
**Information technology — Security
techniques — Information security
management guidelines for
telecommunications organizations based
on ISO/IEC 27002**

*Technologies de l'information — Techniques de sécurité — Lignes
directrices pour le management de la sécurité de l'information pour les
organismes de télécommunications sur la base de l'ISO/CEI 27002*

Withhold

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.

Withdrawn

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2008

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
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published by ISO in 2009

Published in Switzerland

CONTENTS

	<i>Page</i>	
1	Scope	1
2	Normative references	1
3	Definitions and abbreviations	1
	3.1 Definitions	1
	3.2 Abbreviations	2
4	Overview	3
	4.1 Structure of this guideline	3
	4.2 Information security management systems in telecommunications business	3
5	Security policy	5
6	Organization of information security	5
	6.1 Internal organization	5
	6.2 External parties	7
7	Asset management	10
	7.1 Responsibility for assets	10
	7.2 Information classification	12
8	Human resources security	13
	8.1 Prior to employment	13
	8.2 During employment	15
	8.3 Termination or change of employment	15
9	Physical and environmental security	15
	9.1 Secure areas	15
	9.2 Equipment security	17
10	Communications and operations management	19
	10.1 Operational procedures and responsibilities	19
	10.2 Third party service delivery management	21
	10.3 System planning and acceptance	21
	10.4 Protection against malicious and mobile code	22
	10.5 Back-up	22
	10.6 Network security management	22
	10.7 Media handling	23
	10.8 Exchange of information	23
	10.9 Electronic commerce services	23
	10.10 Monitoring	23
11	Access control	25
	11.1 Business requirement for access control	25
	11.2 User access management	26
	11.3 User responsibilities	26
	11.4 Network access control	26
	11.5 Operating system access control	26
	11.6 Application and information access control	26
	11.7 Mobile computing and teleworking	26
12	Information systems acquisition, development and maintenance	26
	12.1 Security requirements of information systems	26
	12.2 Correct processing in applications	26
	12.3 Cryptographic controls	26
	12.4 Security of system files	26
	12.5 Security in development and support processes	27
	12.6 Technical vulnerability management	27
13	Information security incident management	28
	13.1 Reporting information security events and weaknesses	28
	13.2 Management of information security incidents and improvements	29

	<i>Page</i>
14 Business continuity management	31
14.1 Information security aspects of business continuity management	31
15 Compliance	33
Annex A – Telecommunications extended control set.....	34
A.9 Physical and environmental security	34
A.10 Communications and operations management.....	37
A.11 Access control	39
A.15 Compliance.....	39
Annex B – Additional implementation guidance	42
B.1 Network security measures against cyber attacks.....	42
B.2 Network security measures for network congestion.....	42
Bibliography	44

Withdrawn

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.

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 ITU-T Rec. X.1051 (02/2008).

Introduction

This Recommendation | International Standard provides interpretation guidelines for the implementation and management of information security management in telecommunications organizations based on ISO/IEC 27002 (Code of practice for information security management). In addition to the application of security objectives and controls described in ISO/IEC 27002, telecommunications organizations have to take into account the following security features:

1) *Confidentiality*

Information related to telecommunications organizations should be protected 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. Persons engaged by the telecommunications organization should 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*

The installation and use of telecommunications facilities should be controlled, ensuring the authenticity, accuracy and completeness of information transmitted, relayed or received by wire, radio or any other methods.

3) *Availability*

Only authorized access should be provided when necessary to telecommunications information, facilities and the medium used for the provision of communication services whether it might be provided by wire, radio or any other methods. As an extension of the availability, telecommunications organizations should give priority to essential communications in case of emergency, and comply with regulatory requirements.

Information security management in telecommunications organizations is required regardless of the method, e.g., wired, wireless or broadband technologies. If information security management is not implemented properly, the extent of telecommunications risks regarding confidentiality, integrity and availability may be increased.

Telecommunications organizations are designated to provide telecommunications services by intermediating communications of others through facilities for the use of others communications. Therefore, it should be taken into account that information processing facilities within a telecommunication organization are accessed and utilized by not only its own employees and contractors, but also various users outside of the organization.

In order to provide telecommunications services, telecommunications organizations need to interconnect and/or share their telecommunications services and facilities, and/or use the telecommunications services and facilities of other telecommunications organizations. Therefore, the management of information security in telecommunications organizations is mutually dependent and may include any and all areas of network infrastructure, services applications and other facilities.

Regardless of operational scales, service areas or service types, telecommunications organizations should implement appropriate controls to ensure confidentiality, integrity, availability and any other security property of telecommunications.

Audience

This Recommendation | International Standard provides telecommunications organizations, and those responsible for information security; together with security vendors, auditors, telecommunications terminal vendors and application content providers, with 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 – Information security management
guidelines for telecommunications organizations based on ISO/IEC 27002****1 Scope**

The scope of this Recommendation | International Standard is to define guidelines supporting the implementation of information security management 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 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements.*
- ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management.*