BS ISO/IEC 27010:2012

BSI Standards Publication

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

bsi.

...making excellence a habit.™

Document Sharing Hub

National foreword

This British Standard is the UK implementation of ISO/IEC 27010:2012.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2012. Published by BSI Standards Limited 2012

ISBN 978 0 580 68032 8

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 April 2012.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27010:2012

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)

Documents
Document Sharing Hub

© ISO/IEC 2012

Full document details: BS ISO/IEC 27010:2012

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2012

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 in Switzerland

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27010:2012

Contents

Page

Foreword vi

Introduction vii

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Concepts and justification 2
4.1 Introduction 2
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 Security policy 5
5.1 Information security policy 5
5.1.1 Information security policy document 5
5.1.2 Review of the information security policy 5

6 Organization of information security 5
6.1 Internal organization 5
6.2 External parties 5
6.2.1 Identification of risks related to external parties 5
6.2.2 Addressing security when dealing with customers 5
6.2.3 Addressing security in third party agreements 5

7 Asset management 6
7.1 Responsibility for assets 6
7.1.1 Inventory of assets 6
7.1.2 Ownership of assets 6
7.1.3 Acceptable use of assets 6
7.2 Information classification 6
7.2.1 Classification guidelines 6
7.2.2 Information labelling and handling 6
7.3 Information exchanges protection 7
7.3.1 Information dissemination 7
7.3.2 Information disclaimers 7
7.3.3 Information credibility 8
7.3.4 Information sensitivity reduction 8
7.3.5 Anonymous source protection 8
7.3.6 Anonymous recipient protection 9
7.3.7 Onwards release authority 9

8 Human resources security 9
8.1 Prior to employment 9
8.1.1 Roles and responsibilities 9
8.1.2 Screening 9
8.1.3 Terms and conditions of employment 9
8.2 During employment 10
8.3 Termination or change of employment 10

9 Physical and environmental security 10

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 27010:2012

10 Communications and operations management 10
10.1 Operational procedures and responsibilities 10
10.2 Third party service delivery management....10
10.3 System planning and acceptance 10
10.4 Protection against malicious and mobile code 10
10.4.1 Controls against malicious code 10
10.4.2 Controls against mobile code 10
10.5 Back-up 10
10.6 Network security management....11
10.7 Media handling....11
10.8 Exchange of information....11
10.8.1 Information exchange policies and procedures....11
10.8.2 Exchange agreements....11
10.8.3 Physical media in transit....11
10.8.4 Electronic messaging....11
10.8.5 Business information systems....11
10.9 Electronic commerce services 11
10.10 Monitoring 11
10.10.1 Audit logging....11
10.10.2 Monitoring system use....12
10.10.3 Protection of log information 12
10.10.4 Administrator and operator logs....12
10.10.5 Fault logging 12
10.10.6 Clock synchronisation 12

11 Access control 12

12 Information systems acquisition, development and maintenance....12
12.1 Security requirements of information systems 12
12.2 Correct processing in applications....12
12.3 Cryptographic controls 12
12.3.1 Policy on the use of cryptographic controls 12
12.3.2 Key management 12
12.4 Security of system files....13
12.5 Security in development and support processes 13
12.6 Technical vulnerability management....13

13 Information security incident management 13
13.1 Reporting information security events and weaknesses 13
13.1.1 Reporting information security events....13
13.1.2 Reporting security weaknesses 13
13.1.3 Early warning system 13
13.2 Management of information security incidents and improvements....14
13.2.1 Responsibilities and procedures 14
13.2.2 Learning from information security incidents 14
13.2.3 Collection of evidence....14

14 Business continuity management 14
14.1 Information security aspects of business continuity management 14
14.1.1 Including information security in the business continuity management process 14
14.1.2 Business continuity and risk assessment 14
14.1.3 Developing and implementing continuity plans including information security....14
14.1.4 Business continuity planning framework 15
14.1.5 Testing, maintaining and re-assessing business continuity plans....15

15 Compliance....15
15.1 Compliance with legal requirements 15
15.1.1 Identification of applicable legislation 15
15.1.2 Intellectual property rights (IPR)....15
15.1.3 Protection of organizational records....15
15.1.4 Data protection and privacy of personal information....15
15.1.5 Prevention of misuse of information processing facilities 15

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 27010:2012

15.1.6 Regulation of cryptographic controls **15**
15.1.7 Liability to the information sharing community **15**
15.2 Compliance with security policies and standards, and technical compliance **16**
15.3 Information systems audit considerations **16**
15.3.1 Information systems audit controls **16**
15.3.2 Protection of information systems audit tools **16**
15.3.3 Audit of community functions **16**

Annex A (informative) **Sharing sensitive information** **17**

Annex B (informative) **Establishing trust in information exchanges** **22**

Annex C (informative) **The Traffic Light Protocol** **27**

Annex D (informative) **Models for organizing an information sharing community** **28**

Bibliography **34**

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

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*.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

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.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

Documents
Document Sharing Hub

INTERNATIONAL STANDARD ISO/IEC 27010:2012(E)

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

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

4 Concepts and justification

4.1 Introduction

ISMS guidance specific to inter-sector and inter-organizational communications has been identified in Clauses 5 to 15 below.

ISO/IEC 27002:2005 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 anonymisation of information. This International Standard defines additional potential controls and provides additional guidance and interpretation of ISO/IEC 27001:2005 and ISO/IEC 27002:2005 in order to meet these requirements.

