BS ISO/IEC 27033-1:2015

BSI Standards Publication

Information technology — Security techniques — Network security

Part 1: Overview and concepts

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2015

National foreword

This British Standard is the UK implementation of ISO/IEC 27033-1:2015. It supersedes BS ISO/IEC 27033-1:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/-/4, IT Security Techniques - Security Controls and Ser.

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 81999 5

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 2015.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2015

INTERNATIONAL STANDARD

ISO/IEC 27033-1

Second edition
2015-08-15

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 27033-1:2015(E)

© ISO/IEC 2015

Full document details: BS ISO/IEC 27033-1:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2015

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **2**
4 Symbols and abbreviated terms **6**
5 Structure **8**
6 Overview **10**
6.1 Background 10
6.2 Network security planning and management 11
7 Identifying risks and preparing to identify security controls **13**
7.1 Introduction 13
7.2 Information on current and/or planned networking 13
7.2.1 Security requirements in corporate information security policy 13
7.2.2 Information on current/planned networking 14
7.3 Information security risks and potential control areas 18
8 Supporting controls **21**
8.1 Introduction 21
8.2 Management of network security 21
8.2.1 Background 21
8.2.2 Network security management activities 21
8.2.3 Network security roles and responsibilities 23
8.2.4 Network monitoring 24
8.2.5 Evaluating network security 25
8.3 Technical vulnerability management 25
8.4 Identification and authentication 25
8.5 Network audit logging and monitoring 26
8.6 Intrusion detection and prevention 27
8.7 Protection against malicious code 28
8.8 Cryptographic based services 28
8.9 Business continuity management 29
9 Guidelines for the design and implementation of network security **30**
9.1 Background 30
9.2 Network technical security architecture/design 30
10 Reference network scenarios – Risks, design, techniques and control issues **32**
10.1 Introduction 32
10.2 Internet access services for employees 33
10.3 Enhanced collaboration services 33
10.4 Business to business services 33
10.5 Business to customer services 34
10.6 Outsourced services 34
10.7 Network segmentation 34
10.8 Mobile communication 34
10.9 Networking support for travelling users 35
10.10 Networking support for home and small business offices 35
11 'Technology' topics — Risks, design techniques and control issues **35**
12 Develop and test security solution **36**
13 Operate security solution **36**

Documents
Document Sharing Hub

© ISO/IEC 2015 – All rights reserved

Full document details: BS ISO/IEC 27033-1:2015

14 Monitor and review solution implementation **37**

Annex A (informative) **Cross-references between ISO/IEC 27001/27002 network security related controls and ISO/IEC 27033-1 clauses/subclauses** **38**

Annex B (informative) **Example template for a SecOPs document** **42**

Bibliography **47**

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27033-1:2009), which have 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*

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

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

— *Part 6: Securing wireless IP network access*

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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.

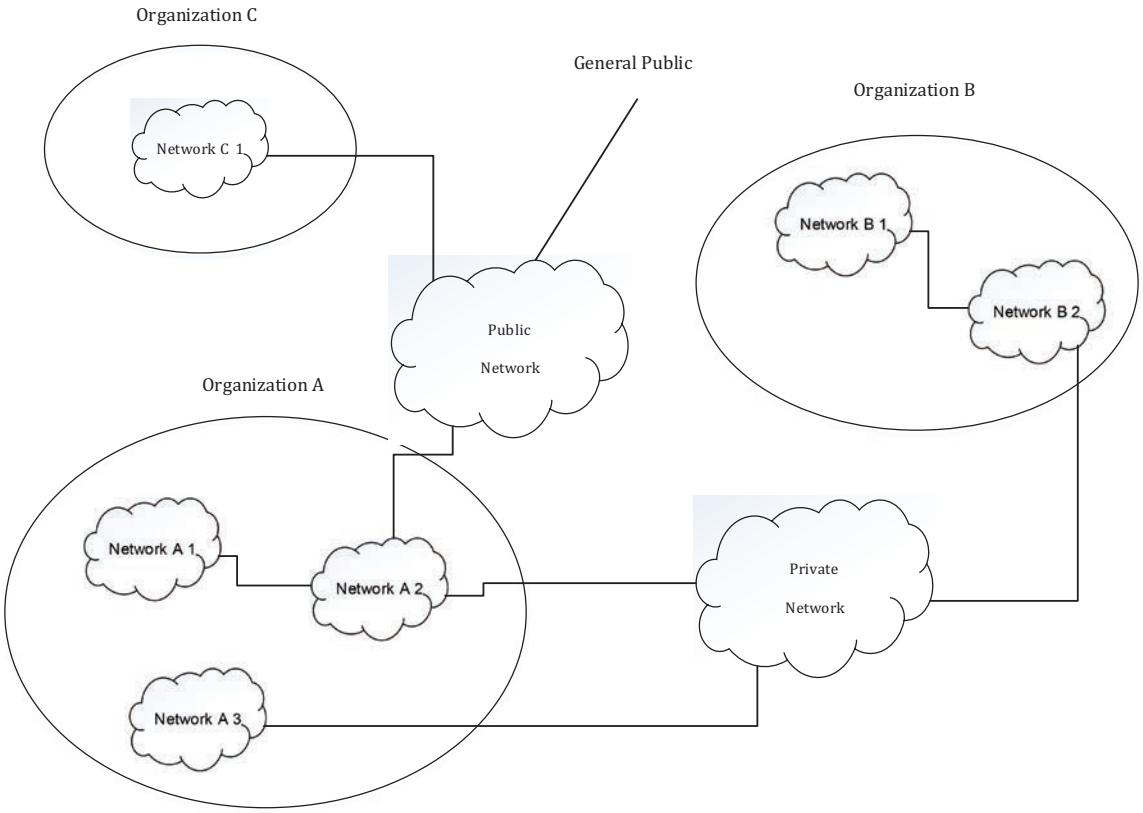

Figure 1 — Broad types of network connection

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 homework 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

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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 this International Standard 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, 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 analyse 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, 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, 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).

