BRITISH STANDARD

BS ISO/IEC 27033-1:2009

Information technology — Security techniques — Network security

Part 1: Overview and concepts

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Documents
Document Sharing Hub
British Standards

Full document details: BS ISO/IEC 27033-1:2009

National foreword

This British Standard is the UK implementation of ISO/IEC 27033-1:2009. It supersedes BS ISO/IEC 18028-1:2006 which is withdrawn.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.

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 January 2010

© BSI 2010

ISBN 978 0 580 59492 2

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2009

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)

Documents
Document Sharing Hub
© ISO/IEC 2009

Full document details: BS ISO/IEC 27033-1:2009

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/IEC 2009

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 2009 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2009

Contents

Page

1 Scope ... 1
2 Normative references ... 2
3 Terms and definitions ... 2
4 Abbreviated terms ... 6
5 Structure ... 9
6 Overview ... 11
6.1 Background ... 11
6.2 Network Security Planning and Management ... 12
7 Identifying Risks and Preparing to Identify Security Controls ... 14
7.1 Introduction ... 14
7.2 Information on Current and/or Planned Networking ... 15
7.3 Information Security Risks and Potential Control Areas ... 19
8 Supporting Controls ... 22
8.1 Introduction ... 22
8.2 Management of Network Security ... 23
8.3 Technical Vulnerability Management ... 26
8.4 Identification and Authentication ... 27
8.5 Network Audit Logging and Monitoring ... 28
8.6 Intrusion Detection and Prevention ... 29
8.7 Protection against Malicious Code ... 29
8.8 Cryptographic Based Services ... 30
8.9 Business Continuity Management ... 31
9 Guidelines for the Design and Implementation of Network Security ... 32
9.1 Background ... 32
9.2 Network Technical Security Architecture/Design ... 32
10 Reference Network Scenarios – Risks, Design, Techniques and Control Issues ... 34
10.1 Introduction ... 34
10.2 Internet Access Services for Employees ... 34
10.3 Enhanced Collaboration Services ... 35
10.4 Business to Business Services ... 35
10.5 Business to Customer Services ... 35
10.6 Outsourcing Services ... 35
10.7 Network Segmentation ... 36
10.8 Mobile Communications ... 36
10.9 Network Support for Traveling Users ... 36
10.10 Network Support for Home and Small Business Offices ... 36
11 'Technology' Topics – Risks, Design Techniques and Control Issues ... 37
12 Develop and Test Security Solution ... 37
13 Operate Security Solution ... 38
14 Monitor and Review Solution Implementation ... 38
Annex A (informative) **'Technology' Topics – Risks, Design Techniques and Control Issues** ... 39
Annex B (informative) **Cross-references Between ISO/IEC 27001 and ISO/IEC 27002 Network Security Related Controls, and clauses within this part of ISO/IEC 27033** ... 64
Annex C (informative) **Example Template for a SecOPs Document** ... 69

Documents
Document Sharing Hub

© ISO/IEC 2009 – All rights reserved

Full document details: BS ISO/IEC 27033-1:2009

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.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

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.

