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)

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.

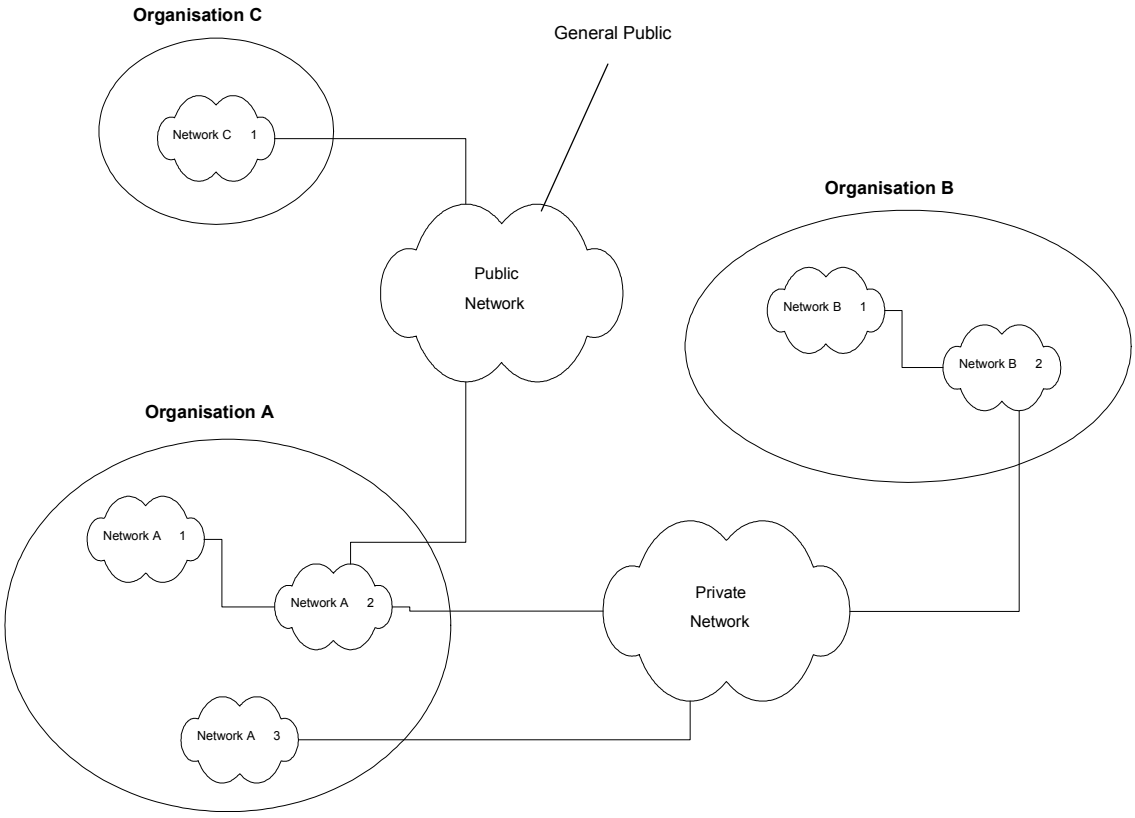


Figure 1 — Broad types of network connection

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”.

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.

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

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.

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.

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.

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

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

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

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.

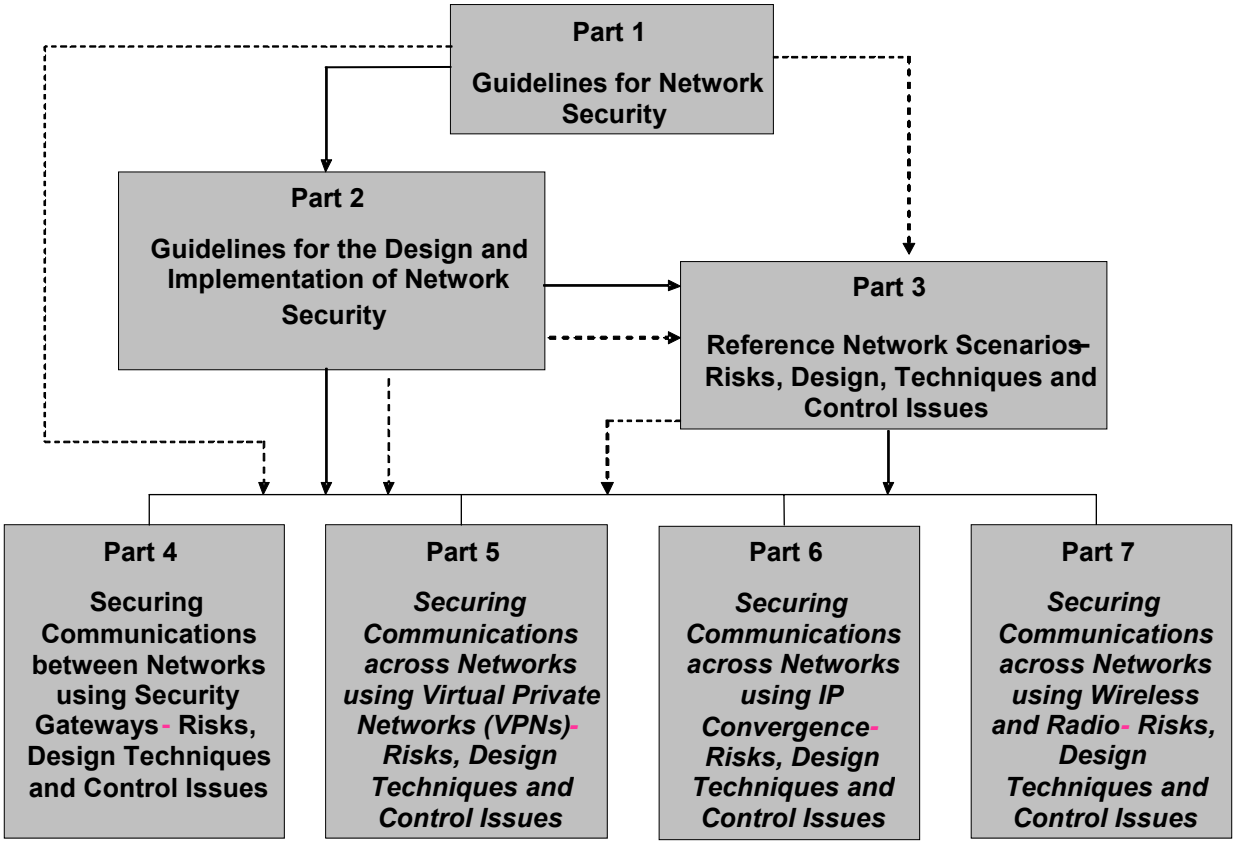
It is noted that in Figure 2 the solid lines indicate the natural hierarchy of the Parts of ISO/IEC 27033. The dotted lines indicate that in following the processes described in (a) Part 1 – Parts 3, 4, 5, 6 and 7 may be consulted for information on security risks, and (b) Part 2 - Parts 3, 4, 5, 6 and 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).



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),

- 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.)

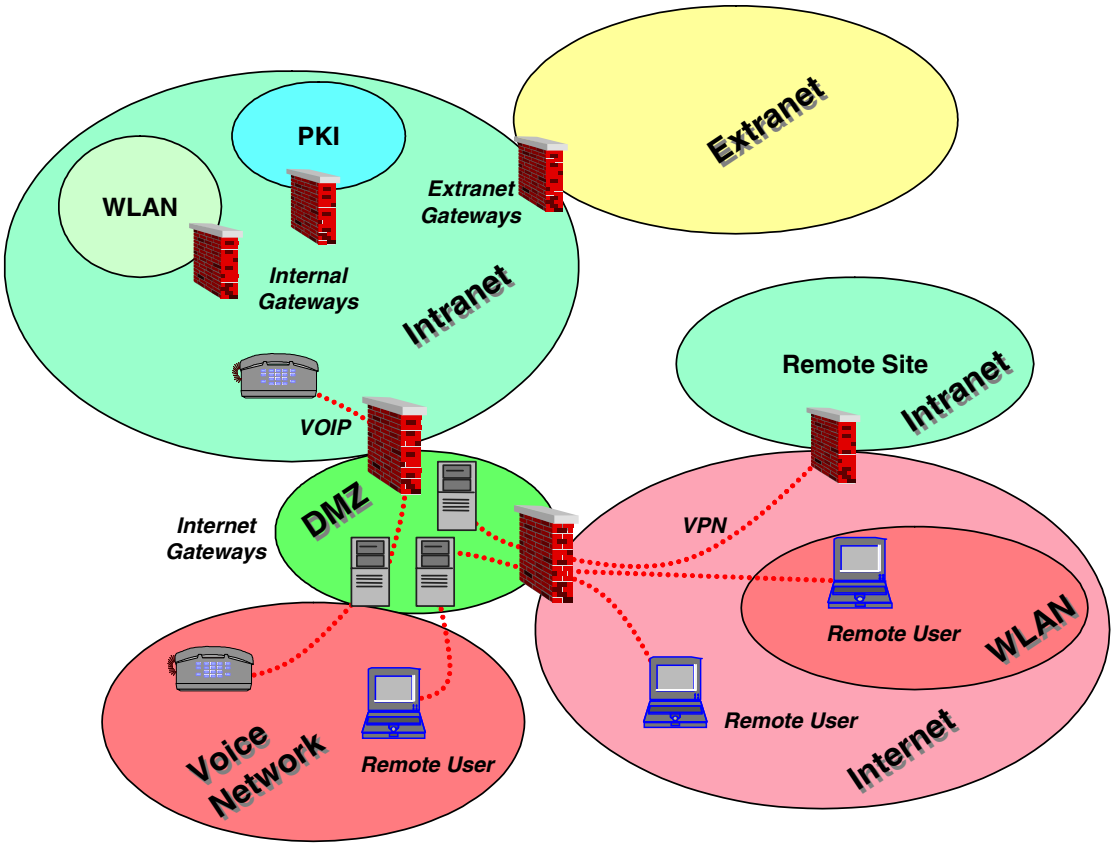


Figure 3 — Example Network Environment

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

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.

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)],

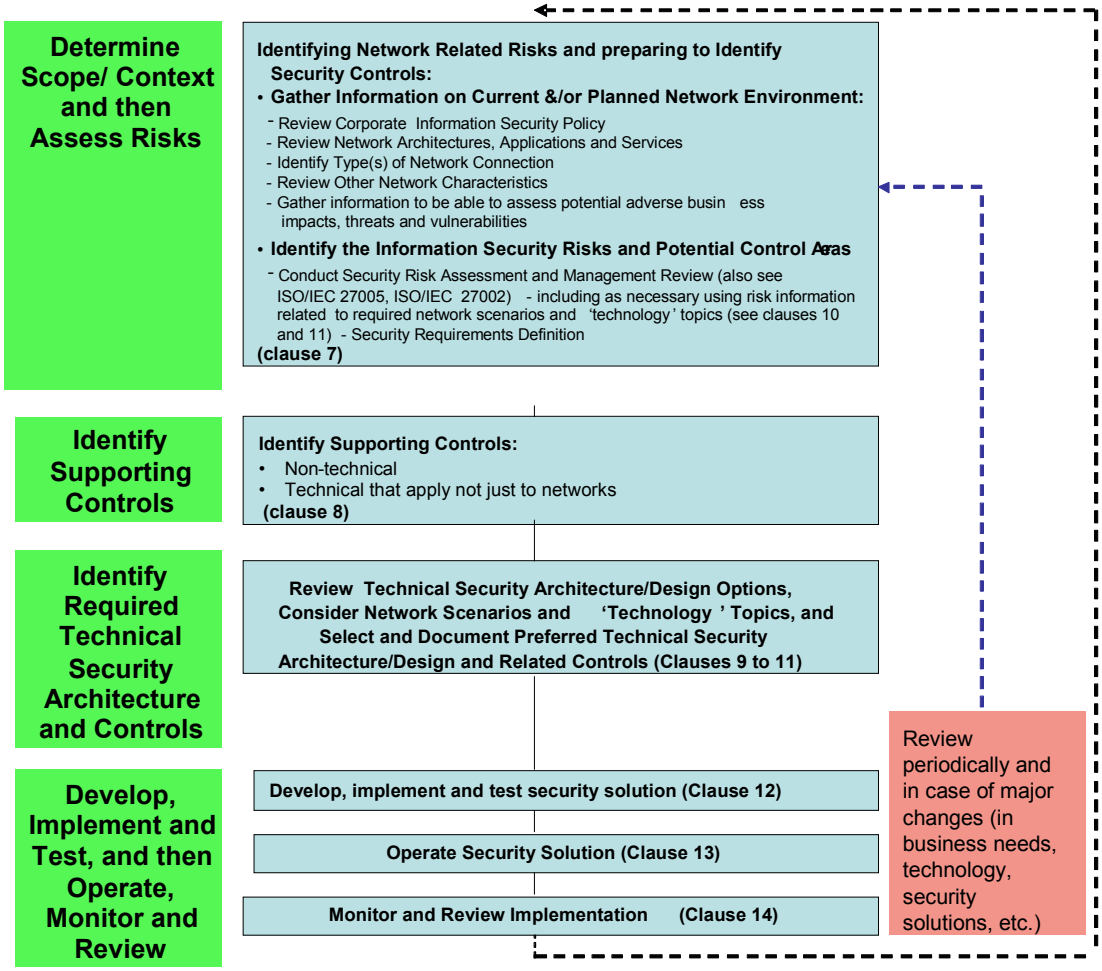
d) develop and test the security solution (see clause 12),

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.



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.

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.

(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.

The following examples show how application characteristics influence the security requirements for the network environments they may use:

- messaging applications (that provide encryption and digital signatures for messages) can provide an adequate security level without the implementation of dedicated security controls on the network,

- thin client applications may need to download mobile code for proper functionality. Whereas confidentiality may not be a major issue in this context, integrity is important and the network should provide appropriate mechanisms for this. Alternatively, if higher requirements need to be fulfilled, digital signing of mobile code will provide integrity and additional authentication. Often this is done within an application framework itself, and therefore there may be no need to provide these services in the network,

- store and forward or spooler based applications typically temporarily store important data on intermediate nodes for further processing. If there are integrity and confidentiality requirements, appropriate controls will be needed in the network to protect the data in transit. However, due to the temporary storage of data on intermediate hosts, these controls may not be sufficient. Thus, additional controls may need to be applied to also protect data stored on intermediate nodes.

The type of services (e.g. DNS, e-mail, voice) used over a network should also be considered in the context of security.

When reviewing the network architecture, applications and services, consideration should also be given to existing network connections within, to or from the organization/community, and to the network to which a connection is proposed. The organization/community's existing connections can restrict or prevent new connections, e.g. because of agreements or contracts. The existence of other connections to or from the network to which a connection is required could introduce additional vulnerabilities and thus higher risks, possibly warranting stronger and/or additional controls.

(General guidance on network and application architectures can be found in ISO/IEC 7498.)

7.2.2.3 Types of Network Connection

There are many generic types of network connection that an organization/community may need to utilize. Some of these types of connection can be made through private networks (to which access is restricted to a known community), and some could be made through public networks (to which access is potentially available to any organization or person). Further, these types of network connection could be used for a variety of services, e.g. electronic mail, and could involve use of Internet, Intranet or Extranet facilities, each with differing security considerations. Each of the types of connection can have different vulnerabilities and thus associated security risks, and consequently eventually require a different set of controls.

One way of categorizing the generic types of network connection that may be required to conduct business, is as follows:

– interconnection between different parts of the same organization within the same controlled location, i.e. a single controlled building or site,

– interconnection between different geographically disparate parts of the same organization, e.g. regional offices with a headquarters site, across a wide area network. Most if not all users are able to access the information systems available via the network, but not all users within the organization would have authorization for access to all applications or information,

– connections between an organization site and personnel working in locations away from the organization, or the establishment of remote links to an organization's computing systems by employees working from home or other remote sites not linked via a network maintained by the organization,

– connections between different organizations within a closed community, e.g. because of contractual or other legally binding situations, or of similar business interests, e.g. banking or insurance. Such connections would not provide access to the full range of applications used by each of the participating organizations,

– connections with other organizations, e.g. for access to remote databases held by other organizations. In this type of network connection, all users, including those of the connecting organization, are individually pre-authorized by the external organization whose information is being accessed.

– connections with the general public domain, with access initiated by the organization's users to public access databases, web sites, and/or electronic mail facilities (e.g. via the Internet),

– connections to the public telephone network from an IP environment, with access initiated to the PSTN from a telephone in an IP network. Such connections are uncontrolled as calls could be received from any location in the world.

Whatever means of categorization is used, the different types of connection in the current and/or planned network environment should be reviewed for their security implications and the information obtained should be used in 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.

7.2.2.4 Other Network Characteristics

Other characteristics of the current and/or planned network(s) should be reviewed. It is particularly important to identify whether the network used/to be used is a public network – a network accessible by anyone, or a private network, e.g. a network consisting of owned or leased lines, therefore considered to be more secure than a public network. It is also important to know the type of data transported by the network, for example a:

- data network – a network transferring primarily data and making use of data protocols,
- voice network – a network intended for telephone but also usable for data, or
- 'hybrid' network encompassing both data and voice, and possibly video.

Other information, such as:

- whether the network is a packet, switched or MPLS network,
- whether it supports a QoS, i.e. in an MPLS network. (QoS concerns consistent performance, reliability and availability. Network services should be delivered to provide the minimum performance level to be usable. For example, voice services will stutter and break up if the bandwidth is inadequate. QoS refers to a network system's ability to sustain a given service at or above its required minimum performance level.),

is also relevant.

Further, it should also be established whether a connection is permanent, or established at time of need.

Once these characteristics of the current and/or planned network have been identified, and at minimum it has been established if the network is public or private, then it is worth considering the following for input into the network security risk assessment and management review. Roughly categorize the network into something like – network with:

- an unknown community of users,
- a known community of users and within a closed business community (of more than one organization),
- a known community of users solely within the organization.

Then consider the category in the context of whether the network used/to be used is a public or private network, and further categorize as:

– an unknown community of users, and use of a public network,

– a known community of users and within a closed business community, and use of a public network,

– a known community of users solely within the organization, and use of a public network,

– an unknown community of users and use of a private network,

– a known community of users and within a closed business community, and use of a private network,

– a known community of users solely within the organization, and use of a private network.

Whichever way this is reviewed, be aware that certain combinations are likely to mean lower levels of risk than others. The information obtained should be used in 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.

7.2.2.5 Other Information

Finally, other information should be gathered to be properly prepared for the ISO/IEC 27001 and 27002 compatible network security risk assessment and management review, including to carefully define the review boundary/scope. Doing this at the earliest opportunity will avoid later ambiguity, unnecessary work and will improve the focus and effectiveness of the review. The boundary/scope definition should clearly indicate which of the following have to be considered when carrying out the network security risk assessment and management review:

– information types,

– business processes,

– actual or potential hardware components, software, services, connections, etc. details (if not known specifically, in general terms),

– actual or potential environments (e.g. locations, facilities),

– activities (operations).

This information, along with that gathered in accordance with clause 7.2 above, should be used in the network security risk assessment and management review, the activities of which are summarized in clause 7.3 below.

7.3 Information Security Risks and Potential Control Areas

As reflected earlier, the majority of organizations today are dependent on the use of networks and related information systems and information to support their business operations. Further, in many cases there is a definite business requirement for the use of networks between the information systems at each organization's location, and to other locations both within and outside the organization, including to/from the general public. When a connection is made to another network, considerable care should be taken to ensure that the connecting organization is not exposed to additional risks (from potential threats exploiting vulnerabilities). These risks could, for example, result from the connection itself or from network connections at the other end.

Some of these risks can be related to ensuring adherence to relevant legislation and regulation. (Particular attention should be given to privacy and data protection legislation. Several countries have legislation placing controls on the collection, processing and transmission of personal data, i.e. data that can be related to a specific person or persons. Depending on the respective national legislation, such controls can impose duties on those collecting, processing and disseminating personal information through networks and can even restrict the ability to transfer that data to certain other countries, yielding additional important security concerns. Less obvious examples of data that can be subject to such legislation are some hardware and IP addresses.)

Thus the risks faced could relate to concerns about unauthorized access to information, unauthorized sending of information, the introduction of malicious code, denial of receipt or origin, denial of service connection, and unavailability of information and service. These can relate to loss of:

- confidentiality of information and code (in networks and in systems connected to networks),
- integrity of information and code (in networks and in systems connected to networks),
- availability of information and network services (and systems connected to networks),
- non-repudiation of network transactions (commitments),
- accountability of network transactions,
- authenticity of information (as well of course of network users and administrators),
- reliability of information and code (in networks and in systems connected to networks),
- ability to control unauthorized use and exploitation of network resources, including in the contexts of organization policy (e.g. selling bandwidth or using bandwidth for own benefits) and responsibilities in relation to legislation and regulation (e.g. storing child pornography),
- ability to control abuse of authorized access.

A conceptual model of network security showing where the types of security risk may occur is shown in Figure 5 below.

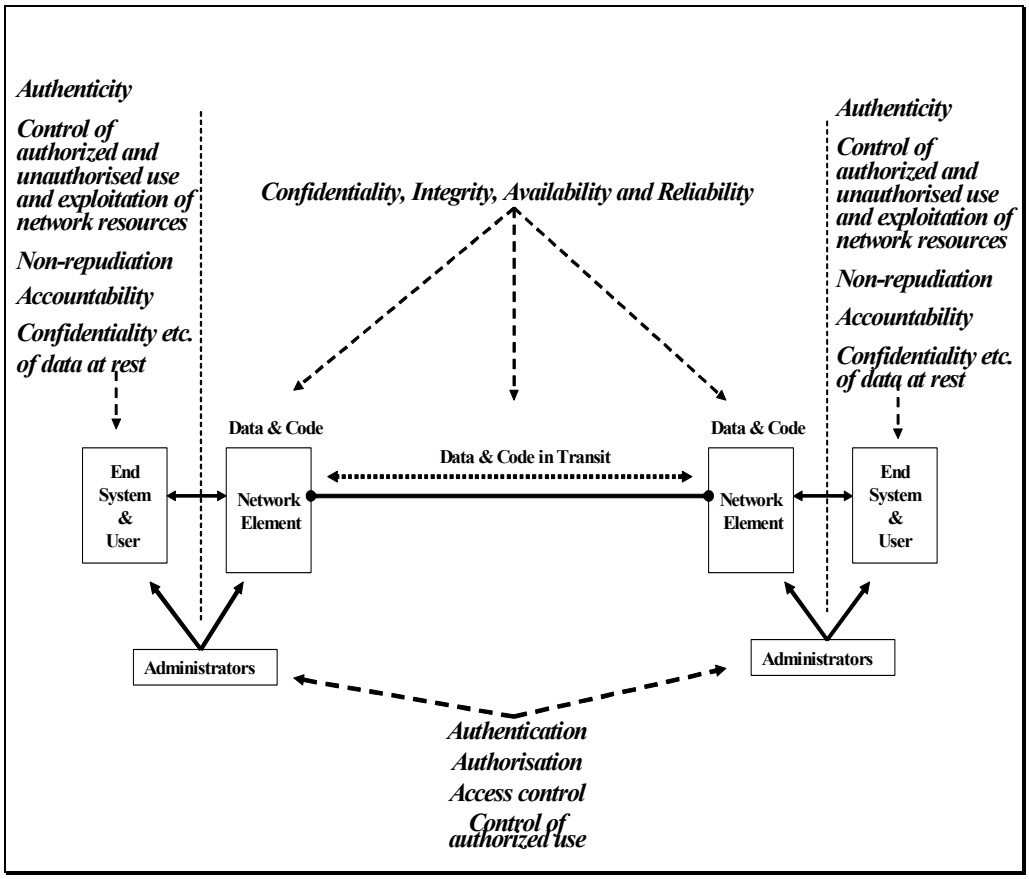


Figure 5 — A Conceptual Model of Network Security Risk Areas

Thus, a network security risk assessment and management review should be conducted to identify and confirm the technical security controls and technical security architecture/design aspects, and supporting non-technical security controls, and in line with recognized good security practice, such as given in ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005. This involves five main activities:

- determining the measures of the importance of information and service, expressed in terms of the potential adverse impacts on business operations were unwanted incidents to occur (sometimes called asset valuations). This will include the values to business operations of the information to be transferred via a network, any other information potentially accessible in an unauthorized way through the network, and of the services provided),

- identifying and assessing the likelihood or levels of threats against the information and service,

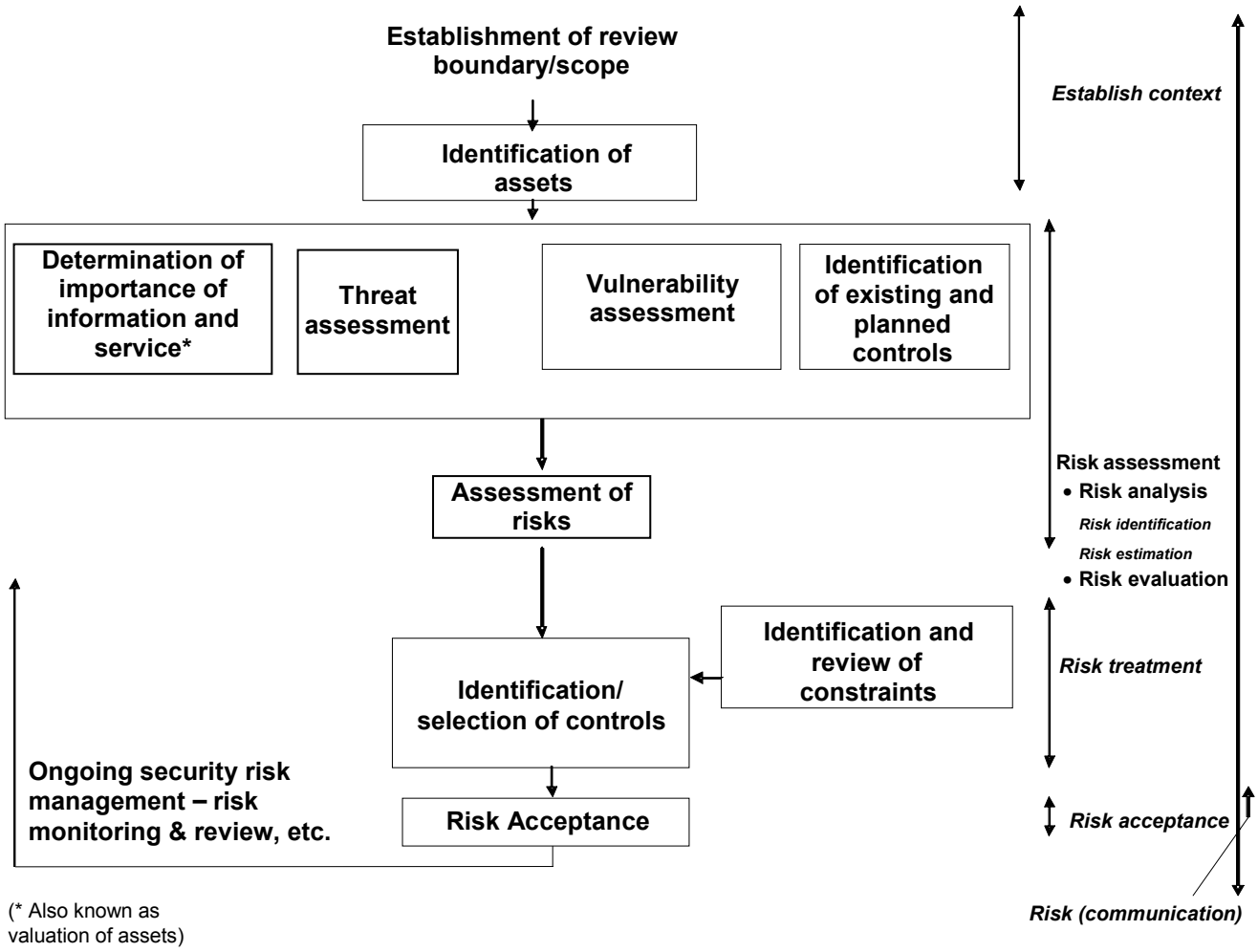
- identifying and assessing the degrees of seriousness or levels of vulnerabilities (weaknesses) that could be exploited by the identified threats,

- assessing the measures of risks, based on the determined measures of the potential adverse impacts on business operations and the levels of threats and vulnerabilities,

- identifying the technical security architectural/design aspects and potential security control areas that are justified by, and thus required to ensure that assessed risks remain within acceptable limits.

The main processes of network security risk assessment and management are shown in Figure 6 below. (This is in effect an expansion of the box in Figure 4 above entitled “Determine Scope/ Context and then Assess Risks” and its related box “Identifying Network Related Risks and preparing to Identify Security Controls”.)

In Figure 6 the first two rows of boxes labelled “Establishment of Review Boundary/Scope” and “Identification of Assets” indicate the preparatory activities. The next two rows of boxes indicate the risk assessment activities, and final two rows indicate the information security control selection and (residual) risk acceptance activities.



The terms as used in ISO 27001 and related standards are shown in italics.

Figure 6 — Network Security Risk Assessment and Management Processes

NOTE For detailed information on the conduct of network security risk assessment and management reviews, see ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005.

It is emphasized that in conducting such reviews use should be made, where applicable, of the risk (and security control) information related to required network scenarios and 'technology' topics - see clauses 10 and 11, and Annex A, below, and Parts 3 to 7.

8 Supporting Controls

8.1 Introduction

This clause provides 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. Information on many of these types of controls can be found in ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005. The controls that are especially important with regard to the use of networks are expanded upon in the clause 8.2 to 8.9 below, which address the management of network security (network security management activities, network security roles and responsibilities, network monitoring and evaluating network security), technical vulnerability management, identification and authentication, network audit logging and monitoring, intrusion detection, protection against malicious code, cryptographic based services, and business continuity management. As relevant, references are provided to the relevant content of ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27005.

8.2 Management of Network Security

8.2.1 Background

The overall management of network security should be undertaken in a secure manner, and be accomplished with due consideration of the different network protocols available and related security services. In furtherance of this, an organization should consider a number of network security controls, the majority of which can be identified through using ISO/IEC 27002 and ISO/IEC 27005. Those that need to be expanded upon in the context of network security are described in clauses 8.2.2 to 8.2.5 below.

8.2.2 Network Security Management Activities

8.2.2.1 Introduction

A key requirement for any network is that it is supported by secure management activities, which will initiate and control the implementation, and operation, of security. These activities should take place to ensure the security of all of an organization/community's information systems. Network security management activities should include:

- definition of all responsibilities related to network security, and designation of a security manager with overall responsibility,
- documented network security policy, and accompanying documented technical security architecture,
- documented network SecOPs,
- the conduct of security compliance checking, including security testing, to ensure security is maintained at the required level,
- documented security conditions for network connection, to be adhered to before connection is permitted - as relevant by internal and external organizations or people,
- documented security conditions for remote network users,
- a network security incident management scheme,
- documented and tested business continuity/disaster recovery plans.

For detailed information on these topics reference should be made to ISO/IEC 27002, ISO/IEC 27005 and ISO/IEC 27035. Only those of the above topics that are especially important with regard to the use of networks is further guidance provided in the clauses below.

8.2.2.2 Network Security Policy

It is the responsibility of management to visibly accept and support the organization's network security policy (as referred to in ISO/IEC 27002). This network security policy should flow from, and be consistent with, the organization's information security policy. The policy should be capable of implementation, readily available to authorized members of the organization, and encompass clear statements on the:

- organization's stance with respect to acceptable network usage,
- explicit rules for the secure use of specific network resources, services and applications,
- consequences of failure to comply with security rules,
- organization's attitude towards network abuse,
- rationale(s) for the policy, and for any specific security rules.

(In some circumstances these clear statements can be incorporated into the information security policy, if this is more convenient for the organization and/or it would be clearer for its personnel.)

The content of the network security policy should usually include a summary of the results from the network security risk assessment and management review (which provides the justification for spend on controls), including detail of all security controls selected commensurate with the assessed risks (see Clause 7.3 above).

8.2.2.3 Network Security Operating Procedures

In support of the network security policy, SecOPs documents should be developed and maintained. They should contain details of the day-to-day operating procedures associated with network security, and who is responsible for their use and management. An example template is shown at Annex C.

8.2.2.4 Network Security Compliance Checking

For all networks, security compliance checking should take place against a comprehensive checklist constructed from the controls specified in the:

- network security policy,
- related SecOPs,
- technical security architecture,
- security gateway service access (security) policy,
- business continuity plan(s),
- where relevant, security conditions for connection.

This should occur prior to live operation of any network, prior to a major new release (related to significant business or network related change), and otherwise annually.

This should include the conduct of security testing to recognized standards, with a security testing strategy and related plans produced beforehand setting out exactly what tests are to be conducted, with what, where and when. This should encompass a combination of vulnerability scanning and penetration testing. Prior to the commencement of any such testing, the testing plan should be checked to ensure that the testing will be conducted in a manner fully compatible with relevant legislation. When carrying out this checking it should not be forgotten that a network may not just be confined to one country – it may be distributed through different countries with different legislation. Following the testing, the reports should indicate the specifics of the vulnerabilities encountered and the fixes required and in what priority.

8.2.2.5 Security Conditions for Multiple Organization Network Connections

Unless security conditions for connection are in place and contractually agreed, an organization is in effect accepting the risks associated with the other end of a network connection outside of its domain. Such risks can include those related to privacy/data protection, where a connection can be used to exchange personal data subject to national legislation at one or both ends, and, where the other end of a network connection (outside an organization's domain) is in another country, the legislation may be different.

As an example, organization A may require that before organization B can be connected to its systems via a network connection, B should maintain and demonstrate a specified level of security for its system involved in that connection. In this way A can be assured that B is managing its risks in a way that is acceptable. In such cases A should produce a security conditions for connection document that details the controls to be present at B's end. These should be implemented by B, followed by that organization signing a binding statement to that effect and that security will be maintained. A would reserve the right to commission or conduct a compliance check on B.

There will also be cases where organizations in a community mutually agree a 'security conditions for connection' document which records obligations and responsibilities for all parties, including reciprocal compliance checking.

8.2.2.6 Documented Security Conditions for Remote Network Users

Users authorized to work remotely should be issued with a documented 'security conditions for remote network users' document. This should describe user responsibilities for the hardware, software and data in relation to the network, and its security.

8.2.2.7 Network Security Incident Management

Information security incidents are more likely to occur, and more serious adverse business impacts to result, where networks are used (as opposed to where there are none). Further, with networks connecting to other organizations in particular there could well be significant legal implications connected with security incidents.

Thus, an organization with network connections should have a well documented and implemented information security incident management scheme and related infrastructure in place to be able to respond quickly as security incidents are identified, minimize their impact and learn the lessons to attempt to prevent re-occurrence. This scheme should be able to address both information security events (identified occurrences of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant), and information security incidents (a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security). Further detail on information security incident management is provided in ISO/IEC 27035.

8.2.3 Network Security Roles and Responsibilities

The roles and responsibilities that should be instigated associated with network security management are as follows. (Note that, depending upon the size of the organization, these roles can be combined.)

Senior management:

- define the organization's security objectives,
- initiate, approve, publish, and impose the organization's security policy, procedures and rules,
- initiate, approve, publish, and impose the organization's acceptable usage policy,
- ensure security and acceptable usage policies are enforced,

NOTE Senior management includes the business owners.

Network management:

- develop detailed network security policy,
- implement the network security policy,
- implement the acceptable usage policy,
- manage the interface with external stakeholders / external service providers to ensure conformance with internal and external network security policies,
- ensure that operational responsibility for networks is separated from computer operations, where appropriate,

Network Security team:

- acquire, develop, test, check and maintain network security components and tools,
- maintain network security tools and components to follow closely the evolution of threats (e.g. updating malicious code (including virus) signature files),
- update network security relevant configurations (e.g. access control lists) according to changing business needs,

Network administrators:

- install, update, use and protect network security services and components,
- carry out the necessary daily tasks to apply the network security specifications, rules, and parameters required by the network security policies in force,
- take appropriate measures to assure the protection of network security components (e.g. back-ups, monitoring network activity, responding to security incidents or alarms, etc.),

Network users:

- communicate their security requirements,
- comply with corporate security policy,
- comply with corporate acceptable usage policies for network resources,
- report network security events and incidents,
- provide feedback on network security effectiveness,

Auditors (internal and/or external):

- review and audit (e.g. periodically test the effectiveness of network security),
- check compliance with network security policy,
- check and test compatibility of operating network security rules with the current business requirements and legal restrictions (e.g. lists granted for network accesses).

8.2.4 Network Monitoring

Network monitoring is a very important part of network security management. This is dealt with in Clause 8.5 below.

8.2.5 Evaluating Network Security

Network security is a dynamic concept. Security staff should keep up to date with developments in the field and ensure that networks continues to work with the most current security patches and fixes available from vendors. Steps should be taken periodically to audit existing security controls against established benchmarks, including by security testing – vulnerability scanning, etc. Security should be a primary consideration in evaluating new network technology and network environments.

8.3 Technical Vulnerability Management

Network environments, as other complex systems, are not free of errors. Technical vulnerabilities are present in, and are published for, components frequently used in networks. The exploitation of these technical vulnerabilities can have severe impact on the security of networks, most often observed in the areas of availability and confidentiality. Thus technical vulnerability management should be present covering all network components, and should include:

- obtaining timely information about technical vulnerabilities,
- evaluating the exposure of networks to such vulnerabilities,
- defining appropriate security controls to address the associated risks, and
- the implementation and verification of the defined security controls.

A prerequisite for technical vulnerability management should be the availability of a current and complete inventory of all network components, providing the necessary technical information, e.g. type of device, vendor, version numbers of hardware, firmware or software, and also organizational information, e.g. the responsible administrative persons.

If the organization has already set up an overall technical vulnerability management program, the integration of technical network vulnerability management into the overall task should be the preferred solution. (Further information on technical vulnerability management, including implementation guidance, can be found in ISO/IEC 27002.)

8.4 Identification and Authentication

It is important to be able to restrict access through connections to authorized personnel (whether internal or external to the organization). For example, it is a common policy requirement that access to certain network services and related information should be restricted to authorized personnel. Requirements for these are not exclusive to the use of network connections, and thus detail appropriate to the use of networks should be obtained by using ISO/IEC 27002 and ISO/IEC 27005.

Three security control areas that could be relevant to the use of networks, and related information systems, are:

- *remote log-ins* – whether from authorized personnel working away from the organization, from remote maintenance engineers, or personnel from other organizations, which are accomplished either via dial-ups to the organization, Internet connections, dedicated trunks from other organizations, or shared access through the Internet. They are connections established at need by either internal systems or contractual partners using public networks. Each type of remote log-in should have additional security controls appropriate to the nature of the network concerned, e.g. not allowing direct access to system and network software from accounts used for remote access, except where additional authentication has been provided (see below) – and perhaps end-to-end encryption, and protecting information associated with e-mail software and directory data stored on PCs and laptops used outside of an organization's offices by its personnel from unauthorized access,

- *authentication enhancements* – whilst the use of user id/password pairs is a simple way to authenticate users, they can be compromised or guessed. Thus other more secure ways to authenticate users should be considered – particularly for remote users and/or when a high possibility exists that an unauthorized person may gain access to protected and important systems – say because the access may be initiated using public networks, or the accessing system can be out of the direct control of the organization (e.g. via a laptop). Simple examples are using CLID (but as this is open to spoofing it should not be used as a proven ID without further authentication) and links via modems that are disconnected when not in use – and only connected after verification of the caller's identity. More complex, but much more secure, examples – particularly in the context of remote access, are using other means of identification to support the authentication of users such as remotely verified tokens and smart cards – and ensuring that the token or card can only function in conjunction with the authorized user's authenticated account (and preferably, that user's PC and location/access point) and, for example, any related PIN or biometric profile. Generically this is termed strong, two factor, authentication,

- *secure single sign-on* – where networks are involved users are likely to encounter multiple identification and authentication checks. In such circumstances users can be tempted to adopt insecure practices such as writing down passwords or re-using the same authentication data. Secure single sign-on can reduce the risks associated with such behavior by reducing the number of passwords that users have to remember. As well as reducing risks, user productivity may be improved and helpdesk workloads associated with password resets may be reduced. However, note that the consequences of failure of a secure single sign-on system could be severe because not one but many systems and applications would be at risk and open to compromise (sometimes termed the "keys to the kingdom" risk). Stronger than normal identification and authentication mechanisms can therefore be necessary, and it may be desirable to exclude identification and authentication to highly privileged (system level) functions from a secure single sign-on regime.

8.5 Network Audit Logging and Monitoring

It is very important to ensure the effectiveness of network security through audit logging and ongoing monitoring, with the rapid detection, investigation and reporting of, and response to, security events and then incidents. Without this activity, it is not possible to be sure that network security controls always remain effective and that security incidents will not occur with resultant adverse effects on business operations.

Sufficient audit log information of error conditions and valid events should be recorded to enable thorough review for suspected, and of actual, incidents. However, recognizing that recording huge amounts of audit related information can make analysis difficult to manage, and can affect performance, care has to be taken over time in what is actually recorded. For network, audit logs should be maintained that include the following types of event:

- remote failed log-on attempts with dates and times,
- failed re-authentication (or token usage) events,
- security gateway traffic breaches,
- remote attempts to access audit logs,
- system management alerts/alarms with security implications (e.g. IP address duplication, bearer circuit disruptions).

In a network context, audit logs should be drawn from a number of sources, such as routers, firewalls, IDS, and sent to a central audit server for consolidation and thorough analysis. All audit logs should be examined in both real time and off line. In real time, logs can be displayed on a rolling screen and used to alert potential attacks. Off line analysis is essential as this allows the greater picture to be determined with trend analysis being undertaken. First indications of an attack can be that there are substantial “drops” in the firewall logs, indicating probing activity against a potential target. An IDS system can also detect this in real time against an attack signature.

It is emphasized that for analysis and investigative purposes suitable approved audit log management and analysis software must be used for log storage and retrieval, traceability and reporting from audit logs (against particular users, applications and information types, and by time period, particularly when required for investigative purposes) and reporting – with quick, focused and readily understandable outputs. The audit log analysis reports must be held in a secure location, and archived for an agreed period of time. Further, identification and authentication, and access control, protection must be place for the audit logs themselves.

Ongoing monitoring should include coverage of

- audit logs from firewalls, routers, servers, etc.,
- alerts/alarms from such as audit logs pre-configured to notify certain event types, from such as firewalls, routers, servers,
- output from IDS,
- results from network security scanning activities,
- information on events and incidents reported by users and support personnel, and
- results from security compliance reviews.

Audit trails should be maintained online for a period in accordance with the needs of the organization, with all audit trails backed up and archived in a manner that ensures integrity and availability, e.g. by using WORM media such as CDs. Further, audit logs contain sensitive information or information of use to those who may wish to attack the system through network connections, and possession of audit logs can provide proof of transfer over a network in the event of a dispute – and are therefore particularly necessary in the context of

ensuring integrity and non-repudiation. Therefore all audit logs should be appropriately protected, including when archived CDs are destroyed at the designated date. Audit trails should be securely retained for a period in accordance with organizational requirements and national legislation, It is also important that time synchronization is properly addressed for all audit trails and related servers, for example using NTP, particularly for forensics and possible use in prosecutions.

It is emphasized that network monitoring should be conducted in a manner fully compatible with relevant national and international legislation and regulation. This includes legislation for data protection and for regulation of investigatory powers (where by law all users have to be informed of any monitoring before it is conducted). In general terms monitoring should be conducted responsibly, and not for instance used for reviewing the behavior of employees in countries with very limited privacy laws. Obviously the actions taken should be consistent with the security and privacy policies of the organization/community, and appropriate procedures with related responsibilities put in place. Network audit logging and monitoring should also be conducted in a forensically secure manner if audit log evidence is to be used in criminal or civil prosecution.

Most audit logging and monitoring controls required in relation to use of networks and related information systems can be determined by using ISO/IEC 27002 and ISO/IEC 27005.

8.6 Intrusion Detection and Prevention

As the use of networks increases, it becomes easier for intruders to find multiple ways to penetrate an organization or community's information systems and networks, to disguise their initial point of access, and to access through networks and target internal information systems. Further, intruders are becoming more sophisticated, and more advanced methods of attack and tools are easily available on the Internet or in the open literature. Indeed, many of these tools are automated, can be very effective, and easy to use – including by persons with limited experience.

For most organizations it is economically impossible to prevent all potential penetrations. Consequently, some intrusions are likely to occur. The risks associated with most of these penetrations should be addressed through the implementation of good identification and authentication, logical access control and accounting and audit controls, and, if justified, together with intrusion detection and prevention capabilities. Such capabilities provide the means by which to predict intrusions, identify intrusions in real-time and raise appropriate alarms, and to prevent intrusions. It also enables local collection of information on intrusions, and subsequent consolidation and analysis, as well as analysis of an organization's normal information system patterns of behavior/usage.

An IDS listens all traffic into internal networks to identify that an intrusion has been attempted, is occurring, or has occurred and possibly respond to intrusions, as well as alerting appropriate personnel. There are two types of IDS:

- NIDS, which monitor packets on a network and attempts to discover an intruder by matching the attack pattern to a database of known attack patterns, and

- HIDS, which monitor activity on the hosts (servers) – by monitoring security event logs or checking for changes to the system, such as changes to critical system files, or to the systems registry.

An IPS checks all traffic before it passes into internal networks and automatically blocks all recognized attacks; in other words and IPS is specifically designed to provide an active response capability.

Detailed guidance on intrusion detection and prevention is provided in ISO/IEC 18043.

8.7 Protection against Malicious Code

Malicious code (viruses, worms, Trojans, spyware, etc. – which are often collectively termed 'malware') can be introduced through network connections. Malicious code can cause a computer to perform unauthorized functions (e.g. bombard a given target with messages at a given date and time), or indeed destroy essential resources (e.g. delete files) as soon as it has replicated to try to find other vulnerable hosts. Malicious code can not be detected before damage is done unless suitable controls are implemented. Malicious code may result in compromise of security controls (e.g. capture and disclosure of passwords), unintended disclosure of

information, unintended changes to information, destruction of information, and/or unauthorized use of system resources.

Some forms of malicious code should be detected and removed by special scanning software. Scanners are available for firewalls, file servers, mail servers, and PCs/workstations for some types of malicious code. Further, to enable detection of new malicious code it is very important to ensure that the scanning software is always kept up to date, desirably through daily updates. However, users and administrators should be made aware that scanners cannot be relied upon to detect all malicious code (or even all malicious code of a particular type) because new forms of malicious code are continually arising. Typically, other forms of control are required to augment the protection provided by scanners (where they exist).

Overall, it is the job of anti-malicious code software to scan data and programs to identify suspicious patterns associated with malware. The library of patterns to be scanned for is known as signatures, and should be updated at regular intervals, or whenever new signatures become available for high-risk malware alerts. In the context of remote access, anti-malicious code software should be run on the remote systems and also on the servers on the central system – especially Windows and e-mail servers.

Network users and administrators should be made aware that there are greater than normal risks associated with malicious software when dealing with external parties over external links. Guidelines for users and administrators should be developed outlining procedures and practices to minimize the possibility for introducing malicious code.

Users and administrators should take special care to configure systems and applications associated with network connections to disable functions that are not necessary in the circumstances, for example, PC applications could be configured so that macros are disabled by default, or require user confirmation before execution of macros.

Further detail on malicious code protection is provided in ISO/IEC 27002 and ISO/IEC 27005.

NOTE ISO/IEC 11889 describes technology widely deployed in client and server systems that can be used for the detection and isolation of code of malicious or unknown origin.

8.8 Cryptographic Based Services

Where preservation of confidentiality is important, encryption controls should be considered to encrypt information passing over networks. Where preservation of integrity is important, digital signature and/or message integrity controls should be considered to protect information passing over network connections. Digital signature controls can provide similar protection to message authentication controls, but also have properties that allow them to enable non-repudiation procedures.

Where there is a requirement to ensure that substantive proof can be provided that information was carried by a network (non-repudiation), controls such as the following should be considered:

- communication protocols that provide acknowledgement of submission,
- application protocols that require the originator’s address or identifier to be provided and check for the presence of this information,
- gateways that check sender and receiver address formats for validity of syntax and consistency with information in relevant directories,
- protocols that acknowledge delivery from networks, and that allow the sequence of information to be determined.