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.

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:

— 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 centralised supporting entity to organize and support information sharing. Such an entity can provide many supporting controls such as anonymisation 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 to this International Standard describe 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.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

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 anonymisation of the source or recipient organizations; this also can be achieved by use of supporting entities.

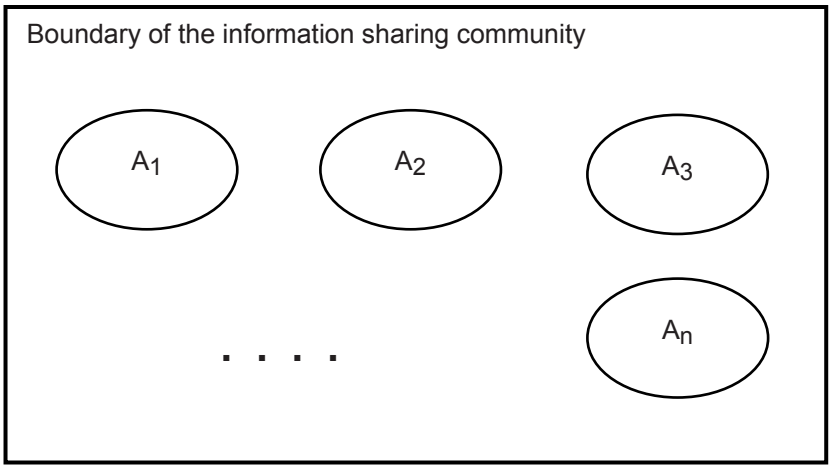
4.6 Conformity

Any information security management system (ISMS) created and operated in accordance with ISO/IEC 27001:2005 and using controls from ISO/IEC 27002:2005, this International Standard and other sources can be assessed for conformity against ISO/IEC 27001:2005, without modification or addition to that International Standard.

However, there are a number of places where ISO/IEC 27001:2005 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 27001:2005 requires that an ISMS is established by an organization and operates within the context of its overall business activities and the risks that it faces (ISO/IEC 27001:2005, 4.1). 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.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

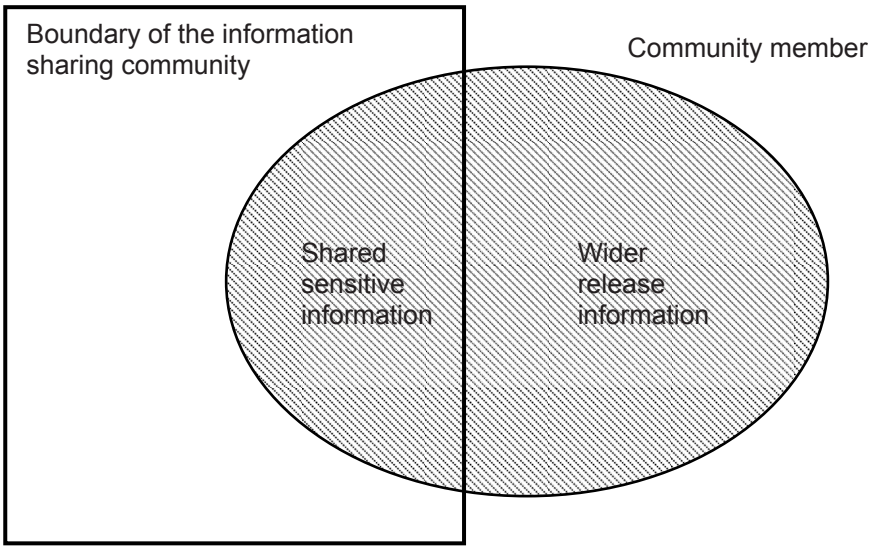


Figure 2 — Member partially in scope

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 would be a case where exclusion from the scope of the member's ISMS might be justified – see ISO/IEC 27001:2005, 4.2.1 a).

When defining its risk assessment approach (ISO/IEC 27001:2005, 4.2.1 c), the information sharing community will need to recognise 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, similarly for its risk assessment criteria.

Measuring the effectiveness of the selected controls (ISO/IEC 27001:2005, 4.2.3 c) will need the participation of all members of the information sharing community. All members will need to provide regular feedback to information providers and the community as a whole concerning the effectiveness of the controls in their own environment.

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.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27010:2012

5 Security policy

5.1 Information security policy

5.1.1 Information security policy document

Control 5.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

The information security policy document 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 available to all employees involved in information sharing within the community. The policy may restrict its dissemination to other employees of community members.

The information security policy document should define the information marking and distribution policy used within the community.

5.1.2 Review of the information security policy

Control 5.1.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

The input to the management review should include information on significant changes to membership of the information sharing community.

6 Organization of information security

6.1 Internal organization

No additional information specific to inter-sector or inter-organizational communications.

6.2 External parties

6.2.1 Identification of risks related to external parties

No additional information specific to inter-sector or inter-organizational communications.

6.2.2 Addressing security when dealing with customers

No additional information specific to inter-sector or inter-organizational communications.

6.2.3 Addressing security in third party agreements

Control 6.2.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

All community members should be made aware of the identities of all third parties involved in the provision of community services, in case they have objections to particular parties being involved in the handling of information that they provide.

The agreements with vendors and service providers associated with provision of community services should enable security reviews and audits of their services to be performed on a regular basis.

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 27010:2012