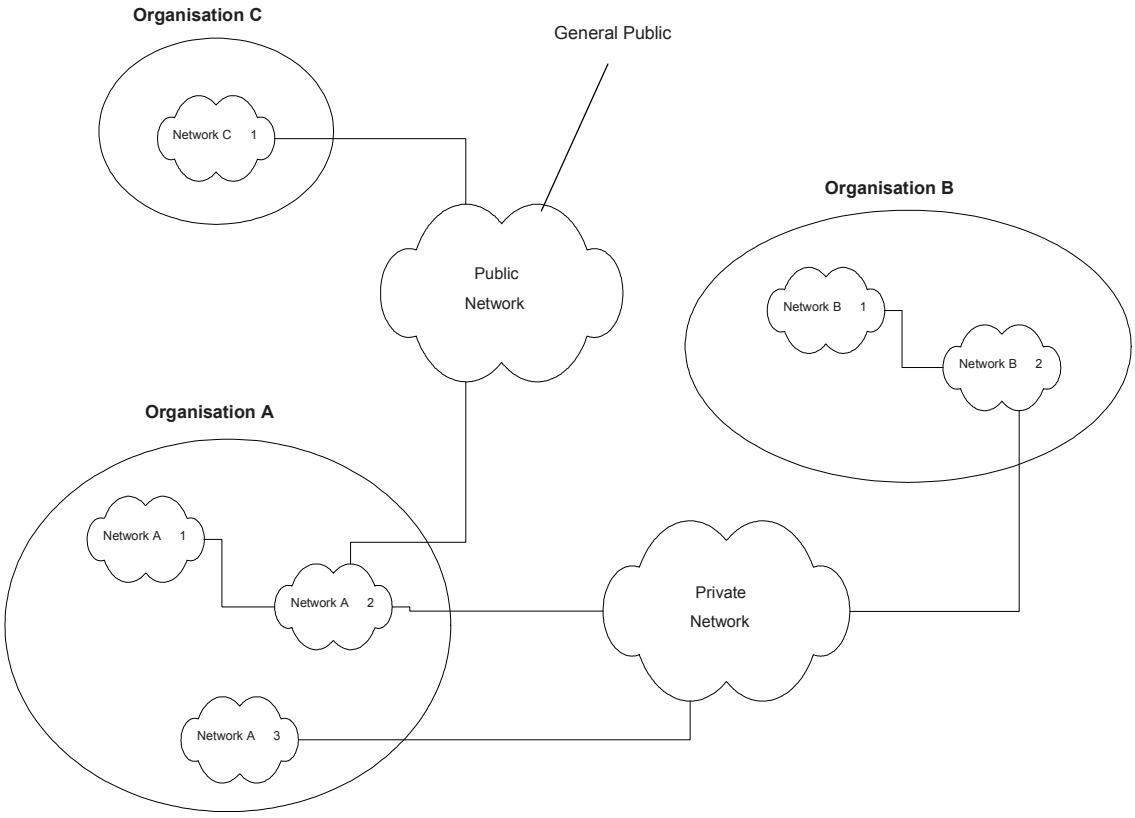


Figure 1 — Broad types of network connection

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,

Documents
Document Sharing Hub

© ISO/IEC 2009 – All rights reserved

Full document details: BS ISO/IEC 27033-1:2009

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).

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

— 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”.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2009

INTERNATIONAL STANDARD ISO/IEC 27033-1:2009(E)

Information technology — Security techniques — Network security —

Part 1: Overview and concepts

1 Scope

This part of ISO/IEC 27033 provides an overview of network security and related definitions. It defines and describes the concepts associated with, and provides management guidance on, network security. (Network security applies to the security of devices, security of management activities related to the devices, applications/services, and end-users, in addition to security of the information being transferred across the communication links.)

It is relevant to anyone involved in owning, operating or using a network. This includes senior managers and other non-technical managers or users, in addition to managers and administrators who have specific responsibilities for information security and/or network security, network operation, or who are responsible for an organization's overall security program and security policy development. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of network security.

This part of ISO/IEC 27033 also

— provides guidance on how to identify and analyse network security risks and the definition of network security requirements based on that analysis,

— provides an overview of the controls that support network technical security architectures and related technical controls, as well as those non-technical controls and technical controls that are applicable not just to networks,

— introduces how to achieve good quality network 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), and

— briefly addresses the issues associated with implementing and operating network security controls, and the on-going monitoring and reviewing of their implementation.

Overall, it provides an overview of the ISO/IEC 27033 series and a "road map" to all other parts.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

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 27005:2008, *Information technology — Security techniques — Information security risk management*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 7498, ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 and the following apply.

NOTE The following terms and definitions will also apply to future parts of ISO/IEC 27033.

3.1
alert
"instant" indication that an information system and network may be under attack, or in danger because of accident, failure or human error

3.2
architecture
fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design and evolution

[ISO/IEC 15288:2008, definition 4.5]

3.3
attacker
person deliberately exploiting vulnerabilities in technical and non-technical security controls in order to steal or compromise information systems and networks, or to compromise availability to legitimate users of information system and network resources

3.4
audit logging
recording of data on information security events for the purpose of review and analysis, and ongoing monitoring

3.5
audit tools
automated tools to aid the analysis of the contents of audit logs

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

3.6
certification authority
CA
authority trusted by one or more users to create and assign public-key certificates

NOTE 1 Optionally, the certification authority can create the users' keys.

NOTE 2 The role of the certification authority (CA) in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with an institution which provides it with information to confirm an individual's claimed identity. CAs are a critical component in information security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

3.7
corporate information security policy
document that describes management direction and support for information security in accordance with business requirements and relevant laws and regulations

NOTE The document describes the high level information security requirements that have to be followed throughout the organization.

3.8
demilitarized zone
DMZ
perimeter network (also known as a screened sub-net) inserted as a “neutral zone” between networks

3.9
denial of service
DoS
prevention of authorized access to a system resource or the delaying of system operations and functions, with resultant loss of availability to authorized users

3.10
extranet
extension of an organization's Intranet, especially over the public network infrastructure, enabling resource sharing between the organization and other organizations and individuals that it deals with by providing limited access to its Intranet

NOTE For example, an organization's customers can be provided access to some part of its Intranet, creating an extranet, but the customers cannot be considered “trusted” from a security standpoint.

3.11
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.12
firewall
type of security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass

3.13
hub
network device that functions at layer 1 of the OSI reference model

NOTE There is no real intelligence in network hubs; they only provide physical attachment points for networked systems or resources.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

3.14
the Internet
global system of inter-connected networks in the public domain

3.15
internet
collection of interconnected networks called an internetwork or just *an* internet

3.16
intranet
private computer network that uses Internet protocols and network connectivity to securely share part of an organization's information or operations with its employees

3.17
intrusion
unauthorized access to a network or a network-connected system, i.e. deliberate or accidental unauthorized access to an information system, to include malicious activity against an information system, or unauthorized use of resources within an information system

3.18
intrusion detection
formal process of detecting intrusions, generally characterized by gathering knowledge about abnormal usage patterns as well as what, how, and which vulnerability has been exploited so as to include how and when it occurred

NOTE See ISO/IEC 18043.