Where it is important that information transmission or receipt can be proven if it is contested (another form of non-repudiation), further assurance should be provided through the use of a standard digital signature method. Senders of information, where proof of source is required, should seal the information using a digital signature to a common standard. Where proof of delivery is required, senders should request a reply sealed with a digital signature.

The decision to use encryption, digital signature, message integrity or other encryption based controls should take account of relevant government laws and regulations, and, as relevant, appropriate public key infrastructures, the requirements for key management, the suitability of the underlying mechanisms used for the type of network involved and the degree of protection required, and reliable and trusted registration of users or entities associated with keys (certified where relevant) used in digital signature protocols.

Encryption mechanisms are standardized in ISO/IEC 18033. One commonly used encryption technique is known as a block cipher, and ways of using block ciphers for encryption protection, known as modes of operation, are standardized in ISO/IEC 10116. Message integrity controls, known as Message Authentication Codes (or MACs), are standardized in ISO/IEC 9797. Digital signature techniques are standardized in ISO/IEC 9796 and ISO/IEC 14888. Further information on non-repudiation is provided in ISO/IEC 14516 and ISO/IEC 13888.

Key management ensures, as a basic service for all other cryptographic services, that all necessary encryption keys are managed during their complete lifecycle and are used in a secure way. For information on key management, and related topics such as PKI or the more encompassing topic of identity management, reference should be made to other documents and standards, such as:

- ISO/IEC 11770 (Key management),
- ISO/IEC 9594-8 (The Directory: Public-key and attribute certificate frameworks),
- ISO 11166-2 (Banking, key management by means of asymmetric algorithms),
- ISO 11568 (Banking – retail key management),
- ISO 11649 (Financial services – Structured creditor reference to remittance information),
- ISO 13492 (Retail key management data elements),
- ISO 21118 (Banking Public Key Infrastructure).

Note that cryptography should also be used for the management of network devices. Further, access and network management logs should be transmitted in secure encrypted sessions to protect sensitive data.

8.9 Business Continuity Management

It is important that controls are in place to ensure the ongoing function of the business in the event of a disaster by providing the ability to recover each part of the business subsequent to a disruption in an appropriate time frame. Thus an organization should have a business continuity management program in place, with processes covering all business continuity stages – business impact analysis review, risk assessment review, establishing business recovery requirements, business continuity strategy formulation, business continuity plan production, business continuity plan testing, ensuring business continuity awareness for all staff, ongoing business continuity plan maintenance, and risk reduction. Only by following all stages can it be ensured that the:

- required business priorities and timescales are in line with business needs,
- preferred business continuity strategy options identified are commensurate with those priorities and timescales, and thus,
- correct and necessary plans and facilities are put in place, and tested, encompassing information, business processes, information systems and services, voice and data communications, people and physical facilities.

Guidance on business continuity management as a whole, including the development of an appropriate business continuity strategy and related plans, and their subsequent testing, can be obtained in ISO/PAS 22399:2007.

From the network perspective, it is the maintenance of network connections, the implementation of alternative connections of sufficient capacity, and the recovery of connections subsequent to unwanted events, that have to be addressed. These aspects and requirements should be based on the importance of the connections to

the functioning of the business over time, and the projected adverse business impacts in the event of disruption. Whilst connectivity can afford many advantages to an organization, in the event of a disruption, in terms of flexibility and the ability to make use of creative approaches, they can also represent points of vulnerability and ”single points of failure”, which could have major disruptive impacts on the organization.

9 Guidelines for the Design and Implementation of Network Security

9.1 Background

This clause addresses the various network technical security architecture/design aspects and related potential control areas. Clause 10 introduces the risk, design techniques and security control areas for reference network scenarios. Clause 11 introduces the risks, design techniques and security control issues for particular ‘technology’ topics of concern to today’s organizations. A particular network security solution can in fact encompass a number of the topics and control areas introduced in Clauses 10 and 11. A table that shows cross-references between ISO/IEC 27001/27002 network security related controls and ISO/IEC 27033-1 clauses is shown at Annex B.

Having followed Clauses 8 to 11 (and Annex A), the proposed technical security architecture/design and list of identified controls should be thoroughly reviewed in the context of the relevant network architectures and applications. The architecture and list of controls should then be adjusted as necessary and subsequently be used as the basis for developing, implementing and testing the technical security solution (see Clause 12 below). Then once the technical security architecture and thus security control implementation have been signed-off, then live operations should commence (see Clause 13 below), with ongoing monitoring and reviewing of the implementation (see Clause 14 below).

9.2 Network Technical Security Architecture/Design

The documentation of the possible technical security architecture/design and implementation options provides a means for the examination of different solutions, and a basis for trade-off analysis. This also facilitates the resolution of issues associated with technical constraints, and contentions between the requirements of the business and for security, that will often arise.

In documenting the options, due account should be taken of any corporate information security policy requirements (see Clause 7.2.1 above), the relevant network architecture, applications, services, types of connection and other characteristics (see Clause 7.2.2 above), and the list of potential controls identified by the security risk assessment and management review (see Clause 7.3 above). In accomplishing this, account should be taken of any existing technical security architectures/designs. Once the options have been documented and reviewed, as part of the technical architecture design process, the preferred security architecture should be agreed and documented in a Technical Security Architecture/Design Control Specification document (that is compatible with the Technical Architecture Design, and vice versa). Then, changes might result to the network architecture, applications and services (to ensure compatibility with the preferred technical security architecture/design), and/or the list of potential controls (e.g. because it is agreed that the security architecture/design can only be technically implemented in a particular way, necessitating an alternative to an identified control).

Note that ISO/IEC 27033-2 defines how organizations should achieve quality technical security architectures/designs that will ensure network security appropriate to their business environments, using a consistent approach to the planning, design and implementation of network security.

The inputs to the network technical security architecture/design development process, as described in ISO/IEC 27033-2, include the:

- the organization/community’s documented service requirements,
- documentation of any existing or planned architecture, design and/or implementation,

- current network security policy (or relevant parts of the associated information system security policy) – preferably based on the results from a security risk assessment and management review,
- definition of the assets that should be protected,
- current and planned performance requirements, including traffic related,
- current product information.

The outputs from the design process include:

- the network technical security architecture/design document,
- service access (security) requirements documents for each security gateway/firewall system (which includes the firewall rule base(s)),
- Security Operating Procedures (SecOPs),
- as relevant, conditions for secure network connection for third parties,
- as relevant, user guidelines for the third party users.

The network technical security architecture/design document is described in detail in ISO/IEC 27033-2, which also contains an example template for service access (security) requirements documents at Appendix D (of ISO/IEC 27033-2). Further information on the other documents referred to can be found in clause 8.2.2 above and also in ISO/IEC 27033-2.

(Further, once the required network technical security architecture/design has been documented and implemented, then security test plans should be produced and security testing conducted. Once acceptable test results have been achieved, with any adjustments made in the light of problems found during testing, then formal management sign-off should be obtained for the network technical security architecture/design and implementation completed (see Clause 12 below).)

Information on each of the following activities is provided in ISO/IEC 27033-2 (and thus not repeated here):

- preparing for the technical design and implementation of network security:
  - network security project initiation,
  - confirming the broad network requirements of the organization/community,
  - reviewing the existing and/or planned technical architecture and implementation. (All existing and/or planned technical architectures and implementations should be described, and checks made that they are consistent with the organization/community's functional requirements and needs – see previous bullet.),
  - asset identification/confirmation,
  - confirming the security risk assessment and management results, and reviewing existing and/or planned network security controls in the context of those results, and selecting potential security controls,
  - reviewing network performance requirements and confirming criteria. (Performance requirements need to be reviewed, queries resolved and the performance criteria required to be met by the technical architecture and related technical security architecture/design formally agreed. Thus data is required to enable the configurations for communication lines, servers, security gateways, etc., etc., to be identified that will ensure the required service availability.),
- network technical security design, including coverage of all applicable technical topics (dealt with in line with the headings in ISO/IEC 27001:2007), and:

- use of “scenario” and “technology” guidance (as provided in ISO/IEC 27033-3 to 27033-6) (also see Clauses 10 and 11 below),
- use of models/frameworks (including ITU-T X.805, and others,
- product selection (which should be conducted as an iterative process associated with the design of the network technical security architecture, and not undertaken in isolation, and should be based on many factors (including technical suitability, performance, expansibility, management facilities, logical security, and of course vendor capability, track record, etc.),
- proof of concept (the undertaking of a proof of concept is recommended where a network technical security architecture and related product set have not been put in place before, and/or a complicated service set is envisaged (recognizing that products do not always conform to vendor provided data!),
- network technical security architecture/design completion, and related documentation,

- preparing for testing (a security testing strategy document should be produced describing the approach to be taken with testing to prove the network technical security architecture, primarily concentrating on how the key technical security controls should be tested. Then a test plan should be developed for the network technical security architecture, encompassing much detail including on the tests to be conducted, by whom and from where.),
- formal network technical security architecture sign-off

General design principles (things that apply in most if not all cases) are described in ISO/IEC 27033-2. Further, reference should be made to the annexes of 27033-2 – example model/framework[1)] (“reference” architecture) for network security, model/framework case study, and example documentation templates.

It is emphasized that the technical security architecture/design for any project should be fully documented and agreed, before finalizing the list of security controls for implementation.

10 Reference Network Scenarios – Risks, Design, Techniques and Control Issues

10.1 Introduction

ISO/IEC 27033 Part 3 describes the risks, design techniques and control issues associated with reference network scenarios. Some examples of these scenarios is introduced in clauses 10. 2 to 10.10 below. Part 3 provides detailed guidance on the security risks and the security design techniques and controls required to mitigate those risks on all specific scenarios. Where relevant, Part 3 includes references to Parts 4 to 7 to avoid duplicating the content of those documents.

10.2 Internet Access Services for Employees

Today almost all organizations provide Internet access services for their employees, and in providing such services should consider access for clear identified and authorized purposes, not general open access. It should be defined in a specific policy which services are provided, and for what purposes. Internet Access is normally allowed for business reasons, and subject to organization policy Internet Access can also allowed (usually in limited form) for private purposes. Consideration needs to be given to which services are allowed to be used – is it basic services such as www (http & https), is only information retrieving allowed and/or employees allowed to participate in chat channels, forums etc., are enhanced collaboration services allowed – if yes they introduce their own set of risks which are dealt within a specific scenario.

The basic principle should be that only services which serve the business needs are allowed, but often business operations require the use of services which have more associated security risks. Even when a restrictive policy is in place, Internet access services for employees does introduce substantial security risks.

1) (in the context of ISO/IEC 27033) used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design.

10.3 Enhanced Collaboration Services

Enhanced collaboration services (such as instant messaging - chat, video-conferencing and document sharing environments), which integrate various communication and document sharing possibilities, are gaining more and more importance in today's business environments. Such collaboration services typically integrate video telephony, voice communication with chat channels, e-mail systems, as well as document sharing and online co-working environments. There are two basic ways how to use such services for an organization:

- use them as internal services only, but with the disadvantage that the services cannot be used with external partners, etc.,

- use them as internal services and services external to an organization. This offers much more benefit from using such services, but at the same time has more associated security risks compared with only internal usage.

Regarding implementation, the services can be implemented in-house, or just bought in as a service from a third party. In many cases where in-house services only are to be used, an in-house implementation will be most likely. If the services are to be used internally and externally, then buying in collaboration services from a third party can be a more appropriate solution. The security risks and advice on security design techniques and controls to mitigate those risks are described for both internal, and internal plus external, usage.

10.4 Business to Business Services

Traditionally business to business services have been implemented by using dedicated leased lines or network segments. The Internet and the related technologies do provide more options, but also introduce new security risks associated with the implementation of such services. Typically business to business services have their own requirements. For example, availability and reliability are very important requirements as frequently organizations are directly dependent on working business to business services.

When using the Internet as a base network connection to implement business to business services, requirements such as availability and reliability need to be handled differently than before. Proven measures such as quality of service assumptions used, e.g. in conjunction with leased lines, do not work any more. The new security risks need to be mitigated by appropriate design techniques and controls.

10.5 Business to Customer Services

Business to customer services include e-commerce and e-banking. Requirements include confidentiality (especially regarding e-banking), authentication (what methods are possible today - e.g. two factor, certificate based, etc., relationship between the cost of implementation - typically high since very large number of customers, and the reductions in the risks of such as financial loss, loss of business reputation/credibility), integrity, and resistance against sophisticated attacks - e.g. ‘man in the middle’ or ‘man in the browser’ attacks.

Characteristics include:

- security only ‘guaranteed’ on the end platform typically under the control of an organization, providing a good environment for implementing controls and maintaining a good platform level security,

- security on the customer platform, often a PC, can typically be poor. It is harder to get controls implemented in such an environment, and thus customer platforms would present significant risks in this scenario (without a ‘conditions for secure connection’ set of requirements in a contract, which can be difficult to impose in such an environment).

10.6 Outsourcing Services

Due to the complexity of today's IT environments many organizations use externally provided IT support services or have fully or partially outsourced the support of their IT infrastructure, and/or use other outsourced services. Many vendors also have requirements for direct access to their products in use in customer organizations, to be able to appropriately handle support and/or incident management issues.

Whilst many outsourced services require permanent access rights, e.g. to a supported infrastructure, others may only need temporary access. In some cases outsourced services need highly privileged access rights in order to fulfill the required tasks, especially in incident management scenarios.

10.7 Network Segmentation

For many, particularly multi-national, organizations country specific legislation has a great influence on information security requirements. International organizations typically do business in a number of different countries, and therefore have an obligation to comply with various country specific legislations, which furthermore could result in different information security requirements for each country an organization is active in. For example, a particular country's legislation can require specific protection of customer/client data, and does not allow the transfer of such data to another country. This typically requires additional information security controls to guarantee compliance with such legislation.

To cover the different information security requirements for the countries an international organization is doing business in, segmentation of a network in effect in line with country borders can be an effective broad solution. In many cases such a broad solution could be used to build up a separate barrier of defense, e.g. in addition to application level access control.

10.8 Mobile Communications

This reference network scenario concerns personal mobile communication devices, e.g. smart phones or PDAs, which have become very popular. (Guidance of the security aspects of the communications over networks to and from such devices is provided in such as ISO 27033-7 on securing communications over wireless and radio networks.)

Although the main driver for the fast development of new features of personal mobile communication devices comes from the consumer market, these features are also used in business environments. As the term 'personal' implicates, often such devices are personally owned and used both for business and private purposes. Even devices directed at the business market need to have features introduced for the consumer market, as the vendors want to gain as much business as possible in a competitive market.

Many of the new features available with such devices, the growth of device memory capabilities, and permanent on line connectivity via the Internet that is open to the public, means significant information security risks – as do situations where a person uses the same device for private as well as business purposes.

Further, with the high popularity of personal mobile communication devices and their status as a 'personal gadget', in many cases restrictive policies to only use a limited feature set or to only allow a limited number of devices are likely to fail or be circumvented and thus meaning limited information security effectiveness.

10.9 Network Support for Traveling Users

Today traveling users expect connectivity levels comparable to what which they have in fixed locations, such as their base office. Solutions and offerings in this area often focus on the functionality side. From an information security viewpoint, the offered functionality levels introduce new risks, e.g. by affecting or invalidating assumptions regarding information security. For example, an assumption of maintaining a well controlled and (from the outside) protected Intranet may be questioned substantially if traveling user access to the Intranet is not implemented with appropriate controls.

10.10 Network Support for Home and Small Business Offices

Home and small business offices often require the extension of the internal network of an organization to a home or small business location. The costs of extensions to home or small business locations is a critical issue, since cost/benefit reflections typically do not require high implementation costs. This means cost limitations on the security controls to be used to secure such network extensions and typically prevents the use of established inter-networking security controls used to connect bigger Intranet segments.

In many home or small business scenarios the infrastructure can also be used for private as well as for business purposes – which can result in additional information security risks. The security risks are defined and advice on security design techniques and controls to mitigate those risks are described.

