INTERNATIONAL STANDARD

ISO/IEC 27010

Second edition
2015-11-15

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles

Reference number
ISO/IEC 27010:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword .... **vi**

Introduction .... **vii**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Concepts and justification **1**

4.1 Introduction 1
4.2 Information sharing communities 2
4.3 Community management 2
4.4 Supporting entities 2
4.5 Inter-sector communication 2
4.6 Conformity 3
4.7 Communications model 4

5 Information security policies **4**

5.1 Management direction for information security 4
5.1.1 Policies for information security 4
5.1.2 Review of the policies for information security 5

6 Organization of information security **5**

7 Human resource security **5**

7.1 Prior to employment 5
7.1.1 Screening 5
7.1.2 Terms and conditions of employment 5
7.2 During employment 5
7.3 Termination and change of employment 5

8 Asset management **5**

8.1 Responsibility for assets 5
8.1.1 Inventory of assets 5
8.1.2 Ownership of assets 5
8.1.3 Acceptable use of assets 6
8.1.4 Return of assets 6
8.2 Information classification 6
8.2.1 Classification of information 6
8.2.2 Labelling of information 6
8.2.3 Handling of assets 6
8.3 Media handling 6
8.4 Information exchanges protection 7
8.4.1 Information dissemination 7
8.4.2 Information disclaimers 7
8.4.3 Information credibility 7
8.4.4 Information sensitivity reduction 8
8.4.5 Anonymous source protection 8
8.4.6 Anonymous recipient protection 8
8.4.7 Onwards release authority 9

9 Access control **9**

10 Cryptography **9**

10.1 Cryptographic controls 9
10.1.1 Policy on the use of cryptographic controls 9
10.1.2 Key management 9

11 Physical and environmental security **9**

12 Operations security **9**
12.1 Operational procedures and responsibilities 9
12.2 Protection from malware 10
12.2.1 Controls against malware 10
12.3 Backup 10
12.4 Logging and monitoring 10
12.4.1 Event logging 10
12.4.2 Protection of log information 10
12.4.3 Administrator and operator logs 10
12.4.4 Clock synchronization 10
12.5 Control of operational software 10
12.6 Technical vulnerability management 10
12.7 Information systems audit considerations 10
12.7.1 Information systems audit controls 10
12.7.2 Community audit rights 10

13 Communications security **11**
13.1 Network security management 11
13.2 Information transfer 11
13.2.1 Information transfer policies and procedures 11
13.2.2 Agreements on information transfer 11
13.2.3 Electronic messaging 11
13.2.4 Confidentiality or non-disclosure agreements 11

14 System acquisition, development and maintenance **11**

15 Supplier relationships **12**
15.1 Information security in supplier relationships 12
15.1.1 Information security policy for supplier relationships 12
15.1.2 Addressing security within supplier agreements 12
15.1.3 Information and communication technology supply chain 12
15.2 Supplier service delivery management 12

16 Information security incident management **12**
16.1 Management of information security incidents and improvements 12
16.1.1 Responsibilities and procedures 12
16.1.2 Reporting information security events 12
16.1.3 Reporting information security weaknesses 13
16.1.4 Assessment of, and decision on, information security events 13
16.1.5 Response to information security incidents 13
16.1.6 Learning from information security incidents 13
16.1.7 Collection of evidence 13
16.1.8 Early warning system 13

17 Information security aspects of business continuity management **13**
17.1 Information security continuity 13
17.1.1 Planning information security continuity 13
17.1.2 Implementing information security continuity 14
17.1.3 Verify, review and evaluate information security continuity 14
17.2 Redundancies 14

18 Compliance **14**
18.1 Compliance with legal and contractual requirements 14
18.1.1 Identification of applicable legislation and contractual requirements 14
18.1.2 Intellectual property rights 14
18.1.3 Protection of records 14
18.1.4 Privacy and protection of personally identifiable information 14
18.1.5 Regulation of cryptographic controls 14
18.1.6 Liability to the information sharing community 14
18.2 Information security reviews 15

Annex A (informative) **Sharing sensitive information** **16**

Annex B (informative) **Establishing trust in information exchanges** 21
Annex C (informative) **The Traffic Light Protocol** 25
Annex D (informative) **Models for organizing an information sharing community** 26
Bibliography 32

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.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27010:2012), which has been revised for compatibility with ISO/IEC 27001:2013 and ISO/IEC 27002:2013.

Introduction

This International Standard is a sector-specific supplement to ISO/IEC 27001:2013 and ISO/IEC 27002:2013 for use by information sharing communities. The guidelines contained within this International Standard are in addition to, and complement, the generic guidance given within other members of the ISO/IEC 27000 family of standards.

ISO/IEC 27001:2013 and ISO/IEC 27002:2013 address information exchange between organizations, but they do so in a generic manner. When organizations wish to communicate sensitive information to multiple other organizations, the originator must have confidence that its use in those other organizations will be subject to adequate security controls implemented by the receiving organizations. This can be achieved through the establishment of an information sharing community, where each member trusts the other members to protect the shared information, even though the organizations may otherwise be in competition with each other.

An information sharing community cannot work without trust. Those providing information must be able to trust the recipients not to disclose or to act upon the data inappropriately. Those receiving information must be able to trust that information is accurate, subject to any qualifications notified by the originator. Both aspects are important, and must be supported by demonstrably effective security policies and the use of good practice. To achieve this, the community members must all implement a common management system covering the security of the shared information. This is an information security management system (ISMS) for the information sharing community.

In addition, information sharing can take place between information sharing communities where not all recipients will be known to the originator. This will only work if there is adequate trust between the communities and their information sharing agreements. It is particularly relevant to the sharing of sensitive information between diverse communities, such as different industry or market sectors.

Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications

1 Scope

This International Standard provides guidelines in addition to the guidance given in the ISO/IEC 27000 family of standards for implementing information security management within information sharing communities.

This International Standard provides controls and guidance specifically relating to initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications. It provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods.

This International Standard is applicable to all forms of exchange and sharing of sensitive information, both public and private, nationally and internationally, within the same industry or market sector or between sectors. In particular, it may be applicable to information exchanges and sharing relating to the provision, maintenance and protection of an organization's or nation state's critical infrastructure. It is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls*