INTERNATIONAL STANDARD

ISO/IEC 18028-1

First edition
2006-07-01

Information technology — Security techniques — IT network security —

Part :1
Network security management

Technologies de /'information — Techniques de securite — Securite de reseaux Tl —

Partie 1: Gestion de securite de r&seau

Reference number
ISO/IEC **18028-1**:2006(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 v
Introduction vi
1 Scope 1
2 Normative references 1
3 Terms and definitions 2
3.1 Terms defined in other International Standards 2
3.2 Terms defined in this part of ISO/IEC 18028 2
4 Abbreviated terms 7
5 Structure 9
6 Aim 10
7 Overview 10
7.1 Background 10
7.2 Identification Process 12
8 Consider Corporate Information Security Policy Requirements 15
9 Review Network Architectures and Applications 15
9.1 Background 15
9.2 Types of Network 16
9.3 Network Protocols 16
9.4 Networked Applications 17
9.5 Technologies Used to Implement Networks 17
9.5.1 Local Area Networks 17
9.5.2 Wide Area Networks 18
9.6 Other Considerations 18
10 Identify Types of Network Connection 18
11 Review Networking Characteristics and Related Trust Relationships 20
11.1 Network Characteristics 20
11.2 Trust Relationships 20
12 Identify the Information Security Risks 22
13 Identify Appropriate Potential Control Areas 27
13.1 Background 27
13.2 Network Security Architecture 27
13.2.1 Preface 27
13.2.2 Local Area Networking 29
13.2.3 Wide Area Networking 31
13.2.4 Wireless Networks 32
13.2.5 Radio Networks 33
13.2.6 Broadband Networking 35
13.2.7 Security Gateways 36
13.2.8 Remote Access Services 37
13.2.9 Virtual Private Networks 38
13.2.10 IP Convergence (data, voice, video) 39
13.2.11 Enabling Access to Services Provided by Networks that are External (to the Organization) 41
13.2.12 Web Hosting Architecture 42
13.3 Secure Service Management Framework 44
13.3.1 Management Activities 44

13.3.2 Networking Security Policy....44
13.3.3 Security Operating Procedures....45
13.3.4 Security Compliance Checking....45
13.3.5 Security Conditions for Connection....45
13.3.6 Documented Security Conditions for Users of Network Services....46
13.3.7 Incident Management....46
13.4 Network Security Management....46
13.4.1 Preface....46
13.4.2 Networking Aspects....46
13.4.3 Roles and Responsibilities....48
13.4.4 Network Monitoring....49
13.4.5 Evaluating Network Security....49
13.5 Technical Vulnerability Management....49
13.6 Identification and Authentication....49
13.6.1 Background....49
13.6.2 Remote Log-in....49
13.6.3 Authentication Enhancements....50
13.6.4 Remote System Identification....50
13.6.5 Secure Single Sign-on....51
13.7 Network Audit Logging and Monitoring....51
13.8 Intrusion Detection....52
13.9 Protection against Malicious Code....53
13.10 Common Infrastructure Cryptographic Based Services....54
13.10.1 Preface....54
13.10.2 Data Confidentiality over Networks....54
13.10.3 Data Integrity over Networks....54
13.10.4 Non-Repudiation....54
13.10.5 Key Management....55
13.11 Business Continuity Management....57
14 Implement and Operate Security Controls....58
15 Monitor and Review Implementation....58
Bibliography....59

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 should not be held responsible for identifying any or all such patent rights.

ISO/IEC 18028-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* Subcommittee SC 27, *IT Security techniques.*

ISO/IEC 18028 consists of the following parts, under the general title *Information technology— Security techniques — IT network security.*

— *Part 1: Network security management*

— *Part 2: Network security architecture*

— *Part 3: Securing communications between networks using security gateways*

— *Part 4: Securing remote access*

— *Part 5: Securing communications across networks using virtual private networks*

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks, and should meet the business requirements for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability 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 end-to-end security solution. Thus, the purpose of ISO/IEC 18028 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 standard to meet their specific requirements. Its main objectives are as follows:

— in ISO/IEC 18028-1, to define and describe the concepts associated with, and provide management guidance on, network security - including on how to identify and analyze the communications related factors to be taken into account to establish network security requirements, with an introduction to the possible control areas and the specific technical areas (dealt with in subsequent parts of ISO/IEC 18028);

— in ISO/IEC 18028-2, to define a standard security architecture, which describes a consistent framework to support the planning, design and implementation of network security;

— in ISO/IEC 18028-3, to define techniques for securing information flows between networks using security gateways;

— in ISO/IEC 18028-4, to define techniques for securing remote access;

— in ISO/IEC 18028-5, to define techniques for securing inter-network connections that are established using virtual private networks (VPNs).

ISO/IEC 18028-1 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.

ISO/IEC 18028-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-3 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network managers, administrators, engineers and network security officers).

ISO/IEC 18028-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of remote access security (for example network managers, administrators, engineers, and network security officers).

ISO/IEC 18028-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network managers, administrators, engineers, and network security officers).

Information technology— Security techniques— IT network security —

Parti:
Network security management

1 Scope

ISO/IEC 18028-1 provides direction with respect to networks and communications, including on the security aspects of connecting information system networks themselves, and of connecting remote users to networks. It is aimed at those responsible for the management of information security in general, and network security in particular. This direction supports the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, provides an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and provides an overview of the possible control areas including those technical design and implementation topics dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

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 18028-2:2005, *Information technology — Security techniques — IT network security — Part 2: Network security architecture*

ISO/IEC 18028-3:2005, *Information technology — Security techniques — IT network security — Part 3: Securing communications between networks using security gateways*

ISO/IEC 18028-4:2005, *Information technology — Security techniques — IT network security — Part 4: Securing remote access*

ISO/IEC 18028-5:2006, *Information technology — Security techniques — IT network security — Part 5: Securing communications across networks using virtual private networks*

ISO/IEC 13335-1:2004, *Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management*

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*

ISO/IEC 18044:2004, *Information technology — Security techniques — Information security incident management*

ISO/IEC 18043:2006, *Information technology— Security techniques — Selection, deployment and operations of intrusion detection systems*

3 Terms and definitions

3.1 Terms defined in other International Standards

For the purposes of this document, the terms and definitions given in ISO/IEC 7498 (all parts) and the following terms defined in ISO/IEC 17799 and ISO/IEC 13335-1 apply: accountability, asset, authenticity, availability, baseline controls, confidentiality, data integrity, impact, integrity, security policy, non-repudiation, reliability, risk, risk analysis, risk assessment, risk management, control, threat and vulnerability.

3.2 Terms defined in this part of ISO/IEC 18028

For the purposes of this document, the following terms and definitions apply.

3.2.1
alert
'instant' indication that an information system and network may be under attack, or in danger because of accident, failure or people error

3.2.2
attacker
any 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

3.2.3
audit
formal inquiry, formal examination, or verification of facts against expectations, for compliance and conformity

3.2.4
audit logging
gathering of data on information security events for the purpose of review and analysis, and ongoing monitoring

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

3.2.6
business continuity management
process to ensure that recovery of operations will be assured should any unexpected or unwanted incident occur that is capable of negatively impacting the continuity of essential business functions and supporting elements

NOTE The process should also ensure that recovery is achieved in the required priorities and timescales, and subsequently all business functions and supporting elements will be recovered back to normal. The key elements of this process need to ensure that the necessary plans and facilities are put in place, and tested, and that they encompass information, business processes, information systems and services, voice and data communications, people and physical facilities.