11 'Technology' Topics – Risks, Design Techniques and Control Issues

Details of the security risks, design techniques and control issues associated with 'technology' topics are shown in Annex A. The topics covered are:

- local area networks (see A.1),
- wide are networks (see A.2),
- wireless networks (see A.3),
- radio networks (see A.4),
- broadband networks (see A.5),
- security gateways (see A.6),
- virtual private networks (see A.7),
- voice networks (see A.8),
- IP Convergence (see A.9),
- web hosting (see A.10),
- Internet e-mail (see A.11),
- routed access to third party organizations (see A.12),
- data center (see A.13)

12 Develop and Test Security Solution

Once the technical security architecture has been fully documented and agreed, including by senior management, then the solution should be developed, implemented in 'trial mode' and thoroughly tested and compliance checked.

General 'fit for purpose' testing of the solution should first be conducted, with a testing strategy document produced describing the approach to be taken with testing to prove the solution and then a test plan. There may need to be changes made as a result of deficiencies identified by this type of testing and any necessary re-testing carried out.

Once the 'fit for purpose' testing has been successfully completed and any changes made, the implementation should be reviewed for compliance with the documented technical security architecture and required security controls specified in the following documents:

- technical security architecture,
- network security policy,
- related SecOPs,
- security gateway service access (security) policy,
- business continuity plan(s),
- where relevant, security conditions for connection.

The compliance review should be completed prior to live operation. The review should be complete when all deficiencies have been identified, fixed, and signed off by senior management.

It is emphasized that this should include the conduct of security testing to relevant recognized national, government, community standards (in the absence of international standards), with a security testing strategy and related security test plans produced beforehand setting out exactly what tests are to be conducted, with what, where and when. (An example template for a security test plan is given in ISO/IEC 27033-2.) This should encompass a combination of vulnerability scanning and penetration testing. Prior to the commencement of any such testing, the testing plan should be checked to ensure that the testing will be conducted in a manner fully compatible with relevant legislation and regulation. When carrying out this checking it should not be forgotten that a network may not just be confined to one country – it can be distributed through different countries with different legislation. Following the testing, the reports should indicate the specifics of the vulnerabilities encountered and the fixes required and in what priority, with an addendum confirming that all agreed fixes have been applied. Such reports should be signed off by senior management.

Finally, when all is satisfactory, the implementation should be signed off and accepted - including by senior management.

13 Operate Security Solution

“Operate” means running the live (day to day) networking with the agreed secure solution in place, with security testing having been conducted and related required actions completed beforehand. In other words, once the technical security architecture and thus security control implementation have been signed-off, then live operations should commence. Over time, and if significant change occurs, then further implementation testing and review should be conducted (see also Clause 14 below).

14 Monitor and Review Solution Implementation

Following the commencement of live operations, ongoing monitoring and compliance review activities should be conducted in line with relevant recognized national, government, community standards (in the absence of international standards). Such activities should be conducted prior to a major new release related to significant changes in business needs, technology, security solutions, etc., and otherwise annually. The activities here should follow the pattern as described in Clause 12 above.

Annex A
(informative)

'Technology' Topics – Risks, Design Techniques and Control Issues

A.1 Local Area Networks

A.1.1 Background

A LAN is a network to interconnect computers and servers in a small geographic area. The size ranges from a few interconnected systems, e.g. forming a home network, to a few thousands, e.g. in a campus network. Typical services implemented include the sharing of resources like printers, and the sharing of files and applications. LANs typically also provide central services like messaging or calendar services. In some cases LANs are also used to substitute the traditional function of other networks, e.g. when VoIP protocols and services are provided as a substitute for a PBX based phone network. A LAN can be wired, or wireless based.

A wired LAN usually consists of nodes connected in a network via a network switch using network cables, which can provide high-speed data network capabilities. The most commonly used wired LAN technology is Ethernet (IEEE 802.3).

A WLAN makes use of high frequency radio waves to send network packets over the air. Its flexibility lies in the fact that a LAN can be established quickly without the need of wiring the network. Well-known wireless LAN technologies include IEEE 802.11 implementations and Bluetooth.

When LAN networks are used within physically protected areas, e.g. only within an organization's own premises, then the risks are likely to be such that only basic technical controls are required. However, for use in larger environments, and also when wireless technologies are used, physical protection alone is unlikely to guarantee any level of security.

The desktop is a vulnerable area as it is the user interface. If the desktop is not locked down then it is possible for a user to install unauthorized software on the LAN. Server systems used within a corporate network, both ones exposed to the Internet and internal servers that have no direct connection to the Internet, could have associated major security risks – which have to be taken very seriously. For example, while most IT departments would claim that they are diligent about applying patches as soon as they are available, even large organizations have failed to patch all servers in a timely manner – leading to disruption of internal network traffic by worms and viruses.

A.1.2 Security Risks

In a wired LAN, security risks will arise from the nodes physically connected to the network. Overall, the key security risks related to LANs include those associated with:

- unauthorized access and changes to desktop PCs, servers, and other LAN connected devices,
- unpatched devices,
- poor quality passwords,
- theft of hardware,
- failure of power supplies,
- import of malicious code through e-mail and Web access,
- failure to back up local hard discs,

- failure of hardware, such as hard discs,
- unauthorized connections to the LAN infrastructure, e.g. switches and patch cabinets,
- unauthorized connections to end devices, e.g. laptops,
- default passwords on the management ports of network devices,
- intrusion, where information is disclosed or the integrity and/or availability of data cannot then be guaranteed,
- DoS attacks, where resources become unavailable to authorized users,
- extended latency, which will affect services such as voice over IP services,
- device failure,
- cable failure,
- poor physical security.

The security risks associated with wireless LANS are described in clause A.3.2.

A.1.3 Security Controls

Keeping the LAN space secure requires both the LAN components and connected devices to be secured. Thus the controls to secure a LAN environment could include:

- physical and environmental:
  - use steel cable systems to protect CPUs, monitors and keyboards from theft,
  - use locks on devices to prevent parts, such as memory, from being stolen,
  - use of proximity devices to prevent unauthorized removal from site,
  - ensure that LAN devices, such as switches and routers, are kept in physically secure cabinets in secure communications rooms,
  - provide UPS with auto shutdown for critical devices, and for users' PCs if they do not want to lose work in progress,
- hardware and software:
  - configure devices with private (e.g. IP) addresses,
  - strong password policy,
  - require logon at each PC/workstation, at least with at least a user id/ password pair,
  - display time of last successful log-on,
  - do not re-display the last successful log-on username, nor any list of previously used usernames,
  - install anti-malicious code (including anti-virus) software, and regularly update automatically,
  - implement secure configuration settings,

  - disable floppy disc drive, CD-ROM drive, and USB ports,
  - mirror server drives (or implement RAID) for redundancy,
  - remove unnecessary software,
  - ensure good desktop management in place,
- operational:
  - document software and security settings for future use in configuring new PCs/workstations,
  - schedule periodic download and installation of operating system patches,
  - create and maintain current Emergency Repair Disks, and store in a controlled location,
  - implement log to record maintenance problems and misuse of PCs/workstations,
  - file all PC/workstation component documentation (papers/manuals/disks) for use by service technicians,
  - ensure a back-up regime,
  - ensure that all network devices have default passwords changed,
  - set appropriate network management protocol passwords/community strings,
  - encryption of network traffic,
  - configure audit logs properly, if available, and implement procedures for monitoring audit logs,
  - schedule periodic installation of firmware updates,
  - document equipment settings for future use in reconfiguring equipment; make backup copy of router configuration file, and store in secure location,
  - test all LAN connected devices for vulnerabilities.

The security controls associated with wireless LANS are described in clause A.3.3.

A.2 Wide Area Networks

A.2.1 Background

WANs are used to connect distant locations, and their LANs, together. A WAN can be constructed using cables, circuits from a service provider, or by renting a service from a telecommunications provider. WAN technologies allow the transmission and routing of network traffic over long distance, and usually provide extensive routing features to route network packets to the correct destination LAN. Typically public physical network infrastructure is used for interconnecting LANs, e.g. leased lines, satellite communications or fiber optics. A WAN can be wired, or wireless based.

A wired WAN usually consists of routing devices (e.g. routers) connected to a public or private network via telecommunication wires. A wireless WAN typically uses radio waves to send network packets over the air for a long distance, which can be up to ten kilometers or more.

Whilst the traditional WAN was originally created using fixed links between locations rented from service providers, with the service provider having minimal management activity associated with such links, other than ensuring that they were operational, advances in WAN technology have resulted in a shift of responsibility for

management onto the service provider, with the benefit to an organization of not having to deploy and manage its own network. This means that the onus is on the service provider to ensure that its network management facility is secure. Further, as a WAN is primarily used for routing network traffic over long distance, the routing function should be well secured to ensure that network traffic does not get routed to the wrong destination LAN. Thus, traffic traversing a WAN is prone to interception to those who have access to the WAN infrastructure. Since the WAN infrastructure tends to be more accessible than a LAN, care should be exercised to ensure that sensitive information transmitted over a WAN environment is encrypted. The service provider should be contracted to demonstrate the level of security required by the organization.

A.2.2 Security Risks

Whilst a wired WAN shares the same primary security risks with a wired LAN (see Clause A.1 above), it has more security risks as there is greater exposure of network traffic in a WAN network, meaning that controls, including for access, should be in place to ensure that a wired WAN cannot be easily compromised thereby causing widespread disruption. Similarly, whilst a wireless WAN shares the same primary security risks with a wireless LAN (see Clause A.3 below), it is more prone to disruption due to the possibilities for the jamming of the system used for the transmission of network packets. Overall, the key security risks related to WANs include those associated with:

- intrusion, where information is disclosed or the integrity and/or availability of data cannot then be guaranteed,
- DoS attacks, where resources become unavailable to authorized users,
- extended latency, which will have an effect on services such as voice over IP services,
- jitter on the network, which will affect such as voice quality (caused primarily through the use of copper cables to deliver service),
- device failure,
- cable failure,
- unpatched devices,
- loss of power at a transit site, which affect many others,
- service provider's network management facilities.

A.2.3 Security Controls

The security controls required to secure a WAN should include:

- use of secure management protocols such as SSH,SCP or SNMPv3,
- encryption of management links,
- encryption of network traffic,
- implementation of secure authentication to access the WAN devices, with appropriate alarming of devices,
- securing the physical WAN equipment at each site, such as using locked cabinets with access alarms,
- the use of UPS to ensure against disruption of power supplies,
- dual connected sites, using diverse routes,
- proactive polling of WAN devices,

- network device mapping to identify unauthorized devices,
- patch management,
- encrypted overlays for sensitive data,
- obtaining service guarantees from the service provider, such as for availability, latency and jitter,
- implementation of auditing and accounting for access to WAN devices,
- the use of firewalls that discard any unexpected traffic coming into the network,
- making sure that the infrastructure and addresses are hidden,
- assigning IP addresses that cannot be routed over the Internet,
- the use of software to prevent malicious code, such as Trojans, viruses, spyware and worms, from opening security holes from inside a network,
- the use of IDS to identify suspicious traffic,
- ensuring that the network management systems are logically secure,
- Out of band network management,
- ensuring that the network management locations are physically secure,
- ensuring the devices are backed up,
- performing reliability checks on network management staff.

A.3 Wireless Networks

A.3.1 Background

Wireless networks are specified as networks covering geographically small areas and using non wire-based communication means such as radio waves or infrared. Typically, wireless networks are used to implement equivalent connectivity as provided in LANs and are therefore also called WLANs. The main technologies used are standardized in IEEE 802.11 and Bluetooth. It is emphasized that wireless networks constitute a different category of network from radio networks, such as GSM, 3G and VHF, as those utilize aerial masts for transmission (see Clause A.4 below). In addition, infra-red connections and any other kind of connection supporting wireless connections should be taken into account as a sub-part of wireless network connection considerations.

WLANs suffer from all the vulnerabilities of wired LANs, plus some specific vulnerabilities related to the wireless link characteristics. Some specific technologies (mostly based on encryption) have been developed to address these additional vulnerabilities, although earlier versions of these technologies (e.g. WEP) had architectural weaknesses and thus did not meet the expectations regarding confidentiality requirements.

A.3.2 Security Risks

The key security risks related to the use of WLANs include those associated with:

- eavesdropping,
- unauthorized access,
- interference and jamming,

- misconfiguration,
- secure access mode is off by default,
- insecure encryption protocols,
- insecure management protocols used to manage WLANs,
- it is not always possible to identify WLAN users,
- rogue devices (e.g. at access points).

A.3.3 Security Controls

The controls needed for WLANs could include:

- configure the infrastructure with appropriate technical security measures (including, for example, firewalling the WLAN from the corporate infrastructure),
- encrypt communications and data exchanged, e.g. by implementing an IPsec based VPN over the WLAN between the client and a perimeter firewall,
- giving consideration to improving the security of each WLAN device, by configuring personal firewalls and intrusion detection and anti-malicious code (including anti-virus) software on the client device,
- use authentication,
- control of transmission levels to eliminate a spread outside an organization's physical domain,
- SNMP configured for read only access,
- audit log collection and analysis to detect any corruption or unauthorized usage,
- Out of Band encrypted management, for example using SSH,
- maintaining physical security to wireless access points,
- hardening of any network elements,
- system testing,
- giving consideration to deploying an IDS between the corporate network and the wireless network.

A.4 Radio Networks

A.4.1 Background

Radio Networks are specified as networks using radio waves as a connection medium to cover geographically wide areas. Typical examples of radio networks are mobile phone networks using technologies such as GSM or UMTS and providing public available voice and data services.

It is emphasized that networks using radio waves to cover small areas are considered as a different category and are referred to in Clause A.3 above.

Examples of radio networks include:

– TETRA,

– GSM,

– 3G (including UMTS),

– GPRS,

– CDPD,

– CDMA.

A.4.2 Security Risks

The key security risks related to the use of radio networks in general include those associated with:

– eavesdropping,

– session hijacking,

– impersonation,

– application level threats, e.g. fraud,

– denial of service.

The security risks related to GSM include those associated with the facts that:

– A5/x algorithms and Comp128-1 are weak,

NOTE proprietary algorithm that was initially used by default in SIM cards

– generally GSM encryption is turned off,

– SIM cloning is a reality.

The security risks related to 3G include those associated with the facts that the:

– phones are liable to electronic attack, including the insertion of malicious code, for example viruses,

– opportunities for attack are high because phones are often always on,

– service could be subject to eavesdropping,

– radio network could be jammed,

– insertion of false base stations is possible,

– gateways could be subject to unauthorized access,

– service could be subject to attack and unauthorized access via the Internet,

– introduction of spam is possible,

– management systems could be subject to unauthorized access via RAS,

– service could be attacked via lost or stolen engineering support equipment, including laptops.

UMTS is a key member of the global family of 3G mobile technologies and provides significant capacity and broadband capabilities to support greater numbers of voice and data customers It uses a 5 MHz channel carrier width to deliver significantly higher data rates and increased capacity, providing optimum use of radio resources, especially for operators who have been granted large, contiguous blocks of spectrum – typically ranging from 2x10 MHz up to 2x20 MHz – to reduce the cost of deploying 3G networks. GPRS is an essential first step towards third generation mobile networks, by enhancing the GSM network functionalities. GPRS is a specification for data transfer on GSM networks, which allows both packet switched and circuit switched traffic to exist in the GSM infrastructure. GPRS utilizes up to eight 9.05Kb or 13.4Kb TDMA timeslots, for a total bandwidth of 72.4Kb or 107.2Kb. GPRS supports both TCP/IP and X.25 communications. EDGE enabled GSM networks are able to implement EGPRS , an enhanced version of GPRS, which increases the bandwidth of each timeslot to 60Kb. GPRS enables an 'always-on' Internet connection which is a potential security issue. A GPRS network provider will usually try to elevate the security of the link by providing a firewall between the GPRS network and the Internet, but this should be configured to allow valid services to work, and hence may be exploited by third parties.

CDPD is a specification for supporting wireless access to the Internet and other public packet-switched networks over cellular telephone networks. CDPD supports TCP/IP and CLNP. CDPD utilizes the RC4 stream cipher with 40 bit keys for encryption. CDPD is defined in the IS-732 standard. The algorithm is not strong and can be decrypted by a brute force attack.

