BS ISO/IEC 27033-2:2012

Incorporating corrigendum September 2015

BSI Standards Publication

Information technology - Security techniques - Network security

Part 2: Guidelines for the design and implementation of network security

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27033-2:2012

National foreword

This British Standard is the UK implementation of ISO/IEC 27033-2:2012. It supersedes BS ISO/IEC 18028-2:2006 which is withdrawn.

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 2015. Published by BSI Standards Limited 2015

ISBN 978 0 580 91637 3

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 31 August 2012.

Amendments/corrigenda issued since publication

Date	Text affected
30 September 2015	Implementation of ISO corrected text 15 August 2012: Title and cover page updated.

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-2:2012

INTERNATIONAL STANDARD

ISO/IEC 27033-2

First edition
2012-08-01

Corrected version
2012-08-15

Information technology — Security techniques — Network security

Part 2: Guidelines for the design and implementation of network security

Technologies de l'information — Techniques de sécurité — Sécurité de réseau

Partie 2: Lignes directrices pour la conception et l'implémentation de la sécurité de réseau

Reference number
ISO/IEC 27033-2:2012(E)

Documents
Document Sharing Hub
© ISO/IEC 2012

Full document details: BS ISO/IEC 27033-2:2012

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 27033-2:2012

Contents

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviations 2

5 Document structure 2

6 Preparing for design of network security 3
6.1 Introduction 3
6.2 Asset identification 3
6.3 Requirements collection 3
6.3.1 Legal and regulatory requirements 3
6.3.2 Business requirements 4
6.3.3 Performance requirements 4
6.4 Review requirements 4
6.5 Review of existing designs and implementations 5

7 Design of network security 5
7.1 Introduction 5
7.2 Design principles 6
7.2.1 Introduction 6
7.2.2 Defence in depth 6
7.2.3 Network Zones 7
7.2.4 Design resilience 7
7.2.5 Scenarios 8
7.2.6 Models and Frameworks 8
7.3 Design Sign off 8

8 Implementation 8
8.1 Introduction 8
8.2 Criteria for Network component selection 9
8.3 Criteria for product or vendor selection 9
8.4 Network management 10
8.5 Logging, monitoring and incident response 11
8.6 Documentation 11
8.7 Test plans and conducting testing 11
8.8 Sign off 12

Annex A (informative) Cross-references between ISO/IEC 27001:2005/ISO/IEC 27002:2005 network security related controls and ISO/IEC 27033-2:2012 clauses 13

Annex B (informative) Example documentation templates 14
B.1 An example network security architecture document template 14
B.1.1 Introduction 14
B.1.2 Business related requirements 14
B.1.3 Technical architecture 14
B.1.4 Network services 17
B.1.5 Hardware/physical layout 17
B.1.6 Software 18
B.1.7 Performance 19
B.1.8 Known issues 19
B.1.9 References 19

Documents
Document Sharing Hub

© ISO/IEC 2012 – All rights reserved

Full document details: BS ISO/IEC 27033-2:2012

B.1.10 Appendices 20
B.1.11 Glossary 20
B.2 An example template for a Functional Security requirements document 20
B.2.1 Introduction 20
B.2.2 Firewall configuration 21
B.2.3 Security risks 21
B.2.4 Security management 22
B.2.5 Security administration 22
B.2.6 Authentication and access control 22
B.2.7 (Audit) Logging 23
B.2.8 Information Security incident management 23
B.2.9 Physical security 23
B.2.10 Personnel security 23
B.2.11 Appendices 23
B.2.12 Glossary 23

Annex C (informative) ITU-T X.805 framework and ISO/IEC 27001:2005 control mapping 24

Bibliography 28

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012

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 27033-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This first edition of ISO/IEC 27033-2 cancels and replaces ISO/IEC 18028-2:2006, which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference networking scenarios – Threats, design techniques and control issues*

The following parts are under preparation:

— *Part 4: Securing communications between networks using security gateways*

— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*

Securing IP network access using wireless will form the subject of a future Part 6.

Further parts may follow because of the ever-changing and evolving technology in the network security area.

This corrected version of ISO/IEC 27033-2:2012 corrects the title on the cover page and on page 1.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-2:2012

Information technology — Security techniques — Network security

Part 2:
Guidelines for the design and implementation of network security

1 Scope

This part of ISO/IEC 27033 gives guidelines for organizations to plan, design, implement and document network security.

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 7498 (all parts), *Information technology — Open Systems Interconnection — Basic Reference Model*

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*

ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, and ISO/IEC 27033-1 apply.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012

4 Abbreviations

For the purposes of this document, the abbreviations used in ISO/IEC 27033-1 and the following are applicable.