3.2.7
Comp128-1
proprietary algorithm that was initially used by default in SIM cards

3.2.8
demilitarized zone
DMZ
perimeter network (also known as a screened sub-net) inserted as a "neutral zone" between networks

NOTE It forms a security buffer zone.

3.2.9
denial of service
DoS
prevention of authorized access to a system resource or the delaying of system operations and functions

3.2.10
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

3.2.11
filtering
process of accepting or rejecting data flows through a network, according to specified criteria

3.2.12
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 to another, and vice versa, traverses and only authorized traffic, as defined by the local security policy, is allowed to pass

3.2.13
hub
network device that functions at layer 1 of the OSI reference model (ISO/IEC 7498-1)

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

3.2.14
information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant

NOTE See ISO/IEC 18044.

3.2.15
information security incident
that indicated by 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

NOTE See ISO/IEC 18044.

3.2.16
information security incident management
formal process of responding to and dealing with information security events and incidents

NOTE See ISO/IEC 18044.

3.2.17
internet
global system of inter-connected networks in the public domain

3.2.18
intranet
private network established internally in an organization

3.2.19
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

3.2.20
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 to include how and when it occurred

NOTE See ISO/I EC 18043.

3.2.21
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/I EC 18043.

3.2.22
intrusion prevention system
IPS
variant on intrusion detection systems that are specifically designed to provide an active response capability

NOTE See ISO/IEC 18043.

3.2.23
jitter
one form of line distortion caused when a transmitted signal deviates from its reference

3.2.24
malware
malicious software, such as a virus or a trojan horse, designed specifically to damage or disrupt a system

3.2.25
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.

3.2.26
network administration
day-to-day operation and management of network processes and users

3.2.27
network analyzer
device used to capture and decode information flowing in networks

3.2.28
network element
information system that is connected to a network

NOTE The detailed description of security element is given in ISO/IEC 18028-2.

3.2.29
network management
process of planning, designing, implementing, operating, monitoring and maintaining a network

3.2.30
network monitoring
process of continuously observing and reviewing data recorded on network activity and operations, including audit logs and alerts, and related analysis

3.2.31
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

3.2.32
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 the HTTP protocol.

3.2.33
privacy
right of every individual that his/her private and family life, home and correspondence are treated in confidence

NOTE There should be no interference by an authority with the exercise of this right except where it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, the protection of health or morals, or for the protection of the rights and freedoms of others.

3.2.34 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

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

3.2.36
router
network device that is used to establish and control the flow of data between different networks, which themselves can be based on different network protocols, by selecting paths or routes based upon routing protocol mechanisms and algorithms. The routing information is kept in a routing table

3.2.37
security dimension
set of security controls designed to address a particular aspect of network security

NOTE The detailed description of security dimensions is given in ISO/IEC 18028-2.

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

3.2.39
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

NOTE The detailed description of security gateway is given in ISO/IEC 18028-3.

3.2.40 security layers
that which represents **a** hierarchy of network equipment and facility groupings protected by security dimensions

NOTE The detailed description of security layer is given in ISO/IEC 18028-2.

3.2.41 security plane
that which represents a certain type of network activity protected by security dimensions

NOTE The detailed description of security plane is given in ISO/IEC 18028-2.

3.2.42 spamming
sending of bulk unsolicited messages which on receipt cause adverse effects on the availability of information system resources

3.2.43
spoofing
impersonating a legitimate resource or user

3.2.44
switch
device which provides connectivity between networked devices by means of internal switching mechanisms

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. This ensures the network traffic is only seen by the addressed network devices and enables several connections to exist simultaneously. Switching technology can typically be implemented at layer 2 or layer 3 of the OSI reference model (ISO/IEC 7498-1).

3.2.45
tunnel
data path between networked devices which is established across an existing network infrastructure by using techniques such as protocol encapsulation, label switching, or virtual circuits

3.2.46
virtual private network
restricted-use logical computer network that is constructed from the system resources of a physical network, e.g. by using encryption and/or by tunneling links of the virtual network across the real network

4 Abbreviated terms

NOTE The following abbreviated terms are used in all parts of ISO/IEC 18028.

3G	Third Generation mobile telephone system
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
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
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
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
HIDS	Host based Intrusion Detection System
HTTP	Hypertext Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
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'
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
SSH	Secure Shell
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TelnetTerminal emulation program to work on-line on a remote computer	
TETRA	TErrestial 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
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

5 Structure

The approach taken in ISO/IEC 18028-1 is to:

— first summarize the overall process for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and

— then provide an indication of the potential control areas with respect to security associated with connections to and between communications networks. In doing this indicators are provided to where relevant content of ISO/IEC 13335 and ISO/IEC 17799 may be used, and technical design and implementation topics are introduced with references to where they are dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

Three simple criteria are described to aid persons responsible for information security to identify potential control areas. These criteria identify the:

— different types of network connections,

— different networking characteristics and related trust relationships, and

— potential types of security risk associated with network connections (and the use of services provided via those connections).

The results of combining these criteria are then utilized to indicate potential control areas. Subsequently, summary descriptions are provided of the potential control areas, with indications to sources of more detail.

The areas dealt with are:

— Network Security Architecture, including coverage of:

  - local area networking,
  - wide area networking,
  - wireless networks,
  - radio networks,
  - broadband networking,
  - security gateways (see also ISO/IEC 18028-3),
  - remote access services (see also ISO/IEC 18028-4),
  - virtual private networks (see also ISO/IEC 18028-5),
  - IP convergence (data, voice and video),
  - enabling access to services provided by networks external (to the organization),
  - web hosting architectures,

  (See also ISO/IEC 18028-2 for more detail of Network Security Architecture.)

— Secure Service Management Framework,

— Network Security Management,

— Technical Vulnerability Management,

— Identification and Authentication,

— Network Audit Logging and Monitoring,

— Intrusion Detection,

— Protection Against Malicious Code,

— Common Infrastructure Cryptographic Based Services, and

— Business Continuity Management[1]).

Implementation and operation of security controls, and monitoring and reviewing the implementation, are then dealt with.

6 Aim

The aim of this document is to provide:

— direction for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and

— an indication of the potential control areas, including those dealt with in detail in ISO/IEC 18028-2 to ISO/IEC 18028-5.

7 Overview

7.1 Background

Most government and commercial organizations' information systems are connected by networks, with the conduct of electronic business on a global basis increasing all the time. These network connections can be within the organization, between different organizations, and between the organization and the general public.

Indeed, rapid developments in publicly available network technology, in particular with the Internet and the associated World Wide Web, present great opportunities for business and for the provision of on-line public services. These opportunities range from the provision of lower cost data communications, using the Internet simply as a global means of connection, to more sophisticated ISP services. This means the use of relatively low cost local attachment points at each end of the circuit, to full scale on-line electronic trading and service delivery systems, using Web-based applications and services. In addition the new technologies, including the integration of data and voice, increase the opportunities for telecommuting style business models. This enables employees to operate away from base for much of the time, maintaining contact by using remote facilities, such as dial-in, or increasingly wireless LAN connections, to establish contact with the corporate network and gain access to business support information and services.

Thus, whilst this environment brings business benefits, it also brings new security risks to be managed. With organizations relying heavily on the use of information to conduct their business activities, the loss of confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information and services can have an adverse impact on business operations. Consequently, there is a critical requirement to protect information and to manage the security of information systems within organizations.

---

1) This includes IT Disaster Recovery Planning.

An example of a typical networking scenario, which can be observed in many organizations today, is shown in Figure 1 below.

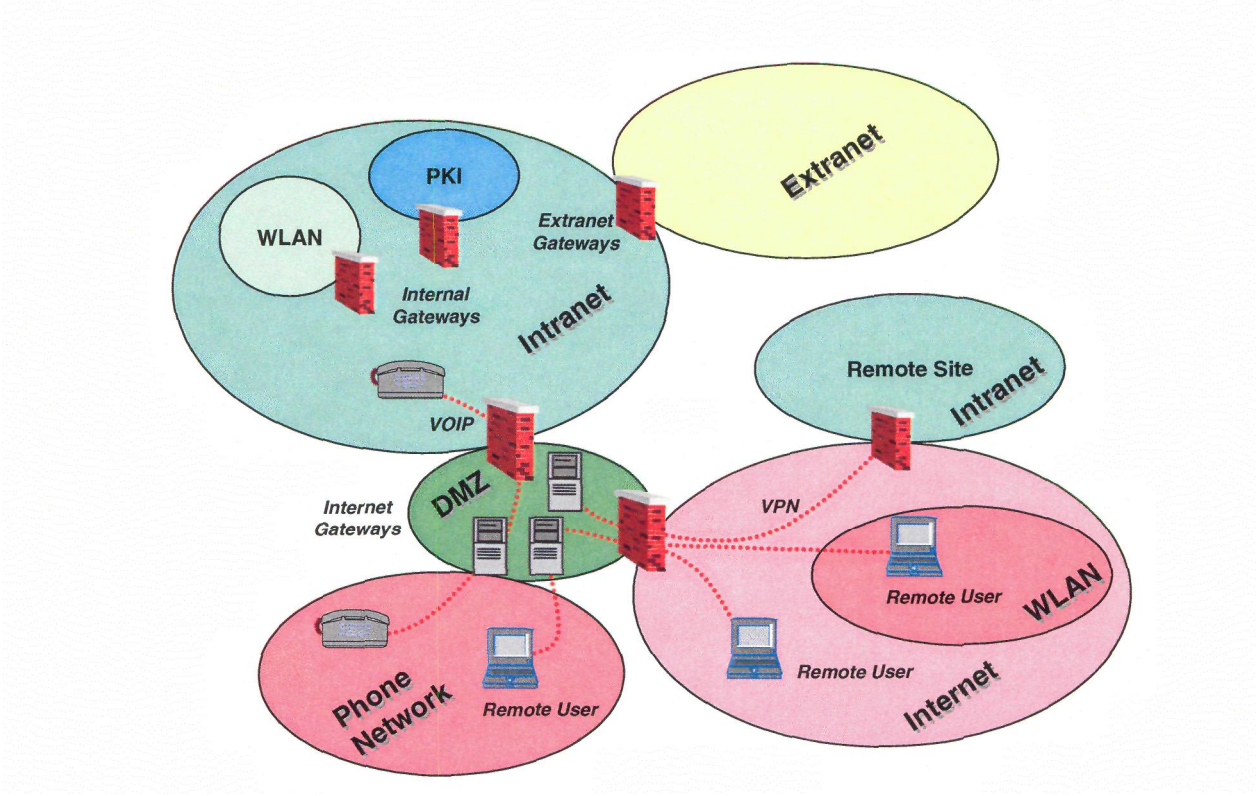

Figure 1 — Typical Networking Environment

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 may 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, may be operated in a dedicated segment of the Intranet. On the other hand, certain technologies may require some isolation because they introduce additional risks, e.g. WLAN infrastructures. For both cases, internal security gateways may 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, mainly the Internet, are further used today to provide cost optimized communications and data exchange facilities with partners and customers (including the 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 may be connected through VPN technology, and they may further use wireless connection facilities like public WLAN hotspots for accessing the Internet. Alternatively, remote users may 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.

Whilst in many respects the technologies which are used within such a typical networking scenario are providing expanded opportunities and benefits to the business, for example by reducing or optimizing costs, they also lead to quite complex environments and usually introduce new information security risks. Therefore, the risks posed by these environments should be properly assessed and the assessed risks mitigated by implementing the appropriate security controls.

In other words, the business opportunities afforded by these new 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. 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. A major strength of the Internet is that it is a very open system, originally developed in the academic research community responding to US Government project requirements, with widespread publication of results and free distribution of software and specifications. This has aided the popularity and rapid growth of the Internet. However this very popularity and openness creates a significant security vulnerability. 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 problems, ranging from unauthorized access to full-scale destructive denial of service.

In summary, successful commercial and governmental exploitation of the opportunities offered by modern networking depends upon the degree to which the risks of operating in an open environment can be managed and controlled.

Clause 7.2 summarizes the recommended process for the identification and analysis of the communications related factors that should be taken into account to establish network security requirements, and the provision of an indication of the potential control areas. Subsequent clauses then provide further detail of this process.

7.2 Identification Process

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. In addition, they should be aware of the security risks to, and related control areas for, such network connections. The business requirements and benefits are likely to influence many decisions and actions taken in the process of considering network connections, identifying potential control areas, and then eventually selecting, designing, implementing and maintaining security controls. Thus, these business requirements and benefits should be kept in mind throughout the process. In order to identify the appropriate network related security requirements and control areas, the following tasks should be completed (also see ISO/IEC 17799):

— review the general security requirements for network connections as set out in the organization's corporate information security policy [2]) (see Clause 8),

— review the network architectures and applications that relate to the network connections, to provide the necessary background to conduct subsequent tasks (see Clause 9),

— identify the type or types of network connection that should be considered (see Clause 10),

— review the characteristics of the networking proposed (aided as necessary by the information available on network and application architectures), and the associated trust relationships (see Clause 11),

---

2) This will include this policy'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), (2) the classification of the data to be stored or transported on the network.

— determine the related types of security risk, where possible with the help of risk assessment and management review results - including consideration of the value to business operations of the information to be transferred via the connections, any other information potentially accessible in an unauthorized way through these connections, and of the services provided [3]) (see Clause 12),

— identify the control areas that are appropriate, commensurate with the type(s) of network connection, the networking characteristics and associated trust relationships, and the types of security risks, determined, and in parallel document and review the technical security architecture options and agree the preferred option[4], (see Clause 13),

— implement and operate security controls (see Clause 14), and

— monitor and review implementation of the security controls on an ongoing basis [5]) (see Clause 15).

It should be noted that general advice on the identification of controls is contained in ISO/IEC 17799, and will be in ISO/IEC 13335-2 when published. ISO/IEC 18028-1 is complementary to these standards, providing an introduction on how to identify appropriate control areas with respect to security associated with connections to communications networks, and thence to ISO/IEC 18028-2 to ISO/IEC 18028-5.

Figure 2 below explains the overall process of identification and analysis of the communications related factors to be taken into account to establish network security requirements, and the provision of indications of potential control areas. Each step of the process is described in further detail in the clauses following Figure 2.

---

3) 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 classification of the data to be stored or transported on the network.

4) 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).

5) 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).

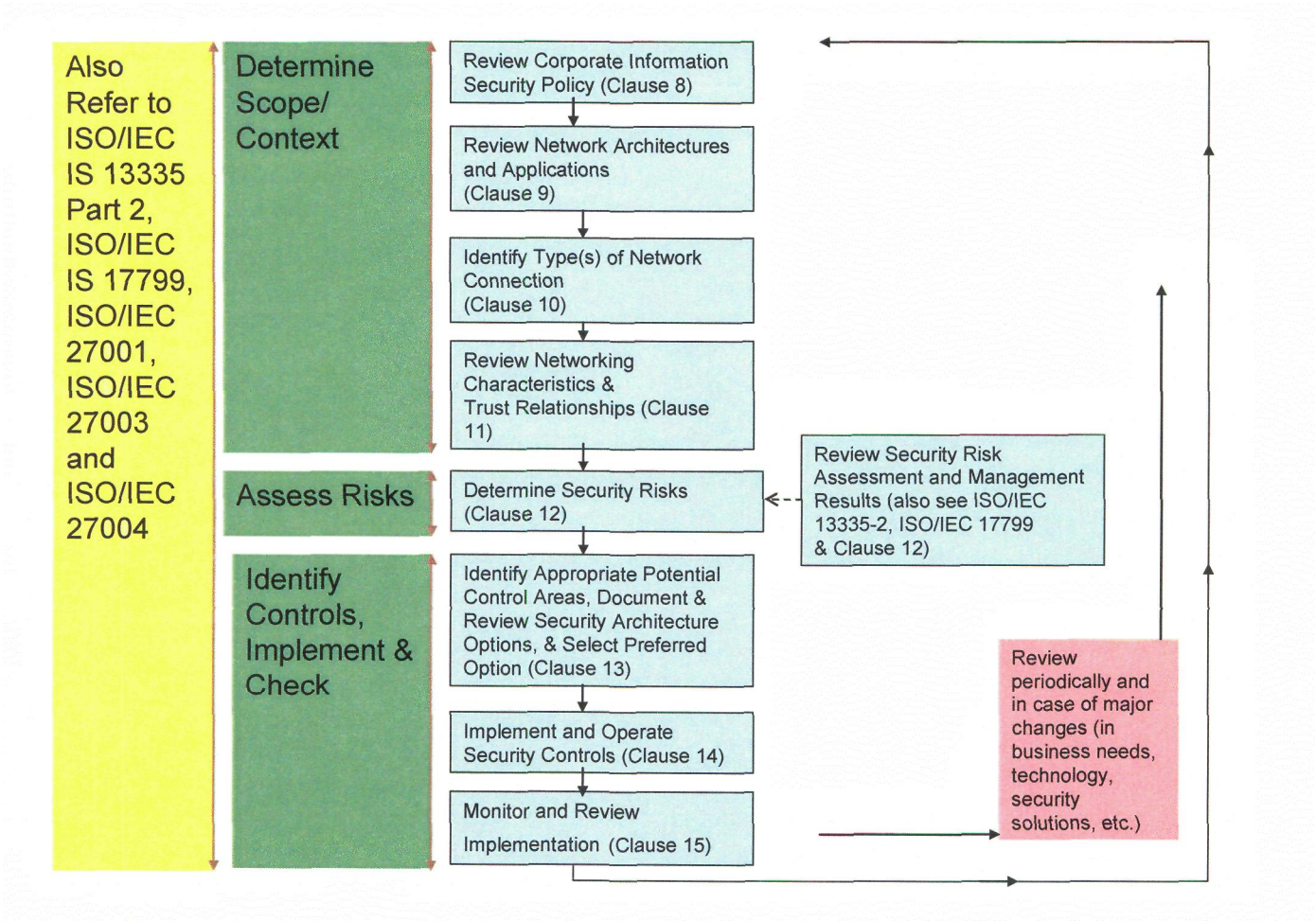

Figure 2 — Management Process in the Context of Network Security

In Figure 2 the solid black lines represent the main path of the process, and the dotted black line where the types of security risk may be determined with the aid of results from a security risk assessment and management review.

In addition to the main path of the process, in certain steps there should be a need to re-visit the results of earlier steps to ensure consistency, in particular the steps "Review Corporate Information Security Policy" and "Review Network Architectures and Applications". For example,

— after types of security risk have been determined there may be a need to review corporate information security policy because something has arisen that is in fact not covered at that policy level,

— in identifying potential control areas, the corporate information security policy should be taken into account, because it may, for example, specify that a particular control has to be implemented across the organization regardless of the risks, and

— in reviewing security architecture options, to ensure compatibility the network architectures and applications should be considered.

8 Consider Corporate Information Security Policy Requirements

An organization's corporate information security policy may include statements on the need for confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability, as well as views on types of threat, and control requirements, that relate directly to network connections.

For example, such a policy could state that:

— 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, and

— no payment instruction is valid without a digital signature.

Such statements, views and requirements, being applicable organization or community-wide, should be accounted for in the determination of the types of security risk (see Clause 12 below) and the identification of potential control areas for network connections (see Clause 13 below). If there are any such security requirements then these should be documented in the draft list of potential control areas, and as necessary reflected in security architecture options. Guidance on the positioning of a corporate information security policy document within an organization's approach to information security, and on its content and relationships with other security documentation, is provided in ISO/IEC 13335-1 and ISO/IEC 17799. Guidance will also be provided in ISO/IEC 13335-2, when published.

9 Review Network Architectures and Applications

9.1 Background

As referred to earlier in this standard, the steps to achieve confirmation of the potential controls required for a network are:

— identification of the type(s) of network connection to be used,

— identification of the networking characteristics and associated trust relationships involved,

— determination of the security risks,

— development of the list of required control areas [e]\ and the related designs.

Following these steps should always be accomplished in the context of the network architecture and applications that already exist or are planned.

Thus detail should be obtained of the relevant network architecture and applications, and this should be reviewed to provide the necessary understanding and context for the process steps that follow.

By clarifying these aspects at the earliest possible stage, the process of identifying the relevant security requirement identification criteria, identifying control areas, and reviewing the technical security architecture options and deciding which one should be adopted, should become more efficient and eventually result in a more workable security solution.

The consideration of network and application architectural aspects at an early stage should allow time for those architectures to be reviewed and possibly revised if an acceptable security solution cannot be realistically achieved within the current architecture.

---

6) Including those control areas associated with the use of cryptography for such as confidentiality, integrity and authentication.

The different areas that should be considered include:

— types of network,

— network protocols,

— network applications,

— technologies used to implement networks.

Some of the issues for review for each of these areas are discussed in Clauses 9.2 to 9.6 below. Clause 10 provides guidance on how to identify the types of network connection, and Clause 11 provides guidance on how to determine the networking characteristics and related trust relationships. Clause 12 provides guidance on identifying the security risks. (General guidance on network and application architectures can be found in ISO/IEC7498.)

9.2 Types of Network

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

— Local Area Networks (LANs), which are used to interconnect systems locally, and

— Wide Area Networks (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.)

9.3 Network Protocols

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,

— routing protocols are used to define the route through the different nodes on which information travels within WANs. Information is physically accessible for all systems along the route, and routing may be changed, either accidentally or intentionally, and

— 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 on network, using QoS mechanisms to ensure real time performance.

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

Many protocols may 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.

9.4 Networked Applications

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 (such as encryption and digital signatures for messages) may 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.

9.5 Technologies Used to Implement Networks

Networks may be delivered via a variety of means. A common structuring of these means is based on geographical areas which are covered by a network.

9.5.1 Local Area Networks

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. Small LANs are most commonly implemented by using shared media technologies. The Ethernet protocol is the standard technology used in this context, and has been extended for providing higher bandwidth as well as for supporting wireless environments. Since shared media technologies, and also Ethernet in particular, have limitations in greater size networks, typical WAN technologies such as routable protocols are also often used in LAN environments. A LAN can be wired, or wireless based.

9.5.1.1 Wired **LAN**

A wired LAN usually consists of nodes connected in a network via a network switch or hub using networking cables, which can provide high-speed data networking capabilities. Well-known wired LAN technologies include Ethernet (IEEE 802.3) and Token Ring (IEEE 802.5).

FOJIOBHIIH (J)OH,H

9.5.1.2 Wireless LAN

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.

9.5.2 Wide Area Networks

WANs are used to connect distant locations, and their LANs, together. A WAN can be constructed using cables, circuits from a service provider, or more likely 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 networking infrastructure is used for interconnecting LANs, e.g. leased lines, satellite communications or fiber optics. A WAN can be wired, or wireless based.

9.5.2.1 Wired WAN

A wired WAN usually consists of routing devices (e.g. routers) connected to a public or private network via telecommunication wires. Well-known wired WAN technologies include ATM, Frame Relay and X.25.

9.5.2.2 Wireless WAN

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. Well-known wireless WAN technologies include TDMA, CDMA, GSM, and IEEE 802.16.

9.6 Other Considerations

When reviewing the network architecture and applications, consideration should also be given to existing network connections within, to or from the organization, and to the network to which a connection is proposed. The organization's existing connections may 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.

10 Identify Types of Network Connection

There are many generic types of network connection that an organization or 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 or EDI, and could involve use of Internet, Intranet or Extranet facilities, each with differing security considerations. Each of the types of connection may have different vulnerabilities and thus associated security risks, and consequently eventually require a different set of controls. (Also see ISO/I EC 17799).

Table 1 below shows one way of categorizing the generic types of network connection that may be required to conduct business, with a descriptive example shown for each type.

Taking due account of relevant network architectures and applications (see Clause 9 above), one or more of the types shown in Table 1 should be selected as appropriate to the network connection(s) being considered.

It should be noted that the generic types of network connection described in this document are organized and categorized from a business perspective rather than a technical one. This means that two different types of network connection may sometimes be implemented by similar technical means, and that in some cases the controls may be similar, but there are other cases where they will be different.

Table 1 — Types of Network Connection

Reference Letter	Type of Network Connection	Descriptive Example
A	**Connection within a single controlled location of an organization.**	Interconnection between different parts of the same organization within the same controlled location, i.e. a single controlled building or site.
B	**Connection between different geographically disparate parts of the same organization.**	Interconnection between regional offices (and/or regional offices with a headquarters site) within a single organization across a wide area network. In this type of network connection, 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 (i.e. each user's access would only be in accordance with privileges granted). One type of access from another part of the organization could be for remote maintenance purposes. There might be more access privileges assigned to this type of user and connection.
C	**Connections between an organization site and personnel working in locations away from the organization.**	Use of mobile data terminals by employees (e.g. a salesperson verifying stock availability from a customer site) 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. In this type of network connection, the user is authorized as a system user on his local system.
D	**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.**	Interconnection between two or more organizations where there is a business need to facilitate inter-organizational electronic transactions (e.g. electronic funds transfer in the banking industry). This type of network connection is similar to 'B' above, except that the sites being interconnected belong to two or more organizations, and the connection is not intended to provide access to the full range of applications used by each of the participating organizations.
E	**Connections with other organizations.**	There could be access to remote databases held by other organizations (e.g. through service providers). 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. However, although all users are pre-authorized, there may be no screening of potential users other than in relation to their ability to pay for the services being offered. There could also be access to applications on the organization's systems that store or process the organizational information that may be provided to users from external organizations. In this circumstance, the external users would be known and authorized. One type of access from another organization could be for remote maintenance purposes. There might be more access privileges assigned to this type of user and connection.
F	**Connections with the general public domain.**	Access could be initiated by the organization's users to public access databases, Web sites, and/or electronic mail facilities (e.g. via the Internet), where the access is initiated for purposes such as the retrieval of information or the sending of information from/to persons and/or sites which have not been specifically pre-authorized by the organization. In this type of connection, the organization's users may be utilizing this facility for organizational (possibly even private) purposes; however, the organization may have little, if any, control over the information being transmitted. Access could be initiated by external users to the organization's facilities (e.g. via the Internet). In this type of network connection, access by the individual external users has not been specifically pre-authorized by the organization.
G	**Connections to the Public Telephone Network from an IP environment.**	Access could be initiated to the PSTN from a phone in an IP network. Such connections are uncontrolled as calls could be received from any location in the world.

11 Review Networking Characteristics and Related Trust Relationships

11.1 Network Characteristics

The characteristics of the existing or proposed network should be reviewed. It is particularly important to identify whether the network is a:

— public network - a network accessible by anyone, or

— 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

— network encompassing both data and voice, and possibly video.

Other information, such as:

— whether the network is a packet or switched network,

— whether it supports a QoS, i.e. in an MPLS network,

is also relevant.

(QoS concerns consistent performance. Network services should be delivered to provide the minimum performance level to be useable. For example, voice service 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.)

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

11.2 Trust Relationships

Once the characteristics of the existing or proposed networking have been identified, and at minimum it has been established if the network is public or private (see Clause 11.1 above), then the related trust relationships should be identified.

Firstly, the applicable trust environment(s) associated with the network connection(s) should be identified using the simple list shown below

— Low, such as a network with an unknown community of users,

— Medium, such as a network with a known community of users and within a closed business community (of more than one organization),

■— High, such as a network with a known community of users solely within the organization.

Secondly, the relevant trust environment(s) (from Low, Medium and High) should be related to the applicable network characteristic (public or private) and the type(s) of network connection involved (from 'A' to 'G'), to establish the trust relationships. This can be accomplished using a matrix similar to that shown in Table 2 below.