CDMA, a form of spread-spectrum, is a family of digital communication techniques that have been used for many years. The core principle of spread spectrum is the use of noise-like carrier waves, which have bandwidths much wider than that required for simple point-to-point communication for the same data rate. Digital coding technology allows CDMA to prevent eavesdropping, whether intentional or accidental. CDMA technology splits sound into small bits that travel on a spread spectrum of frequencies. Each small bit of conversation (or data) is identified by a digital code known only to the CDMA phone and the base station. This means that virtually no other device can receive the call. Since there are millions of code combinations available for any call, it protects against eavesdropping.

A.4.3 Security Controls

There are a number of technical security controls to manage the risks from identified threats to radio networks, that could include those for:

- secure authentication,
- encryption with effective algorithms,
- protected base stations,
- firewalls,
- malicious code (Virus, Trojans, etc.) protection,
- anti-spam.

A.5 Broadband Networks

A.5.1 Background

Broadband networks can be from a group of technologies which allow individual subscribers high speed access to an Internet point-of-presence. Examples of broadband technologies are:

- 3G,
- Cable (optical, coax),
- Satellite,

– xDSL,

– FiOS,

– BPL,

– FTTH.

For xDSL, there are two main types. There is asymmetric (ADSL), where the upload speed from the user is lower (quarter to half of the download speed), and symmetric (SDSL), where the upload and download speeds are the same. In either case, the download speed is typically from 128 kbps to 2-8 Mbps, depending on the product. Cable and satellite technologies also have similar types of product.

The main reasons for adopting broadband technologies are that they are a high-speed, always on technology available more cheaply that conventional communications, and can support bandwidth intensive applications (for example, HDTV requires 15-20 Meg at current compressions). All technologies allow access to the Internet and hence span only from the Internet to the subscriber's premises. Use of the Internet as a universal carrier allows links to other sites to be constructed speedily and cheaply, perhaps with the deployment of VPNs for secure links.

A.5.2 Security Risks

Broadband is simply an 'always on' high-speed link between a subscriber and the Internet. These features make the subversion of a broadband-connected system a valuable proposition for hackers. The key security risks related to the use of Broadband include those associated with:

– disclosure, modification or deletion of information, as a result of unauthorized remote access,

– propagation of malicious code,

– upload/download and execution of unauthorized code,

– identity theft,

– misconfiguration of client systems,

– introduction of software vulnerabilities,

– network congestion,

– DoS.

A.5.3 Security Controls

There are a number of technical security controls to manage the risks from identified threats to broadband communications, which could include:

– Small Office/Home Office (SOHO) Firewalls,

– encryption of data,

– anti-malicious code (including anti-virus) software,

– IDS, including IPS,

– VPNs,

– Software Updates/Patching.

A.6 Security Gateways

A.6.1 Background

A suitable security gateway arrangement should protect the organization's internal systems and securely manage and control the traffic flowing across it, in accordance with a documented security gateway service access policy (see Clause A.6.3 below).

A.6.2 Security Risks

Every day, hackers become more sophisticated in their attempts to breach business networks and the gateway is a centre of interest. Attempts at unauthorized access can be malicious, such as that leading to a DoS attack, they may be to misuse resources, or could be to gain valuable information. The gateway needs to protect the organization from such intrusions from the outside world, such as from the Internet or third party networks. Unmonitored content leaving the organization introduces legal issues and a potential loss of intellectual property. In addition, as more organizations are connecting to the Internet to meet their organizational requirements, they are faced with the need to control access to inappropriate or objectionable Web sites. Without that control, organizations risk productivity losses, liability exposure, and misallocation of bandwidth due to non-productive Web surfing. Thus the key security risks to be addressed include those associated with:

- the connections to the outside world becoming unavailable,
- data becoming corrupted,
- valuable company assets being subject to unauthorized disclosure,
- data placed on websites or otherwise transmitted without proper authority incurring legal penalties, e.g. insider trading.

A.6.3 Security Controls

A security gateway should:

- separate logical networks,
- provide restricting and analyzing functions on the information which passes between the logical networks,
- be used by an organization as a means of controlling access to and from the organization's network,
- provide a controlled and manageable single point of entry to a network,
- enforce an organization's security policy, regarding network connections,
- provide a single point for logging.

For each security gateway a separate service access (security) policy document should be developed and the content implemented to ensure that only the traffic authorized is allowed to pass. This document should contain the details of the ruleset that the gateway is required to administer, and the configuration of the gateway. It could be possible to define permitted connections separately according to communications protocol and other details. Thus, in order to ensure that only valid users and traffic gain access from communications connections, the policy should define and record in detail the constraints and rules applied to traffic passing into and out of the security gateway, and the parameters for its management and configuration.

With all security gateways, full use should be made of available identification and authentication, logical access control and audit facilities. In addition, they should be checked regularly for unauthorized software and/or data and, if such is found, incident reports should be produced in accordance with the organization and/or community's information security incident management scheme (see ISO/IEC 27035).

It is emphasized that the connection to a network should only take place after it is checked that the selected security gateway suits the requirements of the organization and/or community, and that all risks resulting from such a connection can be managed securely. It should be ensured that by-passing the security gateway is not possible.

A firewall is a good example of a security gateway. Firewalls should normally be those that have achieved an appropriate assurance level commensurate with the assessed risks, with the standard firewall ruleset usually beginning by denying all access between the internal and external networks, and adding explicit rules to satisfy only the required communications paths.

Further detail on security gateways is provided in ISO/IEC 27033-4 (as well as ISO/IEC 27002 and ISO/IEC 27005).

Note that whilst the network security aspects of personal firewalls, a special type of firewall, are not discussed in 27033-4, they should also be considered. Unlike most central sites which are protected by dedicated firewalls, remote systems may not warrant the expense and specialist skills to support these devices. Instead, a personal firewall can be used, which controls the flow of communications into (and sometimes out of) the remote computer. The administration of the rules (policies) of the firewall can be carried out remotely by personnel at the central site, relieving the remote system user of the requirement of technical understanding. However if this is not possible, care should be taken to ensure effective configuration, especially if those at the remote site are not IT literate. Some personal firewalls can also restrict the ability to transmit over the network to authorized programs (or even libraries), restricting the ability of malware to spread.

A.7 Virtual Private Networks

A.7.1 Background

A VPN is a private network which is implemented by using the infrastructure of existing networks. From a user perspective a VPN behaves like a private network, and offers similar functionality and services. A VPN can be used in various situations, such as to:

- implement remote access to an organization from mobile or off-site employees,
- link different locations of an organization together, including redundant links to implement a fall-back infrastructure,
- set up connections to an organization's network for other organizations/business partners.

In other words, VPNs allow two computers or networks to communicate over a medium such as the Internet. This communication has traditionally been performed at great expense by using leased lines with link encryptors. However with the advent of high-speed Internet links and suitable termination equipment at each end, reliable communications between sites can be established using VPNs.

A.7.2 Security Risks

The key security risk related to communications over an insecure network is that associated with sensitive information potentially being accessible to unauthorized parties - leading to unauthorized disclosure and/or modification. In addition to the security risks typically related to local and wide area networks (see Clauses A.1 and A.2 above respectively), the typical security risks related to VPNs include those associated with:

- insecure implementation through:
  - an untested or defective cipher suite,
  - a weak shared secret that could be easily guessed,
  - poor network topology,
  - uncertainty about the security of the remote client,
  - uncertainty about the authentication of users,

- uncertainty about the security of the underlying service provider,
- poor performance or availability of service,
- non compliance with regulatory and legislative requirements on the use of encryption in certain countries.

A.7.3 Security Controls

In VPNs, cryptographic techniques are commonly used and/or application protocols to implement security functionality and services, especially if the network on which the VPN is built is a public network (for example, the Internet). In most implementations the communications links between the participants are encrypted to ensure confidentiality, and authentication protocols are used to verify the identity of the systems connected to the VPN. Typically, the encrypted information travels through a secure 'tunnel' that connects to an organization's gateway, with the confidentiality and integrity of the information maintained. The gateway then identifies the remote user and lets the user access only the information they are authorized to receive.

Thus, a VPN is a mechanism based on protocol tunneling – treatment of one complete protocol (the client protocol) as a simple stream of bits and wrapping it up in another (the carrier protocol). Normally, the VPN carrier protocol provides security (confidentiality and integrity) to the client protocol(s). In considering the use of VPNs, the architectural aspects that should be addressed include:

- endpoint security,
- termination security,
- malicious software protection,
- strong authentication,
- intrusion detection,
- security gateways (including firewalls),
- encryption of data,
- network design,
- other connectivity,
- split tunneling,
- audit logging and network monitoring,
- technical vulnerability management.

Further detail on VPNs, including on each of these architectural aspects, is provided in ISO/IEC 27033-5.

A.8 Voice Networks

A.8.1 Background

There are PABXs available today that support traditional channel connected telephony to the PSTN. Call set-up information is passed between them using DPNSS (an industry standard interface defined between a PABX and an access network). DPNSS expands the facilities normally only available between extensions on a single PABX to all extensions on PABXs that are connected together in a private network. However, some years ago a new protocol was developed alongside DPNSS to both communicate between PABXs and to communicate between the PABX and the PSTN. This relates to an architecture for private ISDNs and an inter-exchange signaling protocol based upon the ISDN concepts specified in ITU-T Recommendations. The inter-exchange protocol, based on ITU-T Recommendation Q.931, has become known as QSIG. The signaling

protocols are robust and have not caused any security issues, but there are a number of security risks associated with traditional PABX telephone systems.

A.8.2 Security Risks

The security risks related to traditional telephony include those associated with:

- lack of back-up controls of site specific information, that could affect availability in certain circumstances,
- eavesdropping, if physical access can be gained to cabling,
- with the management ports liable to unauthorized intrusion as they are poorly protected with simple dial back systems, this could result in a PABX being re-programmed and used for fraud, or shut down),
- dial-through fraud, because the inter trunk barring tables are often poorly maintained thus permitting calls to be manually routed through a network and then sent out to the PSTN (in a number of cases this circumstance has resulted in major dial through fraud to premium rate numbers – with significant financial loss,
- fraud through ineffectual trunk to trunk barring allowing unauthorized call diversion and call set-up (with the fraud achieved using an associated voice messaging system to redirect calls out to the PSTN),
- lack of resilience and/or capacity, that could affect availability.

A.8.3 Security Controls

The security controls for voice networks could include ensuring that:

- it is not possible to gain physical access to cabling, junction boxes and frames,
- trunk to trunk barring tables are properly used to prevent unauthorized call routing,
- user access to routing codes is not possible,
- frequent system back-ups are taken, with copies taken and stored off site,
- PABXs are configured with multiple processors so that there are no single points of failure,
- battery or UPS power supplies are provided,
- multiple routes to the PSTN are provided, as relevant with selected fall-back analogue telephone lines for emergency use,
- strong authentication is used on all management channels (that may mean the use of additional third party equipment),
- dial-through fraud cannot be achieved, either through the use of unauthorized routing or via associated voice messaging systems,
- anti-spam devices,
- a call analysis system is installed and call costs are regularly checked,
- compliance reviews and testing of services are regularly carried out, and the results acted upon.

It is worth noting that ‘traditional’ PABX telephone systems are becoming obsolescent, and are either being partially migrated to, or replaced by, VoIP systems (see Clause 11.10 below).

A.9 IP Convergence

A.9.1 Background

As IP (data voice and video) convergence gains popularity, the security issues should be recognized and addressed. Although current telephony implementations require security controls to deter toll fraud and other security incidents, these systems are not integrated into the corporate data network and are not subject to the same risks as those associated with IP data networks. With the convergence of voice and data, security controls need to be implemented to reduce the risks associated with attacks.

A VoIP application typically consists of proprietary software hosted on open or commercially available hardware and operating systems. The number of servers depends on vendor implementation as well as the actual deployment. These components communicate via IP over Ethernet and are interconnected via switches and/ or routers.

A.9.2 Security Risks

The main areas of security risks can be associated with IP-based attacks on vendor-specific software vulnerabilities and the hardware or operating system platform hosting the VoIP application. The security risks related to VoIP components include those associated with attacks on network-based devices and applications, and can be enabled or facilitated by vulnerabilities in the design or implementation of the VoIP solution. The key security risks related to IP Convergence include those associated with:

- QoS – without an overall QoS there could be a loss of quality, or interruption of calls due to packet loss, and propagation delay across the network,
- unavailability of service due to DoS attacks, or changes to routing tables,
- integrity and availability can be affected by malicious code (including viruses) which can manage to enter the network through insecure VoIP systems that can degrade or even create a loss of service, and could spread to servers in the network, leading to damaged data storage,
- Spam over IP Telephony (SPIT),
- softphones on client PCs are a substantial risk as these could be an entry point for malicious code (including viruses) and intrusions,
- VoIP servers and VoIP management systems are at risk if not protected behind firewalls,
- data network security could be degraded due to multiple ports being opened on the firewalls to support VoIP. A VoIP session has numerous protocols and port numbers associated. H.323 uses numerous protocols for signaling, and both H.323 and SIP use RTP. The result is that a H.323 session can use up to eleven different ports,
- fraud is a key issue with telephony, and the risks can increase if security is not addressed when VoIP is used. Hackers could gain unauthorized access to the VoIP service by spoofing, replay attacks, or connection hijacking. Toll fraud, or unauthorized calls to premium rate numbers, could then result in substantial losses,
- breaches of confidentiality can occur through the interception of communications., such as man-in-the-middle, is possible within the network by employees and other staff with access to the network,
- eavesdropping of voice calls,
- since IP telephones require power to operate, the telephone network can not be operational in the case of power failure,
- there is a greater likelihood of failure of both voice and data services due to the use of common components, e.g. a LAN.

A.9.3 Security Controls

There are a number of technical security controls to manage the risks from identified threats to converged IP networks, which could include:

- QoS facilities should be implemented in a converged network, otherwise voice quality is likely to suffer. Network service delivery, and where possible, IP links should be delivered to a site over fiber to ensure that jitter (which affects voice quality) is minimized,
- all VoIP servers should be configured with malicious software protection,
- PC supporting softphones should be fitted with personal firewalls and the anti-malicious code (including anti-virus) checking software should be frequently updated,
- VoIP servers and VoIP management systems should be protected behind firewalls to safeguard them from attack,
- usage of dedicated VLANs for each service, and encryption of different data flows,
- designers should ensure that only the minimum number of ports are opened on firewalls to support VoIP services,
- to combat toll fraud anti spoofing, anti replay controls need to be implemented to prevent connection hijacking,
- all access to management servers should be authenticated,
- IDS should be considered for servers supporting VoIP services,
- encryption of the data path should be considered where sensitive information is to be discussed over a VoIP network,
- IP phones should be powered by switches supported by UPS,
- there may be a need to provide a conventional voice service, which has an independent power source for use in an emergency.

A.10 Web Hosting

A.10.1 Background

Web hosting services are offered by many network service providers in the form of a standardized service, often including database facilities for handling persistent data as well as a basic application runtime environment. Although most of the components needed to implement and offer web hosting services are out of scope for this standard (such as web server or database software), some considerations about the whole service itself are documented here as many people consider web hosting as an integral part of a network offering.

Web hosting sites are at risk from a variety of threats, particularly where they are connected to the Internet, for example where prominent organizations may be under attack from fringe groups. Thus, it is important that all potential threats are identified, and then all vulnerabilities which could be exploited by the threats are closed off. This is best achieved by designing out vulnerabilities. By addressing these issues in accordance with the guidance provided, it should be possible to design a web site, which is secure, reliable and has a low likelihood of being defaced.

A.10.2 Security Risks

The key security risks related to web hosting include those associated with:

- access by an attacker to application and data with a single breach of the perimeter protection,
- exposure to vulnerabilities in infrastructure component,
- multiple single points of failure,
- loss of service due to hardware failure,
- inability for to be taken out of service for maintenance,
- unintended access by public users to areas where data is stored,
- attacks against data integrity (e.g. web site defacement or hosting unauthorized content),
- malware being uploaded into the system,
- compromise of a web site using switching functionality,
- inability to take backups without affecting web site performance,
- unauthorized disclosure of an IP addressing plan facilitating attack on the web site,
- exploitation of connections between management stations and the Web site,
- undiscovered attack,
- difficulty in tracking intrusions between devices,
- inability to recover data,
- inability to meet service level agreement requirements,
- inability to maintain continuity of service,
- unauthorized use of web services, including violation of organization policy (e.g. using servers for own benefits) and non-compliance with legislation and regulation (e.g. storing material which violates copyright or storing child pornography).

