INTERNATIONAL STANDARD

ISO/IEC 27033-1

First edition
2009-12-15

Information technology — Security techniques — Network security —

Part 1: Overview and concepts

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

Partie 1: Vue d'ensemble et concepts

Reference number
ISO/IEC 27033-1:2009(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

COPYRIGHT PROTECTED DOCUMENT

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

This first edition of ISO/IEC 27033-1 cancels and replaces ISO/IEC 18028-1:2006.

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

— *Part 1: Guidelines for network security*

The following parts are under preparation:

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

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

Risks, design techniques and control issues for

— securing communications between networks using security gateways,

— securing virtual private networks,

— IP convergence, and

— wireless networks

will form the subject of future parts.

Introduction

In today's world, the majority of both commercial and government organizations have their information systems connected by networks (see Figure 1), with the network connections being one or more of the following:

— within the organization,

— between different organizations,

— between the organization and the general public.

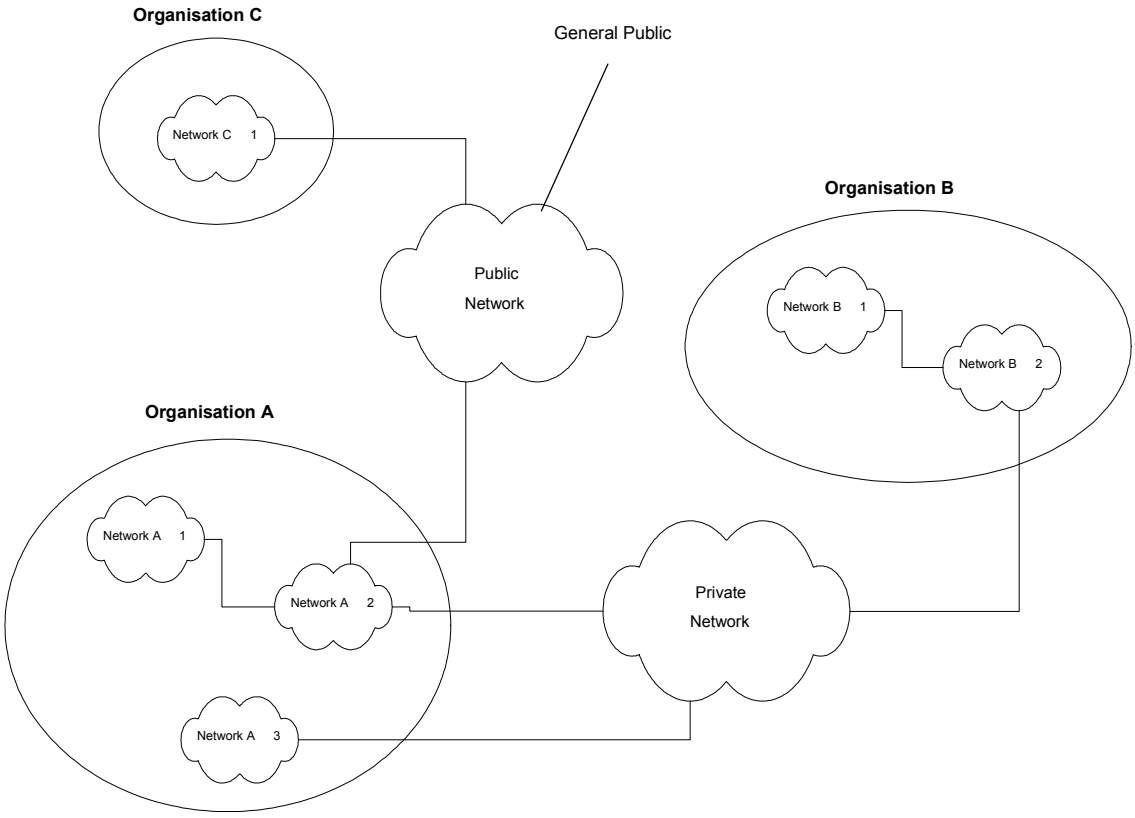

Figure 1 — Broad types of network connection

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet service providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Additionally, the new technology (including the integration of data,

voice and video) increases the opportunities for remote working (also known as “teleworking” or “telecommuting”) that enable personnel to operate away from their home work base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.

However, whilst this environment does facilitate significant business benefits, there are new security risks to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. In other words: *implementing and maintaining adequate network security is absolutely critical to the success of any organization’s business operations.*

In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.

The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this International Standard to meet their specific requirements. Its main objectives are as follows.

— ISO/IEC 27033-1, *Overview and concepts,* to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security risks and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the risk, design and control aspects associated with typical network scenarios and network “technology” areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033).

— ISO/IEC 27033-2, *Guidelines for the design and implementation of network security,* to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their business environments, using a consistent approach to the planning, design and implementation of network security, as relevant, aided by the use of models/frameworks (in this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design), and is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-3, *Risks, design techniques and control issues for reference network scenarios*, to define the specific risks, design techniques and control issues associated with typical network scenarios. It is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

It is proposed that future parts of ISO/IEC 27033 will address the following topics.

— ISO/IEC 27033-4, *Risks, design techniques and control issues for securing communications between networks using security gateways*, to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

— SO/IEC 27033-5, *Risks, design techniques and control issues for securing virtual private networks,* to define the specific risks, design techniques and control issues for securing connections that are established using virtual private networks (VPNs). It will be relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-6, *IP convergence*, to define the specific risks, design techniques and control issues for securing IP convergence networks, i.e. those with the convergence of data, voice and video. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for IP convergence networks (for example network architects and designers, network managers, and network security officers).

— ISO/IEC 27033-7, *Wireless*, to define the specific risks, design techniques and control issues for securing wireless and radio networks. It will be relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless and radio networks (for example network architects and designers, network managers, and network security officers).

It is emphasized that ISOI/IEC 27033 provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

If there are other parts in the future, these will be relevant to all personnel who are involved in the detailed planning, design and implementation of the network aspects covered by those parts (for example network architects and designers, network managers, and network security officers).

It should be noted that this International Standard is not a reference or normative document for regulatory and legislative security requirements. Although it emphasizes the importance of these influences, it cannot state them specifically, since they are dependent on the country, the type of business, etc.

Unless otherwise stated, throughout this part of ISO/IEC 27033 the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.