/ISO/IEC 27011...". [Click here to purchase the full version from the ANSI store.](#)

## 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 first 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.

This is a preview of "INCITS/ISO/IEC 27011...". [Click here to purchase the full version from the ANSI store.](#)

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	Information security policies .....	5
6	Organization of information security.....	5
	6.1 Internal organization .....	5
	6.2 Mobile devices and teleworking.....	6
7	Human resource security .....	6
	7.1 Prior to employment.....	6
	7.2 During employment .....	7
	7.3 Termination or change of employment .....	7
8	Asset management.....	7
	8.1 Responsibility for assets.....	7
	8.2 Information classification.....	8
	8.3 Media handling.....	8
9	Access control .....	8
	9.1 Business requirement for access control .....	8
	9.2 User access management.....	9
	9.3 User responsibilities .....	9
	9.4 System and application access control .....	9
10	Cryptography.....	9
11	Physical and environmental security .....	9
	11.1 Secure areas.....	9
	11.2 Equipment .....	10
12	Operations security.....	12
	12.1 Operational procedures and responsibilities.....	12
	12.2 Protection from malware.....	13
	12.3 Backup .....	13
	12.4 Logging and monitoring.....	13
	12.5 Control of operational software.....	13
	12.6 Technical vulnerability management .....	14
	12.7 Information systems audit considerations .....	14
13	Communications security .....	14
	13.1 Network security management.....	14
	13.2 Information transfer.....	15
14	System acquisition, development and maintenance .....	16
	14.1 Security requirements of information systems .....	16
	14.2 Security in development and support processes .....	16
	14.3 Test data .....	16
15	Supplier relationships .....	16
	15.1 Information security in supplier relationships.....	16
	15.2 Supplier service delivery management.....	17
16	Information security incident management .....	17
	16.1 Management of information security incidents and improvements.....	17
17	Information security aspects of business continuity management.....	19

This is a preview of "INCITS/ISO/IEC 27011...". [Click here to purchase the full version from the ANSI store.](#)

17.2	Redundancies .....	20
18	Compliance.....	20
	Annex A – Telecommunications extended control set .....	21
	Annex B – Additional guidance for network security .....	29
	B.1 Security measures against network attacks .....	29
	B.2 Network security measures for network congestion.....	30
	Bibliography .....	31



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.