INTERNATIONAL STANDARD

ISO/IEC 27010

First edition
2012-04-01

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 27010:2012(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 in Switzerland

Contents

Page

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 27010 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

This International Standard is a supplement to ISO/IEC 27001:2005 and ISO/IEC 27002:2005 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.

Whereas ISO/IEC 27001:2005 and ISO/IEC 27002:2005 address information exchange between organizations, 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 the 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.

This International Standard provides guidelines and general principles on how the specified requirements can be met using established messaging and other technical methods. It is designed to support the creation of trust when exchanging and sharing sensitive information, thereby encouraging the international growth of information sharing communities.

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

1 Scope

This International Standard provides guidelines in addition to 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.

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.

2 Normative references

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

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000 and the following apply.

3.1
information sharing community
group of organizations that agree to share information

NOTE An organization can be an individual.

3.2
trusted information communication entity
autonomous organization supporting information exchange within an information sharing community