Table 2 — Identification of Trust Relationships

TYPES OF NETWORK CONNECTION (See Clause 10)		TRUST ENVIRONMENTS		
		LOW	MEDIUM	HIGH
NETWORK CHARACTERISTICS	PUBLIC	F G	D E	B C
	PRIVATE	E	D E	A B C

From Table 2 the reference category for each relevant trust relationship should be determined. All of the possible categories are described in Table 3 below.

Table 3

Trust Relationship Category	Description
LOW/PUBLIC	Low trust, and use of a public network.
MEDIUM/PUBLIC	Medium trust, and use of a public network.
HIGH/PUBLIC	High trust, and use of a public network.
LOW/PRIVATE	Low trust, and use of a private network.
MEDIUM/PRIVATE	Medium trust, and use of a private network.
HIGH/PRIVATE	High trust, and use of a private network.

— Trust Relationship References

These references should be used when working through Clause 12 to confirm the types of security risk and identify potential control areas.

This task can be aided as necessary by the information available on network architectures and applications (as gained by using Clause 9).

12 Identify the Information Security Risks

As reflected earlier, the majority of organizations today are dependent on the use of information systems and networks to support their business operations. Further, in many cases there is a definite business requirement for the use of network connections 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 may 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 may impose duties on those collecting, processing and disseminating personal information through networks and may even restrict the ability to transfer that data to certain other countries, yielding additional important security concerns. Less obvious examples of data that may be subject to such legislation are some hardware and IP addresses.)

The types of risk reflected in this clause 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. Thus the types of security risk that an organization might face 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).

Not all of the types of security risk will apply to every location, or to every organization. However, the relevant types of security risk should be identified so that potential control areas can be identified (and eventually controls selected, designed, implemented and maintained).

A conceptual model of network security showing where the types of security risk may occur is shown in Figure 3.

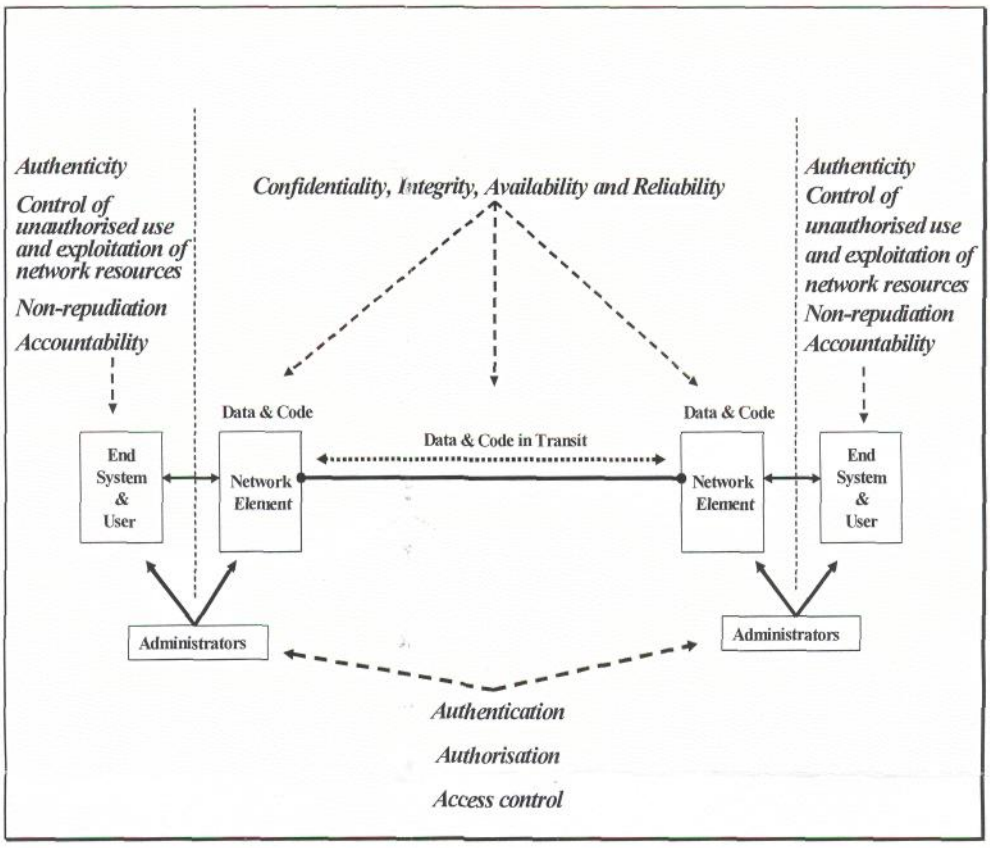

Figure 3 — A Conceptual Model of Network Security Risk Areas

Information should be gathered on the implications to business operations related to the types of security risk referred to above, with due consideration of the sensitivity or value of information involved (expressed as potential adverse business impacts) and related potential threats and vulnerabilities. Related to this, if there is likely to be more than a minor adverse impact on the business operations of the organization, then reference should be made to the matrix in Table 5 below.

It is emphasized that in completing this task, use should be made of the results from security risk assessment and management review(s) [7]) conducted with regard to the network connection(s). These results will enable a focus, to whatever level of detail the review(s) have been conducted, on the potential adverse business impacts associated with the types of security risk listed above, as well as the threat types, vulnerabilities and hence risks of concern.

When considering network vulnerabilities during a security risk assessment and management review, it may be necessary to consider a number of network facets separately. Table 4 below lists the types of vulnerability that could be exploited at each network facet.

7) Guidance on security risk assessment and management approaches is provided in ISO/IEC 17799, and will be in ISO/IEC 13335-2 when published.

Table 4 — Types of Potential Vulnerability

Network Facet	Types of Potential Network Security Vulnerability				
	Interruption	**Interception**	**Modification**	**Intrusion**	**Deception**
Network Users	Users may suffer loss or interruption of service.	User transactions and/or network activity may be monitored.	User details and user data may be modified or destroyed.	Users may be impersonated to gain unauthorized access to facilities.	Users may be impersonated to conduct fraudulent transactions.
Network End-Systems	End-systems may become temporarily or permanently unavailable.	Unauthorized persons may read data or code on end-systems.	Data or code may be modified or destroyed.	End systems may be impersonated to gain unauthorized access to facilities. Unauthorized persons might gain access to system accounts and use them to launch further attacks.	End systems may be impersonated to conduct fraudulent transactions, or to launch further attacks.
Networked Applications	Applications may become temporarily or permanently unavailable.	Data or code may be intercepted in transit, or read on servers, by unauthorized persons.	Data or code may be modified or destroyed.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.
Network Services	Services may become temporarily or permanently unavailable.	Data or code may be intercepted in transit, or read on servers, by unauthorized persons	Data or code may be modified or destroyed.	Unauthorized persons might gain access to system accounts and use them to launch further attacks.	Network servers and devices may be impersonated to gain unauthorized access, to intercept network traffic, or to disrupt network services.
Network Infrastructure	Facilities may become temporarily or permanently unavailable			Unauthorized persons may infiltrate facilities.	

Using the security risk assessment and management review results as the principal guide, the relevant trust relationship references should be determined from using Clause 11 above and identified along the top of the matrix in Table 5 below, with the impacts of concern on the left hand side of the matrix. The references at the pertinent intersections should then be noted - these are the references to the potential control areas that are introduced in Clause 13 below.