3.19
intrusion detection system
IDS
technical system that is used to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions in information systems and networks

NOTE See ISO/IEC 18043.

3.20
intrusion prevention
formal process of actively responding to prevent intrusions

3.21
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

NOTE See ISO/IEC 18043.

3.22
malware
malicious software designed specifically to damage or disrupt a system, attacking confidentiality, integrity and/or availability

NOTE Viruses and Trojan horses are examples of malware.

3.23
multi protocol label switching
MPLS
technique, developed for use in inter-network routing, whereby labels are assigned to individual data paths or flows, and used to switch connections, underneath and in addition to normal routing protocol mechanisms

NOTE Label switching can be used as one method of creating tunnels.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

3.24
network administration
day-to-day operation and management of network processes, and assets using networks

3.25
network analyzer
device or software used to observe and analyze information flowing in networks

NOTE Prior to the information flow analysis, information should be gathered in a specific way such as by using a network sniffer.

3.26
network element
information system that is connected to a network

3.27
network management
process of planning, designing, implementing, operating, monitoring and maintaining a network

3.28
network monitoring
process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis

3.29
network security policy
set of statements, rules and practices that explain an organization's approach to the use of its network resources, and specify how its network infrastructure and services should be protected

3.30
network sniffer
device or software used to capture information flowing in networks

3.31
port
endpoint to a connection

NOTE In the context of the Internet protocol a port is a logical channel endpoint of a TCP or UDP connection. Application protocols which are based on TCP or UDP have typically assigned default port numbers, e.g. port 80 for HTTP.

3.32
remote access
process of accessing network resources from another network, or from a terminal device which is not permanently connected, physically or logically, to the network it is accessing

3.33
remote user
user at a site other than the one at which the network resources being used are located

3.34
router
network device that is used to establish and control the flow of data between different networks by selecting paths or routes based upon routing protocol mechanisms and algorithms

NOTE 1 The networks can themselves be based on different protocols.

NOTE 2 The routing information is kept in a routing table.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

3.35
security domain
set of assets and resources subject to a common security policy

3.36
security gateway
point of connection between networks, or between subgroups within networks, or between software applications within different security domains intended to protect a network according to a given security policy

3.37
spam
unsolicited e-mails, which can carry malicious contents and/or scam messages.

3.38
spoofing
impersonating a legitimate resource or user

3.39
switch
device which provides connectivity between networked devices by means of internal switching mechanisms, with the switching technology typically implemented at layer 2 or layer 3 of the OSI reference model

NOTE Switches are distinct from other local area network interconnection devices (e.g. a hub) as the technology used in switches sets up connections on a point to point basis.

3.40
tunnel
data path between networked devices which is established across an existing network infrastructure

NOTE Tunnels can be established using techniques such as protocol encapsulation, label switching, or virtual circuits.

3.41
virtual local area network
independent network created from a logical point of view within a physical network

4 Abbreviated terms

NOTE The following abbreviated terms are used in all parts of ISO/IEC 27033.

AAA authentication, authorization and accounting

ACL access control list

ADSL asymmetric digital subscriber line

AES advanced encryption standard

ATM asynchronous transfer mode

BPL broadband power line

CA certification authority

CDPD cellular digital packet data

CDMA code division multiple access

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

CLID	calling line identifier
CLNP	connectionless network protocol
CoS	class of service
CRM	customer relationship management
DEL	direct exchange line
DES	data encryption standard
DMZ	demilitarized zone
DNS	domain name service
DPNSS	digital private network signaling system
DoS	denial of service
DSL	digital subscriber line
EDGE	enhanced data-rates for GSM evolution
EDI	electronic data interchange
EGPRS	enhanced general packet radio service
EIS	enterprise information system
FiOS	fiber optic service
FTP	file transfer protocol
FTTH	fiber to the home
GPRS	general packet radio service
GSM	global system for mobile communications
HIDS	host based intrusion detection system
HTTP	hypertext transfer protocol
IDS	intrusion detection system
IG	Implementation Guidance
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
IT	information technology
LAN	local area network
MPLS	multi-protocol label switching

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

MRP	manufacturing resource planning
NAT	network address translation
NIDS	network intrusion detection system
NTP	network time protocol
OOB	out of band
PABX	private automated branch (telephone) exchange
PC	personal computer
PDA	personal data assistant
PIN	personal identification number
PKI	public key infrastructure
PSTN	public switched telephone network
QoS	quality of service
RAID	redundant array of inexpensive disks
RAS	remote access service
RTP	real time protocol
SDSL	symmetric digital subscriber line
SecOPs	security operating procedures
SIM	subscriber identity module
SNMP	simple network management protocol
SPIT	spam over IP telephony
SSH	secure shell
TCP	transmission control protocol
TDMA	time division multiple access
TETRA	terrestrial trunked radio
TKIP	temporal key integrity protocol
UDP	user datagram protocol
UMTS	universal mobile telecommunications system
UPS	uninterruptible power supply
USB	universal serial bus
VHF	very high frequency