— ISO/IEC 27033-4, to define the specific risks, design techniques and control issues for securing information flows between networks using security gateways. It is 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 27033-5, to define the specific risks, design techniques and control issues for securing connections that are established using Virtual Private Networks (VPNs). It is 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, to define the specific risks, design techniques and control issues for securing IP wireless networks. It is relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless networks (for example, network architects and designers, network managers, and network security officers).

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

AVA Documents
Document Sharing Hub

© ISO/IEC 2015 – All rights reserved

Full document details: BS ISO/IEC 27033-1:2015

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 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

INTERNATIONAL STANDARD ISO/IEC 27033-1:2015(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 includes the following:

— 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 this International Standard and a "road map" to all other parts.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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: Naming and addressing*

ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

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

© ISO/IEC 2015 – All rights reserved

AVA Documents Document Sharing Hub

Full document details: BS ISO/IEC 27033-1:2015

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 the following apply.

NOTE The following terms and definitions also apply to all 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

[SOURCE: ISO/IEC 15288:2008, 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

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

Note 1 to entry: Optionally, the certification authority can create the users' keys.

Note 2 to entry: 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 1 to entry: 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

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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 1 to entry: 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 1 to entry: There is no real intelligence in network hubs; they only provide physical attachment points for networked systems or resources.

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

[SOURCE: ISO/IEC 27039, 2.15]

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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

[SOURCE: ISO/IEC 27039, 2.15]

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

[SOURCE: ISO/IEC 27039, 2.15]

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

Note 1 to entry: 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 1 to entry: Label switching can be used as one method of creating tunnels.

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 analyse information flowing in networks

Note 1 to entry: 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

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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 1 to entry: In the context of the Internet protocol, a port is a logical channel endpoint of a TCP connection or UDP messages. 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 to entry: The networks can themselves be based on different protocols.

Note 2 to entry: The routing information is kept in a routing table.

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 emails, 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

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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

Note 1 to entry: 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 Symbols and abbreviated terms

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

3G	third generation mobile telephone system
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
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

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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
IP	Internet protocol
IPS	intrusion prevention system
ISP	Internet service provider
IT	information technology
LAN	local area network
MPLS	multi-protocol label switching
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

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

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
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

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, and 6 may be consulted for information on security risks, and (b) Part 2 - Parts 3, 4, 5, and 6 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, and 6 to avoid duplication (i.e. in using Part 3 there may be a need to consult Parts 4, 5, and 6).

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015

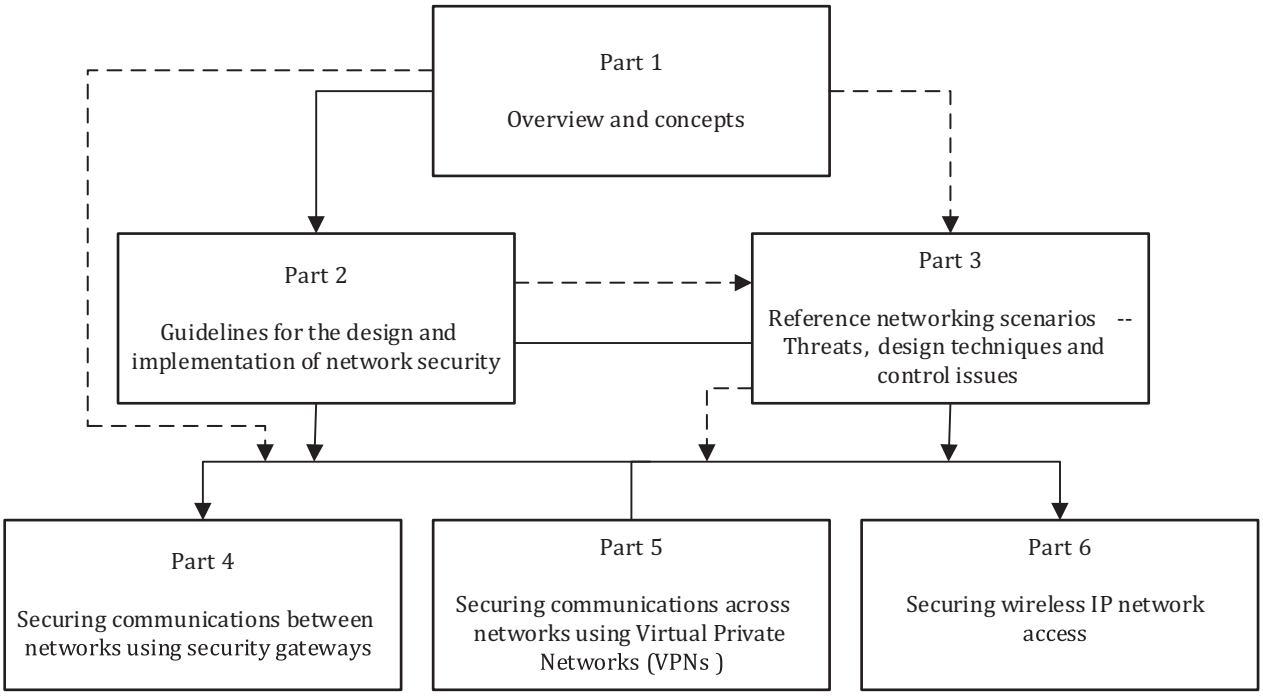

Figure 2 — ISO/IEC 27033 'Road Map'

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 6.

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 email 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 email 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 email and online access).

The structure of this standard 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

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 27033-1:2015