Table 5 — Types of Security Risk and References to Potential Control Areas

Types of Risk	Trust Relationship References					
	LOW/ PUBLIC	MEDIUM/ PUBLIC	HIGH/ PUBLIC	LOW/ PRIVATE	MEDIUM/ PRIVATE	HIGH/ PRIVATE
Loss of Confidentiality	13.2.1 [8)] 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.2 13.10.5	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.2 13.10.5
Loss of Integrity	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.3 13.10.5	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.3 13.10.5

8) Regarding all references to clause 13.2.1 in this table - this clause will apply in a manner appropriate to the networking scenario concerned.

Types of Risk	Trust Relationship References					
	LOW/ PUBLIC	MEDIUM/ PUBLIC	HIGH/ PUBLIC	LOW/ PRIVATE	MEDIUM/ PRIVATE	HIGH/ PRIVATE
Loss of Availability	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.7 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.11	13.2.1 13.2.8 13.2.9 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.11
Loss of Non-Repudiation	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.7 13.2.8 13.3.2 13.3.3 13.3.4 13.3.5 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.7 13.8 13.9 13.10.4 13.10.5 13.11	13.2.1 13.2.8 13.3.2 13.3.3 13.3.4 13.3.6 13.3.7 13.4 13.5 13.6.2 13.6.3 13.6.4 13.6.5 13.7 13.8 13.9 13.10.4 13.10.5 13.11

It should be noted that the table appears to indicate that the more a user is trusted, the more controls are necessary. There are two reasons for this.

Firstly, there are a number of controls described in ISO/IEC 17799 (and which will also be described in ISO/IEC 13335-2, when published), and thus not repeated in this document, that would be selected to protect the host facilities, including for identification and authentication, and logical access control. In low trust situations the strength of identification and authentication, and logical access control, controls should be higher than in high trust situations. If this cannot be assured, then relevant additional controls should be implemented. The configuration of the permissions (privileges) in the lower trust situations should help ensure that access is only provided to resources that are consistent with the trust model and requirements of the intended access.

Secondly, trusted users are usually given access to more important/critical information and/or functionality. This can mean a requirement for additional controls, as a reflection of the value of the resources accessed and not on the trust in the users.

13 Identify Appropriate Potential Control Areas

13.1 Background

On the basis of the results of the risk assessment and management review, and aided by the references identified from using Clause 12, the potential control areas should then be identified and selected from Clause 13 (and of course ISO/IEC 17799). ISO/IEC 13335-2, when published, will also provide relevant information. Clause 13.2 addresses the various network security architecture aspects and related potential control areas, followed by Clauses 13.3 to 13.11 which introduce other related potential control areas. A particular security solution may in fact encompass a number of the potential control areas introduced in Clauses 13.2 to 13.11.

It is emphasized that there are a number of controls that are relevant to information systems whether or not they have any network connections, which should be selected through the use of ISO/IEC 17799. ISO/IEC 13335-2, when published, will also provide relevant information.

The list of identified potential controls should be thoroughly reviewed in the context of the relevant network architectures and applications. The list should then be adjusted as necessary and subsequently be used as the basis for implementing the required security controls (see Clause 14 below) and then monitoring and reviewing the implementation (see Clause 15 below).

13.2 Network Security Architecture

13.2.1 **Preface**

The documentation of the possible security architecture 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 needs 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 8 above), the relevant network architecture and network applications (see Clause 9 above), and the list of potential control areas identified by using Clauses 12 and 13. In accomplishing this, account should be taken of any existing security architectures. 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 and application architectures (to ensure compatibility with the preferred security architecture), and/or the list of potential controls (e.g. because it is agreed that the security architecture can only be technically implemented in a particular way, necessitating an alternative to an identified control).

It should be noted that ISO/IEC 18028-2 describes a "Reference"[9]) security architecture which is very useful as a base point from which to:

— describe a consistent framework to support the planning, design and implementation of network security,

— define the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security.

Based on the "Reference" security architecture, descriptions of the actual different real-world technical security architectures that are needed to address the requirements of today and the near future are introduced in this standard and further developed in ISO/IEC 18028-3 to ISO/IEC 18028-5.

The principles described in the "Reference" security architecture are applicable to any type of modern networking, whether data, voice and converged networks, whether wireless or radio, and can be applied

9) In the context of Part 2 "Reference" is taken to mean one example of how to represent technical security architecture at a very high level. There may be other examples.

independent of the network's technology or location in the protocol stack. It addresses security concerns related to the management, control, and use of network infrastructure, services, and applications, and provides a comprehensive, top down, end-to-end perspective of network security. The "Reference" security architecture has three architectural components:

— Security Dimensions (may also be known as 'Security Control Groups'),

— Security Layers (may also be known as 'Network Security Elements'),

— Security Planes Jmay also be known as 'Security Domains').

Security Dimensions are sets of security controls designed to address a particular aspect of network security. There are eight such sets identified in the "Reference" security architecture, and which extend to applications and end user information, for example:

— Non-Repudiation,

— Data Confidentiality,

— Data Integrity,

— Availability.

In order to provide an end-to-end security solution, the Security Dimensions need to be applied to a hierarchy of network equipment and facility groupings, which are referred to as Security Layers:

— Infrastructure Security Layer,

— Services Security Layer,

— Applications Security Layer.

The Security Layers build on one another to provide network based solutions, i.e. the Infrastructure Layer enables the Services Security Layer and the Services Security Layer enables the Applications Security Layer, and identify where security should be addressed in products and solutions by providing a sequential perspective of network security.

The Infrastructure Security Layer consists of the network transmission facilities as well as individual network parts protected by the mechanisms that are implemented for the Security Dimensions. Examples of components that belong to the Infrastructure Security Layer are individual routers, switches and servers as well as the communication links between individual routers, switches and servers.

The Services Security Layer addresses the security of services that Service Providers provide to their customers. These services range from basic transport and connectivity to service enablers like those that are necessary for providing Internet access (e.g. authentication, authorization, and accountability services, dynamic host configuration services, domain name services, etc.) to value-added services such as free phone service, QoS, VPN, etc.

The Applications Security Layer focuses on the security of the network-based applications accessed by Service Provider customers. These applications are enabled by network services and include basic file transport (e.g. FTP) and web browsing applications, fundamental applications such as directory assistance, network-based voice messaging, and e-mail, as well as high-end applications such as customer relationship management, electronic/mobile commerce, network-based training, video collaboration, etc.

The Security Planes are certain types of network activity protected by the mechanisms that are implemented for the Security Dimensions. The "Reference" security architecture defines three Security Planes to represent the types of protected activities that take place on a network. The Security Planes are the:

— Management Plane,

— Control Plane,

— End-User Plane.

These Security Planes address specific security needs associated with network management activities, network control and signaling activities, and end-user activities correspondingly. Networks should be designed in such a way that events in one Security Plane are kept as much as possible and as appropriate isolated from the other Security Planes.

The following clauses include an introduction to the actual different real-world technical security architecture aspects of the various areas of networking.

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

13.2.2 Local Area Networking

13.2.2.1 Background

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 (also see Clause 13.2.4 below), physical protection alone is unlikely to guarantee any level of security. Furthermore, the shared media technologies most commonly used within LANs do allow access to all network traffic from any system using the shared media.

