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)

COPYRIGHT PROTECTED DOCUMENT

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

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000:2014 apply.

4 Concepts and justification

4.1 Introduction

ISMS guidance specific to inter-sector and inter-organizational communications has been identified in Clauses 5 to 18 of this International Standard.

ISO/IEC 27002:2013 defines controls that cover the exchange of information between organizations on a bilateral basis, and also controls for the general distribution of publicly available information. However, in some circumstances there exists a need to share information within a community of organizations where the information is sensitive in some way and cannot be made publicly available other than to

members of the community. Often the information can only be made available to certain individuals within each member organization, or may have other security requirements such as anonymization of information. This International Standard defines additional potential controls and provides additional guidance and interpretation of ISO/IEC 27001:2013 and ISO/IEC 27002:2013 in order to meet these requirements.

There are four informative annexes. Annex A describes the potential benefits from sharing sensitive information between organizations. Annex B provides guidance on how members of an information sharing community can assess the degree of trust that can be placed in information provided by other members. Annex C describes the Traffic Light Protocol, a mechanism widely used in information sharing communities to indicate the permitted distribution of information. Annex D contains some examples of models for organizing an information sharing community.

4.2 Information sharing communities

To be effective, information sharing communities must have some common interest or other relationship to define the scope of the shared sensitive information. For example, communities may be market sector specific, and limit membership to organizations within that one sector. Of course, there may be other bases for common interest, for example, geographical location or common ownership.

There must also be trust between members, in particular that all members will follow the information sharing agreement.

4.3 Community management

Information sharing communities will be created from independent organizations or parts of organizations. There may, therefore, not be clear or uniform organizational structures and management functions applying to all members. For information security management to be effective, management commitment is necessary. Therefore, the organizational structures and management functions applying to community information security management should be clearly defined.

Differences among member organizations of an information sharing community should also be considered. The differences could include:

— differing legal or regulatory environments,

— whether member organizations already operate their own ISMS, and

— member rules on protections of assets and information disclosure.

4.4 Supporting entities

Many information sharing communities will choose to establish or appoint a centralized supporting entity to organize and support information sharing. Such an entity can provide many supporting controls such as anonymization of source and recipients more easily and efficiently than where members communicate directly.

There are a number of different organizational models that can be used to create supporting entities. Annex D describes two common models, the Trusted Information Communication Entity (TICE) and the Warning, Advice and Reporting Point (WARP).

4.5 Inter-sector communication

Many information sharing communities will be sector based, as this provides a natural scope of common interest. However, there may well be information shared by such communities that would be of interest to other information sharing communities established in other sectors. In such cases it may be possible to establish information sharing communities of information sharing communities, again based on some common interest, such as the nature of the shared information. We refer to this as inter-sector communication.

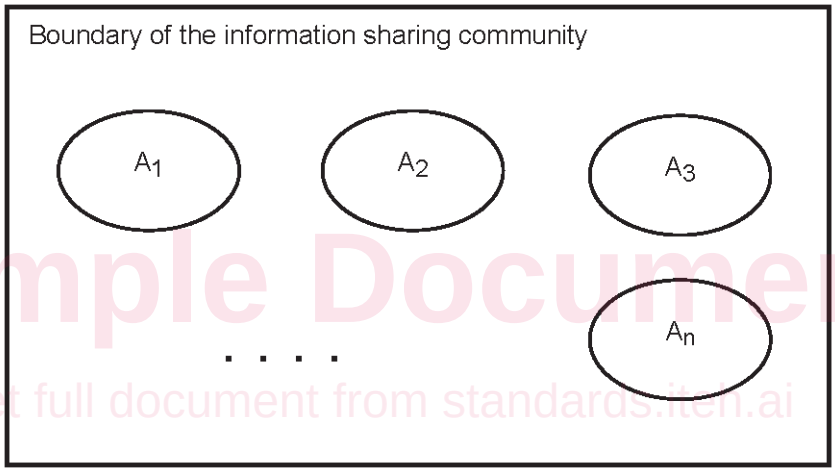
Inter-sector communication is greatly facilitated where supporting entities exist within each information sharing community, as the necessary information exchange agreements and controls can then be established between the supporting entities, rather than between all members of all communities. Some inter-sector communities will require anonymization of the source or recipient organizations; this also can be achieved by use of supporting entities.