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

VoIP	voice over IP
VLAN	virtual local area network
VPN	virtual private network
WAN	wide area network
WAP	wireless application protocol
WEP	wired equivalent privacy
WLAN	wireless local area network
WORM	write once read many
WPA	Wi-Fi protected access
3G	third generation mobile telephone system

5 Structure

The structure of the ISOI/IEC 27033 series of standards is shown in diagrammatic, or 'road map', form in Figure 2 below.

It is noted that in Figure 2 the solid lines indicate the natural hierarchy of the Parts of ISO/IEC 27033. The dotted lines indicate that in following the processes described in (a) Part 1 – Parts 3, 4, 5, 6 and 7 may be consulted for information on security risks, and (b) Part 2 - Parts 3, 4, 5, 6 and 7 may be consulted for information on design techniques and control issues. Further, there are references in Part 3 to particular aspects covered in Parts 4, 5, 6 and 7 to avoid duplication (i.e. in using Part 3 there may be a need to consult Parts 4, 5, 6 and 7).

Thus, for any organization starting from 'scratch', or conducting a major review of existing network(s), it should first use the content of Part 1 and then Part 2, but consulting as necessary and appropriate the information on security risks, design techniques and control issues contained in Parts 3 to 7.

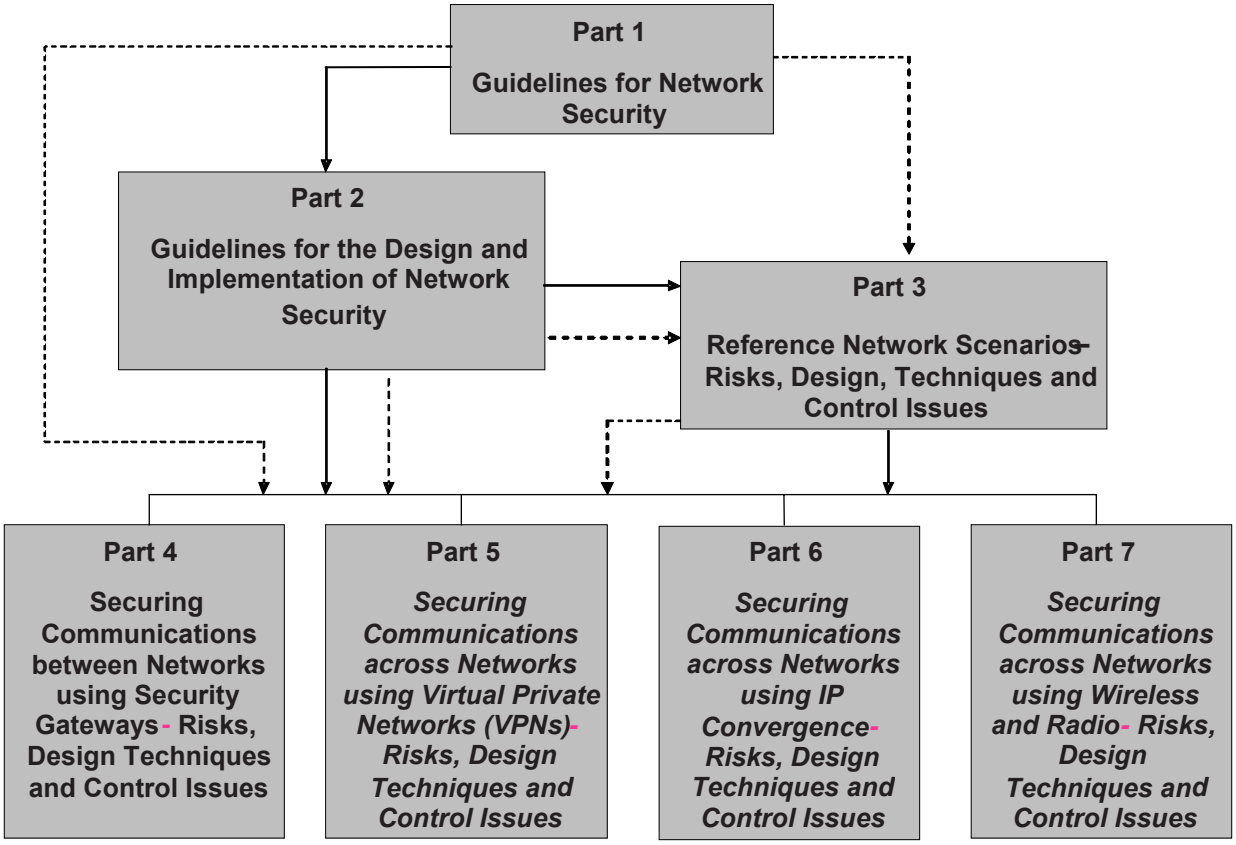
For example, an organization is considering the implementation of a new network environment that includes use of IP convergence, security gateways and some use of wireless, as well as use of web hosting and the Internet (e.g. for e-mail and outgoing online access).

In using the processes described in Part 1 to determine the security risks to the new network environment, the organization would consult the risk related information from the other relevant Parts of ISO/IEC 27033, i.e. those Parts that define the specific security risks (as well as design techniques and control issues) relating to IP convergence, security gateways and some use of wireless, as well as use of web hosting and the Internet (e.g. for e-mail and online access).

In using Part 2 to determine the network technical security architecture required, the organization would consult the information on design techniques and control issues from the other relevant Parts of ISO/IEC 27033, i.e. those that define the specific design techniques and control issues (as well as the security risks) - relating to IP convergence, security gateways and some use of wireless, as well as use of web hosting and the Internet (e.g. for e-mail and online access).

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009



There may be other parts to ISO/IEC 27033 in the future. Examples of possible topics to be covered by future parts include local area networks, wide area networks, broadband networks, web hosting, Internet e-mail, and routed access to third party organizations. The main clauses of all such parts should include but are not limited to the three designations Risks, Design Techniques and Control Issues.

Figure 2 — ISO/IEC 27033 'Road Map'

The structure of ISO/IEC 27033-1 comprises:

- an overview of the approach to network security (see clause 6),
- a summary of the process for identifying network related risks and preparing to identify security controls, i.e. establishing network security requirements (see clause 7),
- an overview of the controls that *support* network security technical architectures and their related technical controls, i.e. other controls (non-technical and technical) that are applicable not just to networks (see clause 8). References are provided to the relevant content of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005,
- an introduction to the achievement of quality technical security architectures that will ensure network security appropriate to organizations' business environments, using a consistent approach to the planning for and design of network security, as relevant aided by the use of models/frameworks (i.e. an introduction to the content of ISO/IEC 27033-2) (see clause 9),
- an introduction to the specific risks, design, techniques and control issues associated with reference network scenarios (i.e. an introduction to the content of ISO/IEC 27033-3) (see clause 10),

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

- an introduction to the specific risks, design techniques and control issues for network 'technology' topics, (i.e. an introduction to the content of ISO/IEC 27033-4, 27033-5, 27033-6, 27033-7 and other possible future parts) (see clause 11 and Annex A),

- a summary of the issues associated with developing, implementing and testing a network security solution (see clause 12), operating a network security solution (see clause 13), and the on-going monitoring and reviewing of a network security implementation (see clause 14), and

- a table that shows cross-references between ISO/IEC 27001/27002 network security related controls and ISO/IEC 27033-1 clauses is given in Annex B.

6 Overview

6.1 Background

An example network environment, which can be observed in many organizations today, is shown in Figure 3 below. (Figure 3 is purely for illustrative purposes in this overview only, and is not intended for any other purpose.)

