INTERNATIONAL STANDARD

ISO/IEC 27011

First edition
2008-12-15

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

Reference number
ISO/IEC 27011:2008(E)

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

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.*