4.6 Conformity

There are a number of places where ISO/IEC 27001:2013 will need to be interpreted when applied to an information sharing community (or, for inter-sector communication, a community of communities).

The first area where interpretation is required is the definition of the organization concerned.

ISO/IEC 27001:2013 requires that an ISMS is established, implemented, maintained and continually improved by an organization (ISO/IEC 27001:2013, 4.4). In this context, the relevant organization is the information sharing community. However, the members of the information sharing community will themselves be organizations – see Figure 1.



Key

A_k Member organization k of the community (k = 1 ... n), including any supporting entity.

Figure 1 — Communities and organizations

Secondly, in many information sharing communities, not all persons within the member organizations will be permitted access to the sensitive information shared between members. In this case, part of the member organization will be within scope of the community ISMS and part will be outside. The part outside the community scope will only have access to community information if it is marked for wider release – see Figure 2.

It is possible that members of the information sharing community may have their own information security management systems and, in consequence, some processes might fall within scope of both the community and members' management systems. In this case, there is at least a theoretical possibility that there might be conflicting and incompatible requirements upon those processes. This might be an issue justifying exclusion from the scope of the member's ISMS – see ISO/IEC 27001:2013, 4.3.

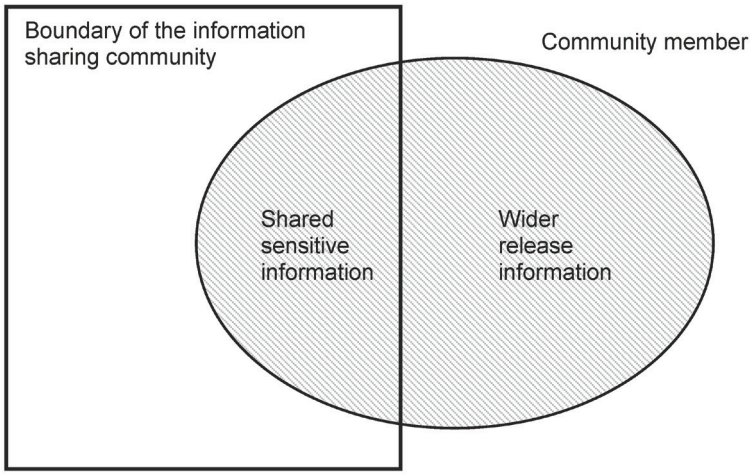


Figure 2 — Member ISMS partially in scope

When defining its risk assessment process (ISO/IEC 27001:2013, 6.1.2), the information sharing community will need to recognize that the impact of risks may be different on different members of the community. The community will, therefore, need to choose a risk assessment methodology that can handle non-uniform impact, and similarly for its risk assessment criteria.

4.7 Communications model

Communications of sensitive information as covered by this International Standard can take any form – written, verbal or electronic – provided that the selected control requirements are met.

In the remainder of this International Standard, individual sensitive communications are described in terms of the following participants:

— The *source* of an item of information is the person or organization that originates an item of information; the source does not need to be a member of the community.

— The *originator* is the member of an information sharing community that initiates its distribution within the community. The originator may distribute the information directly, or send it to a supporting entity for distribution. The originator may, but need not be, the same as the source of the information; the originator may conceal the identity of the source. Communities may provide facilities to enable a member to conceal its own identity as the originator.

— A *recipient* is a receiver of information distributed within the community. Recipients need not be members of the community if the information is identified as available for wider distribution. Communities may provide facilities to enable recipients to conceal their identities from the originators of information.

5 Information security policies

5.1 Management direction for information security

5.1.1 Policies for information security

ISO/IEC 27002:2013, control 5.1.1 is augmented as follows:

Implementation guidance

An information sharing policy should define how the community members will work together to set security management policies and direction for the information sharing community. It should be made