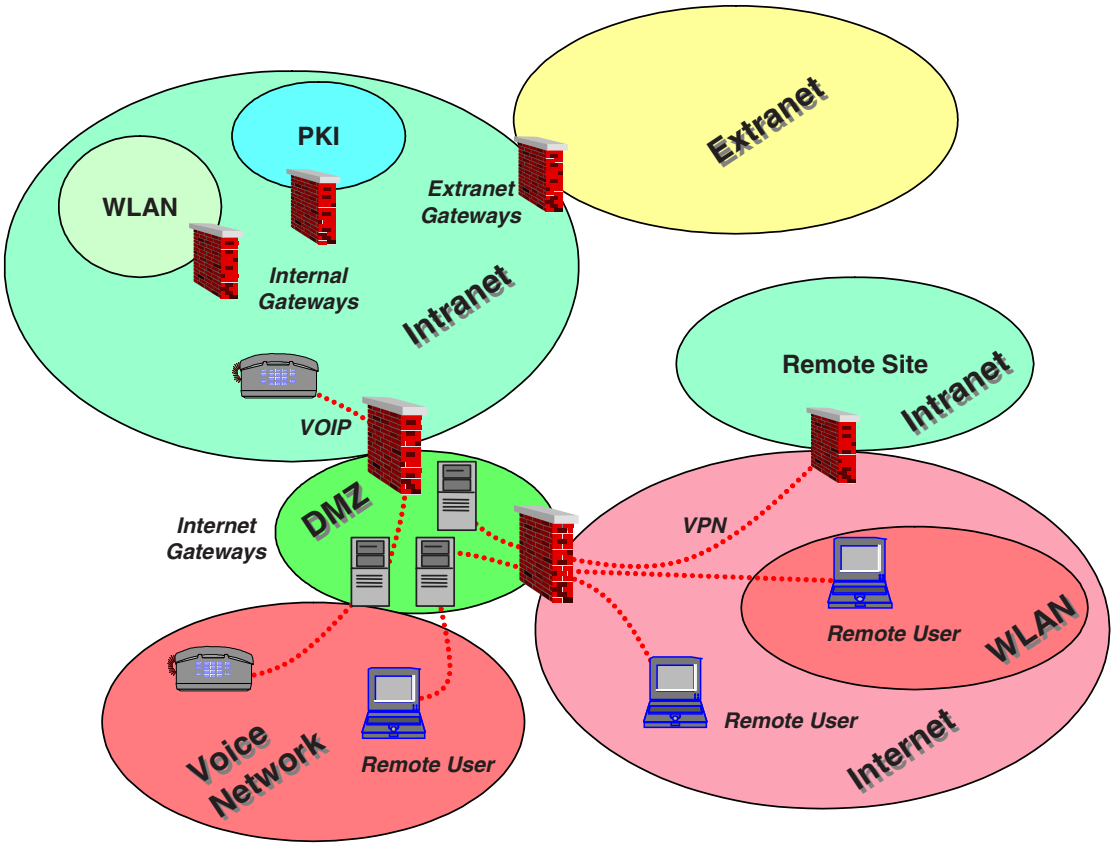


Figure 3 — Example Network Environment

The Intranet specifies the network an organization relies on and maintains internally. Typically, only persons working for the organization have direct physical access to this network, and since the network is located within premises owned by the organization, a level of physical protection could easily be achieved. In most cases the Intranet is not homogenous with regard to the technologies used and security requirements; there can be infrastructures which have a need for a higher protection level than given by the Intranet itself. Such infrastructures, for example the essential parts of a PKI environment, can be operated in a dedicated segment

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

of the Intranet. On the other hand, certain technologies (e.g. WLAN infrastructures) can require some isolation and authentication because they introduce additional risks. For both cases, internal security gateways can be used to implement this segmentation.

The business needs of the majority of organizations today necessitate communications and data exchange with external partners and other organizations. Often the most important business partners are connected in a way directly extending the Intranet towards the network of the partner organization; the term Extranet is commonly used for such extensions. Since trust in the connected partner organizations is in most cases lower than within the organization, extranet security gateways are used to cover the risks introduced with these connections.

Public networks, of which the Internet is the most common example, are further used today to provide cost optimized communications and data exchange facilities with partners, customers and the general public, and to provide various forms of extensions of the Intranet. Due to the low trust level in public networks, especially the Internet, sophisticated security gateways are needed to help manage the associated risks. These security gateways include specific components to address the requirements of the various forms of Intranet extension as well as partner and customer connections.

Remote users can be connected through VPN technology, and they may further use wireless connection facilities like public WLAN hotspots for accessing the Internet. Alternatively, remote users can use the telephone network for establishing direct dial-up connections to a Remote Access Server, which is often located within the DMZ environment of the Internet Firewall.

When an organization decides to use VoIP technologies to implement the internal telephone network, then appropriate security gateways to the phone network are typically present as well.

Business opportunities afforded by new network environments should be balanced against the risks posed by the newer technologies. For example, the Internet has a number of technical features which can cause concerns from a security point of view, as it was originally designed with resilience rather than security as a priority – and many of the underlying protocols in common use are not naturally secure. There are a large number of people in the global environment who have the capacity, knowledge and inclination to access the underlying mechanisms and protocols and create security incidents, ranging from unauthorized access to full-scale destructive denial of service.

6.2 Network Security Planning and Management

When considering network connections, all those persons in the organization who have responsibilities associated with the connections should be clear about the business requirements and benefits, the related security risks, and the related technical security architectural aspects/design techniques and security control areas. The business requirements and benefits will influence many decisions and actions taken in the process of considering network connections, identifying technical security architectural aspects/design techniques and potential security control areas, and then eventually selecting, designing, implementing and maintaining secure networks.

The overall process for achieving and maintaining required network security can be summarized as follows:

a) determine scope/context and then assess security risks:

   1) gather information on the current and/or planned network environment:

      i) review the corporate information security policy for statements on network related risks that will always be considered as high, and on network security controls that will need to be implemented regardless of the assessed risks.

      NOTE This policy should also contain the organization's position on (1) regulatory and legislative security requirements relating to network connections as defined by the relevant regulatory or legislative bodies (including national government agencies), and (2) the sensitivity of the data to be stored or transported on the network.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

ii) gather and review information on the current and/or planned network(s) – the architecture(s), applications, services, types of connection and other characteristics – this will have a bearing on the identification and assessment of risks, and determining what is possible in terms of network technical security architecture/design,

iii) gather other information to be able to assess potential adverse business impacts, threats and vulnerabilities (this will include the value to business operations of the information to be transferred via network connections, any other information potentially accessible in an unauthorized way through these connections, and of the services provided),

