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)

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 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.

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.

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

- 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.

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.

6.5 Review of existing designs and implementations

The review of the existing security controls must be conducted in the light of the results from a security risk assessment and management review (details on risk management can be found in ISO/IEC 27005). The results of the security risk assessment may indicate which security controls are required commensurate with the assessed threats. A gap analysis will need to be completed against the current network security architecture to determine what is not addressed in the existing network security architecture.

The network security architecture should encompass the existing security controls and any missing or new security controls.

7 Design of network security

7.1 Introduction

The network security architecture exists to restrict traffic flowing between different trust domains. The most obvious boundary between trust domains is the interface between an organization's internal network and the outside world. An organisation of any significant size will also have boundaries between internal trust domains which must be identified and controlled. The network security architecture includes a description of the interfaces between an organization's/community's internal network and the outside world. Reflecting the requirements mentioned in clause 6.4 above and addressing how to protect the organization from the common threats and vulnerabilities as described in ISO/IEC 27033-1.

Guidance on general best practice design is provided in clause 7.2 below, and guidance on the network security architecture aspects related to specific networking technologies to address the requirements of today and the near future is provided in ISO/IEC 27033-4 and onward. Guidance on specific scenarios that are possible for an organization are covered in ISO/IEC 27033-3.

Technical assumptions made during the requirements gathering should be documented, for example:

- only authorized IP communications should be allowed (firewalls normally only support IP communications, and if any other protocols were allowed then it could be difficult to manage them);
- if non-IP protocols are a requirement then they should be dealt with either outside the security architecture or by tunnelling the protocol.

A network security architecture would normally encompass services, such as the following but not limited to these:

- identification and authentication (passwords, tokens, smartcards, certificates, RAS/RADIUS/terminal access controller access control system plus (TACACS+), etc.);
- logical access controls (single sign on, role based access control, trusted databases, application controls, firewalls, proxy devices, etc.);
- security audit and accounting (audit logs, audit log analysis facilities, intrusion detection facilities, write once read many (WORM) devices, etc.);
- assured storage clearance/secure deletion (provable 'wipe' facilities);
- security testing (vulnerability scanning, network 'sniffing', penetration testing, etc.);
- secure development environment (separate development and test environments, no compilers, etc.);
- software change control (configuration management software, version control, etc.);
- secure software distribution (digital signing, SSL, transport Layer security (TLS) (RFC 5246), etc.);

- secure maintenance and availability (good back-up/restore facilities, resilience, clustering, data vaults, diverse communications, etc.);

- transmission security (use of transport encryption, spread spectrum technology, Wireless LANS (WLANs), VPNs/extranets.

7.2 Design principles

7.2.1 Introduction

Common risk areas associated with networking security architectures are design failures due to poor design and/or the lack of appropriate consideration of business continuity planning or the design does not correspond to the current or expected threat level. Fundamental elements are needed to develop network security architectures that encompass all the identified security controls and business requirements. Most of these elements can be covered by general network security design best practices. ISO/IEC 27033-4 and onward cover design and implementation in detail on some aspects of the network technical security architecture best practices. Additional detailed guidance on best practice implementations can be found in other publications.

The following sections provide general guidance on design best practices to be followed when considering a network security architecture.

7.2.2 Defence in depth

Organizations need to look at security not just from one perspective, but as a pervasive layered approach. Security must be comprehensive across all network layers. Adopting a layered approach is considered to be defence in depth. The components of security are a combination of policy, design, management and technology. Each organization needs to determine its needs and design a defence in depth based upon those needs.

Many mobile devices have USB and network connectivity, as well as wireless capability. These devices can be connected to the internal network or systems on it in an ad-hoc manner; should this be done with the device's wireless connectivity open and unsecured, these devices could act as a rogue wireless access point on the internal network, bypassing the perimeter controls. Strict policies should be in place to restrict the connection of unsecured mobile devices to the network, and routine scanning of the wireless channels should be done to detect any rogue access points.

Any wireless access points should be in a DMZ. Those that are in the internal network should have strict connections settings: the strongest security (WPA2 where possible), and MAC address filtering to restrict the devices that can connect to it to those that are authorised. ISO/IEC 27033-3 provides more details on the threats presented by mobile communications technology and the relevant controls.

The defense in depth principle represents the use of multiple security controls or security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment. Different security products from multiple vendors may be deployed to defend different potential vectors within the network, helping prevent a shortfall in any one defence leading to a wider failure; also known as a "layered approach"

Figure 1 shows how there is perimeter security, with a more finer grain for infrastructure security, still more finer for the hosts, then applications and finally data. All of the layers are to protect the data.