IPS	Intrusion Prevention System
POC	Proof of Concept
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service
SMS	Simple Message Service
SMTP	Simple Mail Transfer Protocol
TACACS	Terminal Access Controller Access-Control System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

5 Document structure

The structure of ISO/IEC 27033-2 comprises:

- Preparing for Design of Network Security
  - Introduction
  - Asset Identification
  - Requirements collection
  - Review of requirements
  - Review of existing designs and implementations
- Design of Network Security
  - Introduction
  - Design principles
  - Design Signoff
- Implementation
  - Introduction
  - Criteria for network component selection
  - Criteria for product or vendor selection

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012

- Network management
- Logging, monitoring and incident response
- Documentation
- Test Plans and Conducting Testing
- Sign off

6 Preparing for design of network security

6.1 Introduction

The objectives of network security are to enable the information flows that enhance an organisation's business processes, and to prevent information flows that degrade an organisation's business processes. The preparation work for the design and the implementation of network security involves the following stages:

- Asset identification
- Requirements collection
- Review of requirements
- Evaluation of technical options and constraints
- Evaluation of existing designs and implementations

These stages should result in the early documentation consisting of all the inputs for following design and implementation steps.

6.2 Asset identification

Identification of assets is a critical first step in determining the information security risks to any network. The assets to be protected are those which would degrade the organization's business processes were they to be inappropriately disclosed, modified or unavailable. They include physical assets (servers, switches, routers, etc), and logical assets (configuration settings, executable code, data, etc). This register of assets should already exist as part of continutiy planning/Disaster recovery risk analysis. The questions that must be answered are:

- What are the distinct types of network equipment and facility groupings that need to be protected?
- What are the distinct types of network activities that need to be protected?
- What information assets and information processing capabilities need to be protected ?
- Where information assets reside in the information systems architecture?

Identifiable assets include those required to securely support management, control and user traffic and the features required for the functioning of the network infrastructure, services, and applications. These include devices such as hosts, routers, firewalls, etc, interfaces (internal and external), information stored/processed and protocols used. The protection of infrastructure assets is only part of the objective of the network security design. The principle objective is the protection of business assets such as information and business processes.

6.3 Requirements collection

6.3.1 Legal and regulatory requirements

The legal and regulatory requirements for the location and function of the network should be gathered and reviewed to ensure that the requirements are met in the design of the network. Particular care should be taken where information flows across jurisdictional or regulatory boundaries. In such cases, the requirements of both sides of the boundary must be recorded.

© ISO/IEC 2012 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012

6.3.2 Business requirements

The organization's business processes and data classification types determine its access requirements. The network should be configured to enable this access, to and from its information assets, for suitably authorised users, and prevent all other access. Access to Information will often relate to services on open ports (for example HTTP on TCP port 80) specific hosts (such as www.example.org at IP address 10.11.12.13) particular groups of hosts (for example the 172.128.97.64/24 subnet) or particular network interface devices (such as the interface with MAC address 10:00:00:01:02:03). The organisation will need to identify those services that it provides to others, those services that it uses of others, and those services it provides internally.

6.3.3 Performance requirements

Traffic data is required to enable the configurations for the communication lines, servers and security gateways/firewalls to be documented such that on implementation a good level of service can be provided in accordance with user expectations – with no 'over-configuration' and related unnecessary costs. Information should be gathered on such as the speeds of any existing communication links, configuration/capacity of routers at any third party locations, the number of users that will be allowed access via each link (concurrent access and number of users with access), minimum, average and maximum user connect time required, identity of what authorized users will access over the link, number of web page hits required, database access hits required, growth expected over one year and three/five years, and whether a Windows log-on is required. Use could be made of telecommunications table (queuing) theory for sizing the number of ports, channels required, particularly over dial-up links. These performance requirements should be reviewed, queries resolved and the performance criteria required to be met by the technical architecture and related technical security architecture formally agreed.

6.4 Review requirements

A review of the current capabilities and any planned technical network architecture changes needs to be done and compared to the technical security architecture being developed to note any incompatibilities. Any incompatibilities need to then be reviewed and the appropriate architectures modified.

The information to be gathered during the review should include at a minimum the following:

- identification of the type(s) of network connection to be used,
- determination of the security risks,
- development of the list of required technical security architecture and security controls,
- network protocols to be used,
- network applications used on different aspects of the network

The information gathered should be in the context of the network capabilities. Detail should be obtained of the relevant network architecture and this shall be reviewed to provide the necessary understanding and context for process steps that follow. By clarifying these aspects at the earliest possible stage, the process of identifying the relevant security requirement identification criteria, identifying control areas, and reviewing the technical security architecture options and deciding which one shall be adopted, should become more efficient and eventually result in more workable security solution. For example it may be that because of the location there is only one conduit for all network connections to be established through, so even if a security control might be to have different conduits for redundant connections, that is not possible based on the location picked. Other controls may have to be determined then to find the best way to protect the network connections.

The consideration of network and application architectural aspects at an early stage should allow time for those architectures to be reviewed and possibly revised if an acceptable security solution cannot be realistically achieved within the current architecture.

© ISO/IEC 2012 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-2:2012