2) identify and assess the network security risks, and appropriate potential control areas:

i) conduct network security risk assessment and management review including using risk information related to required network scenarios and 'technology' topics (see clauses 10 and 11) – security requirements definition. (Note that this will include (1) assessment of the risks associated with potential breaches of relevant regulation and legislation relating to network connections as defined by the relevant regulatory or legislative bodies (including national government agencies), and (2) using the agreed potential adverse business impacts, confirming the sensitivity/classification of the data to be stored or transported on the network),

b) identify supporting security controls – non-technical and technical that not only apply to networks (see clause 8),

c) review technical security architecture/design options, considering network scenarios and 'technology' topics, and selecting and documenting the preferred technical security architecture/design and related security controls (see clauses 9 to 11, and Annex A). [Note that this will include controls required to comply with relevant regulations and legislation relating to network connections as defined by the relevant regulatory or legislative bodies (including national government agencies)],

d) develop and test the security solution (see clause 12),

e) implement and operate the security controls (see clause 13),

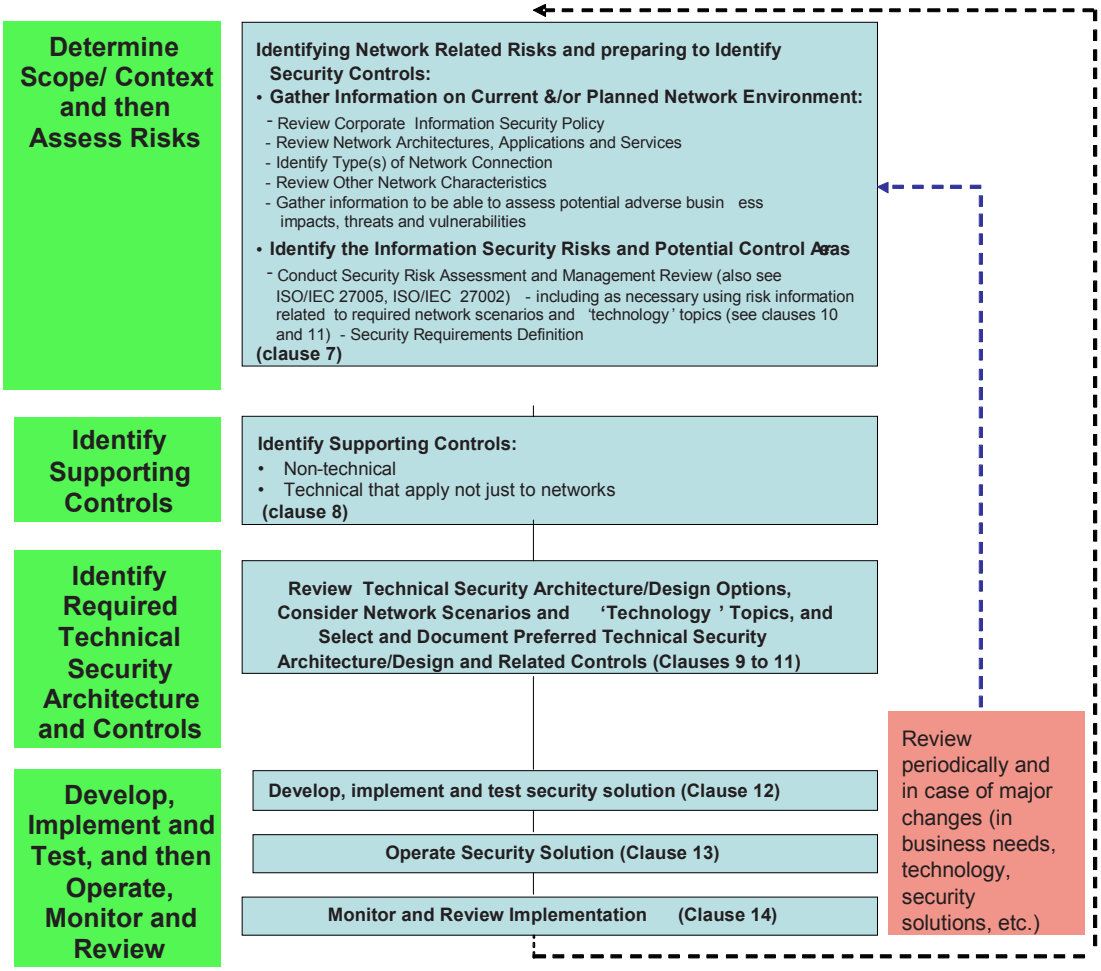
f) monitor and review the implementation (see clause 14). (Note that this will include monitoring and reviewing the controls required to comply with relevant regulations and legislation relating to network connections as defined by the relevant regulatory or legislative bodies (including national government agencies):

1) reviews should be carried out periodically, and in the case of major changes (in business needs, technology, security solutions, etc.), and as necessary the results from the earlier stages outlined above should be re-visited and updated.

An overview of the network security planning and management process is shown diagrammatically in Figure 4 below.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009



NOTE See ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004 and ISO/IEC 27005.

Figure 4 — Network Security Planning and Management Process

It is emphasized that throughout this process reference should be made as appropriate to ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005, including for general advice on the identification of security controls. ISO/IEC 27033-1 is complementary to these standards, providing an introduction on how to identify appropriate network security controls and thence to ISO/IEC 27033-2 to ISO/IEC 27033-7.