A.10.3 Security Controls

The technical security controls to manage the risks from identified threats for web sites could include:

- the provision of zoning and security in depth to limit the effect of a successful attack,
- the specification of different firewall types to counter possible firewall vulnerabilities. (Further information on firewalls is provided in Clause A.6 above and ISO/IEC 27033-4.),
- resilience; the design should be examined for potential single points of failure and these should be eliminated,
- failover/load sharing to guard against equipment failure,
- clustering where high availability in a 24x7 environment is a requirement,
- proxying services to limit access into a web site and to enable a high degree of logging,
- regular integrity checks for unauthorized changes to data,

- anti-malicious code (including anti-virus) controls on uploads to prevent the import of malware,
- layer 2 switching normally used in a web site design. Layer 3 switching should not be used unless it is a business related requirements, such as for load sharing. In addition the same physical switch should not be used either side of a firewall. Test points should be included in the switch design,
- VLANs segregated by function to enable IDS to be more easily tuned as there is a reduced protocol set on any VLAN. In addition, the implementation of a backup VLAN will allow backups to operate at any time of the day without compromising the performance of the site,
- as relevant to business operations, the IP addressing plan to limit the number of public addresses to a minimum, with the IP addressing plan kept "in strictest confidence" as knowledge of it could be used to mount an attack on the web site,
- where management links are connected over public networks, they should be encrypted (see ISO/IEC 27033-4 for further information on remote access). This includes at least alerts/ SNMP traps on console port connections,
- all transaction and event logs from each device copied to an audit server, and then copied to a backup media, such as a CD,
- a time synchronization service implemented as it is key to analyzing unauthorized access and being able to follow the traces through the log files. This requires that the timing of all log files, and hence servers, is synchronized to plus/ minus 1 second or lower. (NTP is relevant here; for further information see ISO/IEC 27002, Clause 10.6.),
- LAN devices configured to control unmanaged changes to MAC addresses,
- a centralized backup service, preferred as this is more likely to be performed as required,
- with web sites needed in most cases to be operating 24 hours per day, this requires high quality hardware that can withstand the environment. The server infrastructure in a web site should be specified to support "24 x 7" operations. The supporting operating systems should be hardened, and all servers and other devices should then undergo security testing to ensure that all devices are fully hardened,
- robust application software implemented, where code has been checked for structure, that is logically correct, and uses approved authentication software.

It should also be noted that business continuity management issues are often not fully considered when designing a web site. Full business continuity management activities should be conducted in relation to web sites.

A.11 Internet E-Mail

A.11.1 Background

The opening up of Internet services to an organization/community to meet legitimate business requirements brings with it a variety of threats which can be used to exploit vulnerable systems. Thus, Internet e-mail can be at risk from a variety of threats, and the target is to design and implement a solution that is secure and reliable. Figure 7 below shows an example potential solution for Internet e-mail.

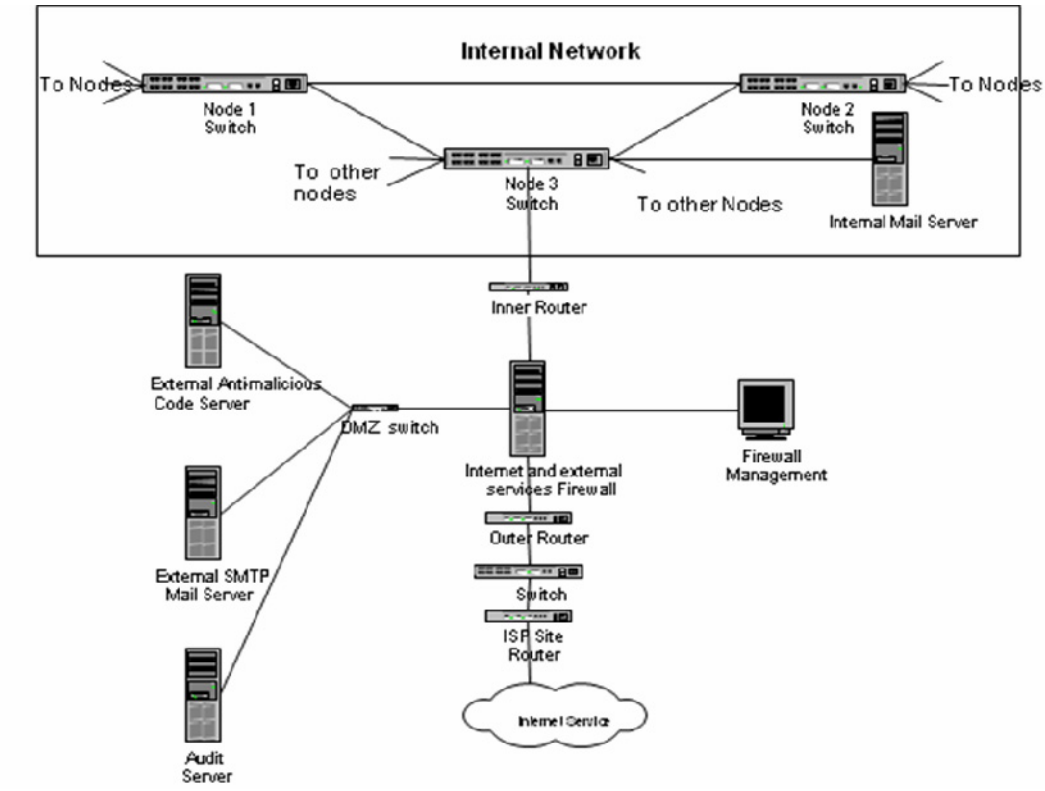


Figure A.1 — Example Internet E-mail Solution

Internet (SMTP) mail systems are fairly simple to deal with in a network technical security architecture as they only have to check and forward mail that has been received. The information to be gathered should include:

- the expected number of messages per day in each direction,
- the type of message and content of the messages that are to be permitted,
- the number and size of messages per day in each direction,
- the average and maximum sizes of messages permitted,
- details of the internal mail system,
- details of the internal mail relay, which will communicate with the mail relay defined in the technical security architecture,
- details of the external mail system(s) (which could be with any mail relay on the Internet, or it could be one specific mail server owned by a service provider),
- details of the mail server authentication requirements for internal communications, and to Internet mail communications,
- details of internal WINS/DNS facilities,
- details of DNS facilities for the Internet,
- if relevant, what access to newsgroups is required and if so are there to be any restrictions placed on what newsgroups can be accessed,
- whether mail/server time synchronization will be required from the Internet,
- whether there is to be more than one route to the Internet,
- requirements for scanning for malicious code (including viruses).

A.11.2 Security Risks

The key security risks related to Internet e-mail include those associated with:

- unauthorized intrusions into an organization's/community's network. Attempts at unauthorized access, including by identity impersonation, could be made 24 h per day, are becoming more sophisticated and creative and can be malicious such as leading to a DoS attack, misusing resources or gaining valuable information,
- uploading of malicious code, which could include the introduction of a Trojan that collects information such as passwords and sends these back out to a remote location or facilitates taking over control of a remote device. Thus, attention should be paid to the more recent 'blended' threats where malicious code contains a 'payload',
- upload of spam (spam is a significant threat to e-mail services – it can adversely affect e-mail activities by consuming network resources to route spams and also system resources for mail gateways, and can be used to propagate malware),
- relaying of spam (if a mail server was configured to allow anonymous mail relay, it could be used by spammers to send spam via the Internet in the name of the organization owning the mail server),
- e-mail spoofing (it is very easy to impersonate the identity of any user to pretend to be someone sending e-mail),
- content forging,
- unmonitored content leaving the organization without the knowledge of information security personnel, which introduces legal implications and potential losses of intellectual property,
- direct DoS attack against the mail system,
- distributed DoS attack where thousands of e-mails are sent from multiple locations to overwhelm the mail server.

A.11.3 Security Controls

The security controls for Internet e-mail could include:

- firewalls used that have assurance levels and rule sets appropriate to the assessed risks. For most security purposes, the initial firewall rule set should be to deny the passage of all traffic across the firewall. For e-mail, it is normal for an e-mail server to send data out to the Internet and to receive incoming data from the Internet. Here, the firewall rule set would be set up to allow the two-way sending of e-mail data. As mentioned earlier, it is advisable to have two firewalls in series that are from different vendors or have different operating systems,
- filing and audit capabilities supported by a fully synchronized time service across all infrastructure components, firewalls and servers. This time synchronization must be addressed in the design, with a description of the master clock and a hierarchy plan for servers and network(s). Often the master clock will be synchronized via either a satellite global positioning service (GPS) or a terrestrial radio time service,
- the Internet (SMTP) mail transport system properly established to fulfil the required security related tasks, including the provision of the interface to the organization/community from the Internet, the transfer of mail from the Internet to the internal mail server and vice versa, the prevention of the relay of mail from the Internet to another addressee on the Internet, and assurance that mail and attachments are malicious code free regardless of the direction,
- for any incoming mail, as a result of a look-up on an Internet DNS server, messages directed to the organization's firewall address and, when received from the Internet checked by the outer router for a source address field outside of the internal address space before being directed to the firewall. At the firewall, the message should be checked for an address field outside the internal address space and the

destination address of the mail server (and of course that it was an e-mail), and then be directed to the SMTP mail server. At the SMTP mail server, the message should be checked that it was from the Internet and that the destination address was for an internal address, and then be directed to the external anti-malicious code server for checking for viruses and any other malicious content. Finally, it should then be sent to the internal mail server for distribution by the internal mail system. Any messages received with an incorrect address should be rejected and an entry included in the log. Any message received with a virus or other malicious content should be quarantined and the appropriate person or group informed,

- for any outgoing mail, messages forwarded via the Internet should first be sent from the internal mail server to the external anti-malicious code server for checking for viruses and any other malicious content before being sent to the external SMTP mail server for direction to the Internet. The external SMTP mail server should check that the address is outside the internal address space and that it was not destined for any other mail routes, and then forward the message to the Internet,

- choosing one of the two options of the external SMTP mail server sending the message to a single ISP mail server for onward routing or to any valid mail address on any mail server. The first option should be the most secure as it means that the (presumably mail expert) ISP is responsible for organizing and supporting the forwarding of mail, but could introduce delays in mail transmission. The second option is much more flexible and would not incur delays due to ISP forwarding, but it could be less secure if not properly managed – with the organization/community having to support mail to many mail servers and running the risk of rejection if its mail relay is not recognized by the remote mail server, albeit that this could be overcome by authentication procedures between the corresponding mail servers. Which option is chosen depends on the technical merits of the solution and the level of expertise of those that will support the mail system,

- access control measures implemented based on the principle of least privilege,

- the e-mail server configured to block or remove e-mails that contain file attachments that are commonly used to spread malicious code, such as: .vbs, .bat, .exe, .pif and .scr files,

- infected computers being quickly removed from the network to prevent further compromise, and forensic analysis being performed and restoration accomplished using trusted media,

- staff trained not to open attachments unless they are expecting them, and not to execute software that is downloaded over the Internet unless it has been scanned for malicious code,

- ACLs used on routers. Router ACLs specify how to handle an incoming IP packet, with typical actions including forward, log, and drop (or deny). Combined with the appropriate router default policy (e.g. deny all), it is possible to define a rule set for a router which greatly assists in maintaining the security of the underlying network,

- anti-spoofing enabled. Spoofing typically refers to the situation where the source (originating) address of a message appears to come from someone or somewhere other than that of the true originator. Anti-spoofing measures take the form of not accepting the message from the Internet if it claims to have originated from inside the organization, and vice versa (see RFC2827, Network Ingress Filtering: Defeating Denial of Service, for more detail),

- e-mail proxies enabled. A proxy server is a server that acts as an intermediary between a PC/workstation user and the Internet so that the enterprise can ensure security, administrative control and caching service. Security is enforced as follows:

  - scanning the data for known patterns (for example, to check for sensitive words for compliance assurance),

  - translating between internal and external addresses,

  - creating a log of requests and requesters,

  - anti-malicious code facilities based at the proxies,

The proxy servers can also check for malicious content by simply processing the request. If the request is malicious, there is a likelihood that the proxy server itself will crash. As proxies are generally implemented in the DMZ, a semi-trusted zone, this behaviour acts as a 'fuse' to protect the real requester or server,

- anti-malicious code controls implemented on e-mail proxies. Once information systems are shown to be free of malicious code (including viruses), the only route for malicious code to be introduced is by introduction as data (or programs). Thus, e-mail facilities are prime candidates for transmission of malicious code, and represent prime points for the implementation of anti-malicious code controls. Typical controls include facilities to quarantine suspicious files (for example, by content type), and screening of requested e-mail addresses against a blacklist. Further, to deal with the more recent blended threats, where malicious code contains a payload, blocking of certain attachments containing executable code needs to be considered,

- anti-spam technologies deployed and users educated on protecting their e-mail addresses when accessing sites,

- anti-relay implemented on e-mail servers and reverse DNS look-ups. One of the possible ways in which an e-mail server can be exploited from the Internet is to send it a message which is actually destined for a third party. Then if the e-mail server accepts the message it will be forwarded to the third party, apparently from the organization/community rather than its true originator. This mechanism can be used by 'spammers' or to overwhelm the third party's network by a DoS attack. Anti-relay controls detect if an incoming e-mail is for the organization/community. If not, the e-mail is logged (or quarantined) and the e-mail server takes no further action,

- alerts and SNMPv3 traps enabled. SNMP can be used for the remote control of a networked device, and for the device to send messages (or 'traps') to notify a monitoring station of conditions at that device. The protocol is relatively insecure, and tends not to be used for device control purposes. However, SNMP traps are widely used and are transmitted via the network to notify a central location of statistics or error conditions,

- audit management implemented. All logs pertaining to e-mail should be captured to an audit server, and checked daily for unusual activity. This includes the logs from the firewall and the e-mail SMTP proxy. The logs should be examined using a quality event correlation and analysis tool,

- 'out of band' (OOB) firewall management instituted. This refers to the practice of using different networks for data and management to ensure it is not possible for an attacker to connect to their target device (firewall, in this instance). Many mechanisms exist to implement OOB management:

  - management by physical access only,

  - separate management network,

  - use of VLANs to create separate channels over the data network, allowing data and management traffic to be segregated,

Otherwise management should be by physical access only.

A.12 Routed Access to Third Party Organizations

A.12.1 Background

Third party connections are on the increase as organizations move towards more collaborative working, which requires a direct connection and gateway facilities between the organizations. Figure 8 below shows an example technical security solution for routed access to third party organizations.