7 Identifying Risks and Preparing to Identify Security Controls

7.1 Introduction

As reflected in clause 6 above, the first stage in identifying and assessing network related risks and preparing to identify security controls is to gather information on the current and/or planned network environment. Clause 7.2 below provides guidance on this. The next stage is to identify and assess the network security risks, and appropriate potential control areas. Clause 7.3 below provides guidance on this.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

7.2 Information on Current and/or Planned Networking

7.2.1 Security Requirements in Corporate Information Security Policy

An organization (or community)'s corporate information security policy can include statements on the need for confidentiality, integrity, non-repudiation and availability, as well as views on types of threat and risk, and network security controls that will need to be implemented regardless of the assessed risks. Thus the first step should be to review the corporate information security policy for details of any network related risks that will always be considered as high and of network security controls that must be implemented.

For example, such a policy could state that

- the availability of certain types of information or services is a major concern,
- no connections via dial-up lines are permitted,
- all connections to the Internet should be made through a security gateway,
- a particular type of security gateway should be used,
- no payment instruction is valid without a digital signature.

Such requirements should be accounted for in the conduct of the risk assessment and management review, and the identification of the technical security architectural/design aspects and potential security controls. Any such requirements should be documented in the draft list of potential control areas, and as necessary reflected in the technical security architecture/design options.

Guidance on information security policy is provided in ISO/IEC 27002 and ISO/IEC 27005.

7.2.2 Information on Current/Planned Networking

7.2.2.1 Introduction

The next step should be to gather and review information on the current and/or planned network(s) – the architecture(s), applications, services, types of connection and other characteristics – this will have a bearing on the identification and assessment of risks, and determining what is possible in terms of network technical security architecture/design. These aspects are described below.

7.2.2.2 Network Architectures, Applications and Services

Detail should be obtained of the relevant current and/or planned network architecture, applications and services, and reviewed to provide the necessary understanding and context for the conduct of the network security risk assessment and management review and thence considering the network technical security architecture options. By clarifying these aspects at the earliest possible stage, the process of identifying and assessing the security risks and associated security controls, and the network technical security architecture options and deciding which one should be adopted, should become more efficient and eventually result in a more workable security solution.

Further, the consideration of the current and/or planned network architecture, application and service aspects at an early stage should allow time for those aspects to be reviewed and possibly revised if an acceptable security solution cannot be realistically achieved within the current and/or planned environment.

Depending on the area they cover, networks can be very broadly categorized as:

- LANs, which are used to interconnect systems locally, and
- WANs, which are used to interconnect systems up to a world-wide coverage.

© ISO/IEC 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009

(Some sources also define the term Metropolitan Area Network (MAN) for a locally restricted WAN, e.g. within a city. However, nowadays the same technologies are used as for WANs and thus there are no significant differences between MAN and WAN any more. Further, for the purposes of this standard Personal Area Networks (PANs) will be categorized as LANs. Another term used today is Global Area Network (GAN), i.e. a global WAN. Note that today there are terms used for storage related networks, such as Storage Area Network (SAN) and Network Attached Storage (NAS), but these are not in the scope of IS 27033.)

Different protocols have different security characteristics and should be afforded special consideration. For example:

- shared media protocols are mainly used in LANs and provide mechanisms to regulate the use of shared media among the systems connected. As a shared media is used, all information on the network is physically accessible by all connected systems. An example here is Ethernet hub,

- access control protocols that are designed to allow entry to a network. Examples here include IEEE 802.1x and WPA,

- routing protocols are used to define the route through the different nodes on which information travels across network segments, either LANs or WANs. Information is physically accessible for all systems along the route, and routing can be changed, either accidentally or intentionally,

- MPLS protocols, on which many carrier networks are based, allows a carrier core network to be shared by multiple private networks without any member of one private network being aware that there are other private networks sharing the core network. The major application is the implementation of VPNs, where different labels are used to identify and segregate traffic belonging to different VPNs (an MPLS based VPN is not based on data encryption mechanisms). This enables corporate customers to outsource their internal network to a service provider and thus avoid the need to deploy and manage their own core IP network. A key benefit is the ability to converge network services, such as voice and data over one network, using QoS mechanisms to ensure real time performance.

Many of the protocols used in networks do not implement any security. For example, tools to acquire passwords from network traffic are commonly used by attackers. This makes protocols like Telnet that send unencrypted passwords over a public network highly vulnerable.

NOTE Telnet is Terminal emulation program to work on-line on a remote computer

Many protocols can be used in conjunction with different network topologies and media, and by using wired as well as wireless technologies. In many cases this has further impact on the security characteristics.

The type of applications used over a network should be considered in the context of security. Types can include:

- thin client applications,

- desktop applications,

- terminal emulation based applications,

- messaging infrastructures and applications,

- store and forward or spooler based applications, and

- client server applications.

© ISO/IEC 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2009