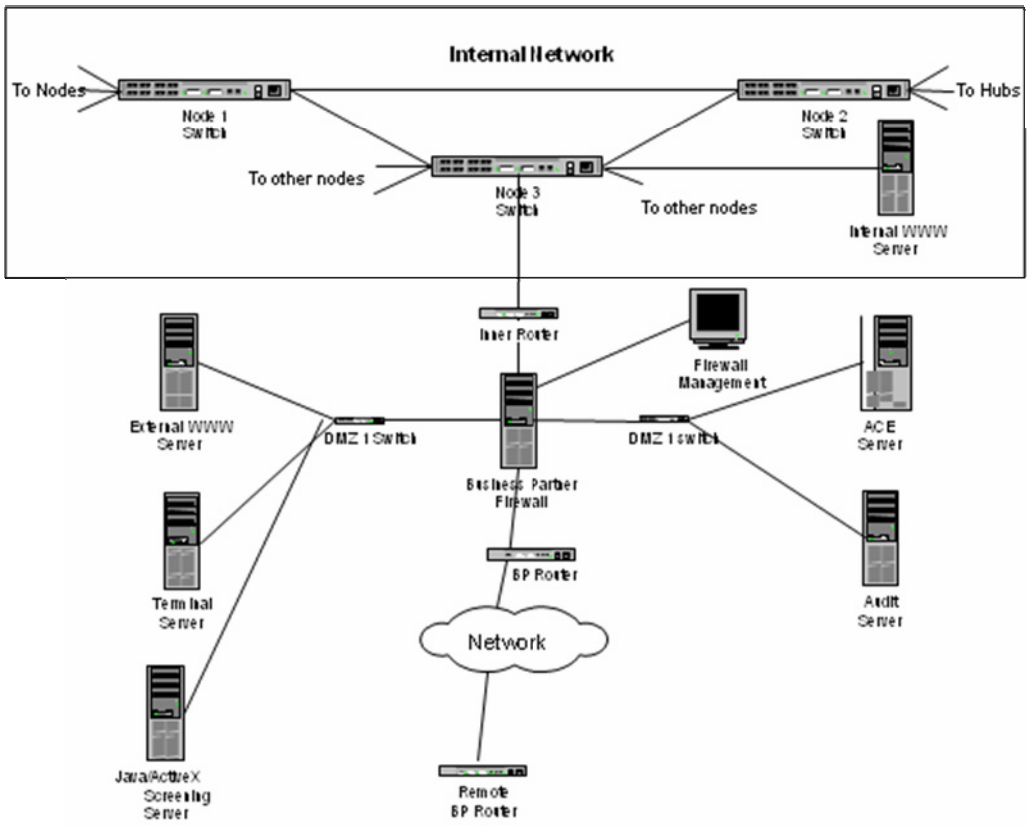


Figure A.2 — Example Routed Access to Third Party Organizations Solution

Routed access to other organizations could be made via a WAN technologies or broadband, and be required for many reasons, e.g. access can be required to database applications in either direction – in which case either way unauthorized code could be introduced or unauthorized access could be attempted by users within either network to the other. The information to be gathered should include, for example:

- what applications are to be supported over the routed link,
- details of communicating servers and where they are located,
- details of the user PCs and where they are located,
- details of the third party router if it exists (including IP address, method of authentication, e.g. digital certificates, shared secret, RADIUS, TACACS+),
- communications link type and speed, e.g. VPN over broadband, frame relay, private wire link, dial-up and ISDN.

It is also sensible that for each third party access, a configuration document is produced, if it does not already exist, that includes an overview of the requirement, a network diagram, configuration information and details of IP addressing and authentication.

(When considering routed access to third party organizations it would be sensible to refer to ISO/IEC TR 14516:1999 - Guidelines on use and management of Trusted Third Party Services.)

A.12.2 Security Risks

The key security risks related to routed access to third party organizations are principally associated with the fact that any third party is a separate security domain with its own policies – and may not be as secure as your organization. Thus, the key security risks related to routed access to third party organizations include those associated with:

- unauthorized access to your network and related 'systems' and information,
- importation of malicious code through an apparently trusted gateway,
- DoS attack via the third party,
- a belief that the third party network offers a higher level of security than the Internet.

A.12.3 Security Controls

The security controls for routed access to third party organizations could include:

- all third party connections isolated by a different firewall to that used for the Internet and other classes of external connections,
- anti-malicious code software in place, including that which works with the firewall to check for Java and ActiveX code (as mentioned earlier, such code is not recognized by regular anti-malicious code (including anti-virus) software as a virus and thus cannot be detected and checked to see if it is valid or not),
- strong token or card based authentication in place, by way of either digital certificates on key fobs or smartcards or by two factor authentication with tokens,
- if connections are via ISDN routed access, CLID used as an additional authentication method,
- routers, including at the remote end of the connection, authenticated via an authentication server, such as TACACS+. However, if no agreement can be reached for the method of authentication with the third party then shared secrets can be used where there is a small deployment, which is an exchange of passwords. For large numbers of connections, digital certificates should be used as these can be regularly changed,
- the third party router using the same means of authentication, e.g. digital certificates, shared secret, RADIUS, TACACS+,
- routers at both ends of the link kept physically secure,
- all third party connections covered by a conditions for secure connection document that is signed by each third party organization before any connection is permitted,
- consideration of use of IDS/IPS,
- audit and accounting implemented,
- for each third party access, a configuration document produced and agreed that includes an overview of the requirement, a network diagram, configuration information and details of the IP addressing and authentication method.

A.13 Intranet Data Center

A.13.1 Background

The Intranet data center houses most of the critical applications and data for the organization. The Data Center could be a critical part of an organizations infrastructure and has unique concerns beyond those of the other aspects of the network covered in other parts of this annex. Although storage (SANs) and the individual host aspects in a data center are out of scope of this standard (such as hardening of servers or databases), some considerations about the overall security of the data center are documented here.

Threats facing today IT security administrators have grown from the relatively trivial attempts to wreak havoc on networks into sophisticated attacks aimed at profit and the theft of sensitive corporate data. Implementation of robust data center security capabilities to safeguard sensitive mission-critical applications and data is a cornerstone in the effort to secure enterprise networks.

Because a key responsibility of security for the data center is to maintain the availability of services, the ways in which security affects traffic flows, scalability, and failures must be carefully considered.

A.13.2 Security Risks

Attack vectors have moved higher in the stack to subvert network protection and aim directly at applications. HTTP-, XML-, and SQL-based attacks are useful efforts for most attackers because these protocols are usually allowed to flow through the enterprise network and enter the intranet data center.

The following are some of the threat vectors affecting the Intranet data center:

– unauthorized access to data,

– unauthorized access to applications,

– unauthorized device access,

– interruption of critical services through DoS attacks,

– undiscovered attacks,

– loss of data,

– inability to recover data,

– targeted attacks to modify data,

– privilege escalation,

– installation of malware

– unauthorized use of services, including violation of organization policy.

A.13.3 Security Controls

The technical security controls for data centers could include:

- security gateways to control access into the data center.
- use of IPS/IDS in the data center,
- anti-malicious code (including anti-virus) controls on hosts,
- secure management of infrastructure devices,
- logging and audit capabilities supported by a fully synchronized time service across all components in the data center,
- a business continuity plan for failures,
- resilient design,
- regular integrity checks for unauthorized changes to data,
- VLANS to segregate services within the data center to protect more sensitive services,
- LAN devices configured to control unmanaged changes to MAC addresses,
- use of secure management protocols.

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

Table B.1 — Cross references between ISO/IEC 27001 and ISO/IEC 27002, and clauses within this part of ISO/IEC 27033

ISO/IEC 27001 and ISO/IEC 27002 Clause	Provisions	ISO/IEC 27033-1 Clause
10.4.1 Controls against malicious code	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	8.7 Protection against Malicious Code
10.4.2 Controls against mobile code	Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.	7.2.2.2 Network Architectures, Applications and Services
10.6.1- Network Controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	See below against ISO/IEC 27001/27002 clauses 10.6.1 IG a) to e).
10.6.1 IG a)	Operational responsibility for networks should be separated from computer operations where appropriate.	8.2 Management of Network Security.
10.6.1 IG b)	Responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established.	11.7 Remote Access Services. (More detailed information can be found in ISO/IEC 27033-5.)
10.6.1 IG c)	Special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications (see 11.4 and 12.3); special controls may also be required to maintain the availability of the network services and computers connected.	All controls in 11. Technology topics – risks, design techniques and control issues.
10.6.1 IG d)	Appropriate logging and monitoring should be applied to enable recording of security relevant actions.	8.5 Network Audit Logging and Monitoring.
10.6.1 IG e)	Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.	8.2 Management of Network Security.

Table B.1 *(continued)*

10.6.2 – Security of Network Services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	8.2 Management of Network Security (and relating to other clause 8 sub-clauses, and clauses 9 to 11).
10.8.1 Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	6.2 Network Security Planning and Management
10.8.4 Electronic messaging	Information involved in electronic messaging should be appropriately protected.	A.11 Internet E-Mail
10.9.1 Electronic commerce	Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	10.4 Business to Business Services 10.5 Business to Customer Services
10.9.2 On-Line Transaction	Information involved in on-line transactions should be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	10.5 Business to Customer Services
10.9.3 Publicly available information	The integrity of information being made available on a public available system should be protected to prevent unauthorized modification.	A.10 Web Hosting
11.4.1 Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.	8.2.2.2 Network Security Policy
11.4.2 User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.	8.4 Identification and Authentication
11.4.3 Equipment identification in networks	Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.	
11.4.4 Remote diagnostic and configuration port protection	Physical and logical access to diagnostic and configuration ports should be controlled.	
11.4.5 Segregation in networks	Groups of information services, users, and information systems should be segregated on networks.	

Table B.1 *(continued)*

11.4.6 Network connection control	For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of business applications.	11. 'Technology' topics – risks, design techniques and control issues
11.4.7 Network routing control	Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.	A.6 Security Gateways

Table B.2 — Cross references between clauses within this part of ISO/IEC 27033 and ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC 27033-1 Clause	Provisions	ISO/IEC 27001 and ISO/IEC 27002 Clause
6	Overview	
6.2	Network Security Planning and Management	10.8.1 Information exchange policies and procedures
7	Identifying Risks and Preparing to Identify Security Controls	
7.2	Information on Current and/or Planned Networking	
7.2.1	Security Requirements in Corporate Information Security Policy	
7.2.2	Information on Current/Planned Networking	
7.2.2.2	Network Architectures, Applications and Services	10.4.2 Controls against mobile code
7.2.2.3	Types of Network Connection	
7.2.2.4	Other Network Characteristics	
7.2.2.5	Other Information	
7.3	Information Security Risks and Potential Control Areas	
8.2	Management of Network Security	10.6.1 Network Controls
8.2.2	Network Security Management Activities	
8.2.2.2	Network Security Policy	5.1 Information Security Policy
		11.4.1 Policy on use of network services
8.2.2.3	Network Security Operating Procedures	
8.2.2.4	Network Security Compliance Checking	
8.2.2.5	Security Conditions for Network Connection	

Table B.2 *(continued)*

8.2.2.6	Documented Security Conditions for Remote Network Users	
8.2.2.7	Network Security Incident Management	13 Information Security Incident Management
8.2.3	Network Security Roles and Responsibilities	8.1.1 Roles and responsibilities
8.2.4	Network Monitoring	10.10 Monitoring
8.2.5	Evaluating Network Security	
8.3	Technical Vulnerability Management	12.6 Technical Vulnerability Management
8.4	Identification and Authentication	11.4.2 User authentication for external connections
		11.5.2 User Identification and Authentication
8.5	Network Audit Logging and Monitoring	10.6.1 Network Controls
		10.10.1 Audit Logging
8.6	Intrusion Detection and Prevention	
8.7	Protection against Malicious Code	10.4 Protection against Malicious and Mobile Code
8.8	Cryptographic Based Services	12.3 Cryptographic Controls
8.9	Business Continuity Management	14 Business Continuity Management
9	Guidelines for the Design and Implementation of Network Security	
9.2	Network Technical Security Architecture/Design	
10	Reference Network Scenarios – Risks, Design, Techniques and Control Issues	
10.2	Internet Access Services for Employees	
10.3	Enhanced Collaboration Services	
10.4	Business to Business Services	10.9.1 Electronic commerce
10.5	Business to Customer Services	10.9.1 Electronic commerce
		10.9.2 On-Line Transaction
10.6	Outsourcing Services	
10.7	Network Segmentation	
10.8	Mobile Communications	
10.9	Network Support for Traveling Users	
10.10	Network Support for Home and Small Business Offices	
11	'Technology' Topics – Risks, Design Techniques and Control Issues	10.6.1 Network controls
		11.4.6 Network connection control
12	Develop and Test Security Solution	
13	Operate Security Solution	
14	Monitor and Review Solution Implementation	

Table B.2 *(continued)*

Annex A	'Technology' Topics – Risks, Design Techniques and Control Issues	
A.1	Local Area Networks	
A.2	Wide Area Networks	
A.3	Wireless Networks	
A.4	Radio Networks	
A.5	Broadband Networks	
A.6	Security Gateways	11.4.7 Network routing control
A.7	Virtual Private Networks	
A.8	Voice Networks	
A.9	IP Convergence	
A.10	Web Hosting	10.9.3 Publicly available information
A.11	Internet E-Mail	10.8.4 Electronic messaging
A.12	Routed Access to Third Party Organizations	

Annex C
(informative)

Example Template for a SecOPs Document

1 Introduction

- 1.1 Background
- 1.2 Document Structure

2 Scope

- 2.1 Locations
- 2.2 Technical Infrastructure
  - 2.2.1 IT Environment
  - 2.2.2 Network Architecture
  - 2.2.3 Location 1
  - 2.2.4 Location 2
  - 2.2.5 Location 3
  - 2.2.6 External Connections

3 Security Policy

4 Organizing Information Security

- 4.1 Introduction
- 4.2 Security Management Structure and Responsibilities
  - 4.2.1 Organization Security Officer
  - 4.2.2 Deputy Organization Security Officer
  - 4.2.3 Organization Information Security Officer
  - 4.2.5 IT Support Team (as relevant)
  - 4.2.6 Business Area Managers
  - 4.2.7 Staff
  - 4.2.8 Organization Management Board
- 4.3 Information Security Incident and Weakness Reporting
- 4.4 Distribution of SecOPs
- 4.5 Assessment of Risks Associated with External Parties
- 4.6 Agreements on External (Third) Party Access
- 4.7 Outsourcing

5 Asset Management

- 5.1 Inventory of Assets
- 5.2 Acceptable Use of Information and other Assets
- 5.3 Information Classification

6 Human Resources Security

- 6.1 Minimum Personnel Security, including Clearance, Requirements
- 6.2 Terms and Conditions
- 6.3 Information Security Awareness and Training
- 6.4 Disciplinary Process
- 6.5 Monitoring of Personnel
- 6.6 Termination of Employment
- 6.7 Security Access Cards/Building Passes
- 6.8 Physical Access to IT Systems and Networks

Bibliography

[1] ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model: The Basic Model*

[2] ISO/IEC 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Security Architecture*

[3] ISO/IEC 7498-3:1997, *Information technology — Open Systems Interconnection — Basic Reference Model: Naming and Addressing*

[4] ISO/IEC 7498-4:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Management Framework*

[5] ISO/IEC 9595-8, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*

[6] ISO/IEC 10181-1: 1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

[7] ISO 11166-2, *Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using the RSA cryptosystem*

[8] ISO 11568 (all parts), *Banking — Key management (retail)*

[9] ISO 11649, *Financial services — Core banking — Structured creditor reference to remittance information*

[10] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[11] ISO/IEC 11889-1, *Information technology — Trusted Platform Module — Part 1: Overview*

[12] ISO/IEC 11889-2, *Information technology — Trusted Platform Module — Part 2: Design principles*

[13] ISO/IEC 11889-3, *Information technology — Trusted Platform Module — Part 3: Structures*

[14] ISO/IEC 11889-4, *Information technology — Trusted Platform Module — Part 4: Commands*

[15] ISO 13492, *Financial services — Key management related data element — Application and usage of ISO 8583 data elements 53 and 96*

[16] ISO/IEC 13888:2004 (all parts), *Information technology — Security techniques — Non-repudiation*

[17] ISO/IEC 14516:1999, *Information technology — Security techniques — Guidelines for the use and Management of Trusted Third Party services*

[18] ISO/IEC 15288:2008, *Systems and software engineering — System life cycle processes*

[19] ISO/IEC 18043:2006, *Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDS)*

[20] ISO/IEC TR 18044:2004[2)], *Information technology — Security techniques — Information security incident management*

[21] ISO 21118, *Information to be included in specification sheets — Data projectors*

[22] ISO/PAS 22399:2007, *Societal security — Guidelines for incident preparedness and operational continuity management*

[23] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems implementation guidance*

[24] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[25] IETF *Site Security Handbook* (RFC 2196), September 1997

[26] IETF *IP Security Document Roadmap* (RFC 2411), November 1998

[27] IETF *Security Architecture for the Internet Protocol* (RFC 2401), November 1998

[28] IETF *Address Allocation for Private Internets* (RFC 1918), February 1996

[29] IETF *SNMP Security Protocols* (RFC 1352), July 1992

[30] IETF *Internet Security Glossary* (RFC 2828), May 2000

[31] IETF *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing* (RFC 2827), May 2000

[32] NIST Special Publications (800 series) on *Computer Security*

[33] NIST Special Publication 800-10: *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* December 1994.

2) ISO/IEC TR 18044 will be canceled and replaced following the publication of ISO/IEC 27035.

ICS 35.040

Price based on 73 pages