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 the corporate network, both ones exposed to the Internet and internal servers that have no direct connection to the Internet, represent a potential major security risk. While most IT departments would claim that they are diligent about applying patches as soon as they are available, this risk has to be taken very seriously as even large organizations have failed to patch all servers in a timely manner, leading to disruption of internal network traffic by worms.

13.2.2.2 Security Risks

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

— unauthorized access and changes to desktop PCs, servers, and other LAN connected devices,

— un patched servers,

— 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 (laptop),

— unauthorized access to hubs and patch cabinets,

— default passwords on the management ports of hubs and switches,

— poor physical security.

13.2.2.3 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 padlocks on devices to prevent parts, such as memory, from being stolen,
  - use of proximity devices to prevent unauthorized removal from site,
  - ensure that LAN hubs 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 IP addresses,
  - strong password policy,
  - require logon at each workstation, at least with at least a user id/ password pair,
  - install anti-virus software, and regularly update automatically,
  - implement secure registry settings,
  - disable floppy disc drive, CD-ROM drive, and USB ports,
  - mirror server drives (or implement RAID) for redundancy,
  - remove unnecessary software,

— operational:
  - document software and security settings for future use in configuring new 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 workstations,
  - file all workstation component documentation (papers/manuals/disks) for use by service technicians,
  - ensure a back-up regime,
  - ensure that all hubs and switches have default passwords changed,
  - set appropriate network management protocol passwords/community strings,
  - 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.

13.2.3 Wide Area Networking

13.2.3.1 Background

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. However, 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 it's 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.

13.2.3.2 Security Risks

Whilst a wired WAN shares the same primary security risks with a wired LAN (see Clause 13.2.2 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 13.2.2 above), 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 risks associated with WANs include:

— intrusion, where information is disclosed or the integrity of data cannot then be guaranteed,

— DoS attacks, where resources become unavailable to authorized users,

— third party connection and dial-up internet accounts for personal use at home which can easily bypass any controls implemented at the network and server level, exposing the corporate network to e-mail borne worms, Trojans, and viruses,

— extended latency, which will affect voice over IP services,

— jitter on the network, which will affect voice quality (caused primarily through the use of copper cables to deliver service),

— device failure,

— cable failure,

— un patched devices,

— loss of power at a transit site, which affect many others,

— service provider's network management facilities.

13.2.3.3 Controls

The key security controls required to secure a WAN include:

— replacement of inherently insecure protocols such as Telnet and FTP with secure protocols such as SSH and SCP,

— encryption of management links,

— implementation of secure authentication to access the WAN devices, with appropriate alarming of devices, using SNMP reporting,

— 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 facility,
— encrypted overlays for sensitive data,
— obtaining service guarantees from the service provider, such as for 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 MPLS structure and addresses are hidden,
— assigning IP addresses that cannot be routed over the Internet,
— the use of Network address translation that hides internal IP addresses, but allows devices with non-routable addresses to make requests from the Internet,
— the use of anti virus software to prevent malicious code, such as Trojans, viruses, 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,
— ensuring that the network management locations are physically secure,
— ensuring the devices are backed up,
— performing reliability checks on network management staff.

13.2.4 Wireless Networks

13.2.4.1 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 13.2.5 below).

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.

13.2.4.2 Security Risks

The key security risk areas associated with the use of WLANs include:

— eavesdropping,
— unauthorized access,
— interference and jamming,
— mis-configuration,
— secure access mode is off by default,
— flawed WEP or TKIP,

— flawed SNMP used to manage WLANs,

— not always possible to see who is using a WLAN.

13.2.4.3 Controls

The controls needed for WLANs include:

— firewalling the WLAN from the corporate infrastructure,

— 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-virus software on the client device,

— control of transmission levels to eliminate a spread outside an organization's physical domain,

— SNMP configured for read only access,

— Out of Band encrypted management, for example using SSH,

— maintaining physical security to wireless access points,

— hardening of any server components,

— system testing,

— giving consideration to deploying an IDS between the corporate network and the wireless network.

13.2.5 Radio Networks

13.2.5.1 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 13.2.4.

Examples of radio networks include:

— TETRA

— GSM

— 3G (including UMTS),

— GPRS,

— CDPD,

— CDMA.

13.2.5.2 Security Risks

There are a number of general security threat scenarios which can result in risks applicable to radio networks, including:

— eavesdropping,

— session hijacking,

— impersonation,

— application level threats, e.g. fraud,

— denial of service.

Examples of the risks in the context of some types of radio network are shown in the paragraphs below.

The security risks associated with GSM include the facts that:

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

— generally GSM encryption is turned off,

— SIM cloning is a reality.

The security risks associated with 3G include 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.

13.2.5.3 Security Controls

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

— secure authentication,

— encryption with effective algorithms,

— protected base stations,

— firewalls,

— malicious code (virus, trojans, etc.) protection,

— anti-spam.

13.2.6 Broadband Networking

13.2.6.1 Background

Broadband networking is a group of technologies which allow individual subscribers high speed access to an Internet point-of-presence. Currently, there are four main technologies:

— 3G,

— Cable,

— Satellite,

— DSL.

For DSL, 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 is that they are a high-speed, always on technology available more cheaply that conventional communications. 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.

13.2.6.2 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, and lead directly to the following risks:

— 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,

— mis-configuration of client systems,

— introduction of software vulnerabilities,

— network congestion,

— DoS.

13.2.6.3 Security Controls

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

— Small Office/Home Office (SOHO) Firewalls,

— anti-malicious code (including viruses) software,

— IDS, including IPS,

— VPNs,

— Software Updates/Patching.

13.2.7 Security Gateways

13.2.7.1 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 13.2.7.3 below).

13.2.7.2 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. If these threats are not addressed then there is a risk the connections to the outside world could become unavailable, data could become corrupted, or valuable company assets could be subject to unauthorized disclosure. Data placed on websites or otherwise transmitted without proper authority may also incur legal penalties - e.g. insider trading.

13.2.7.3 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 should 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 18044).

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 18028-3 (as well as in ISO/IEC 17799), and will be provided in ISO/IEC 13335-2 when published).

It should be noted that whilst the network security aspects of personal firewalls, a special type of firewall, are not discussed in Part 3, 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 may 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 may 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.

13.2.8 Remote Access Services

13.2.8.1 Background

The aim of RAS is to allow data to be exchanged between a remote site and the central service. There are a variety of solutions for this, including:

— communications via the Internet,

— dial-up IP service.

Communications via the Internet increasingly uses ISP-provided ADSL links to provide high bandwidth from the central site and a lower bandwidth from the remote to the central site. Except for the lowest sensitivity of data, some form of VPN (see Clause 13.2.9 below) should be used to provide security for the exchanged data streams.

Dial-up IP services allow a remote site (usually a single user) to dial up a modem bank at a central location. After authentication, the connection is opened between the remote site and central service. Unless the application implements a security protocol, this mode of communications would normally be in the clear. RAS access may be implemented using ISDN or analogue lines. In either case, the user dials into a central point where some level of authentication occurs. RAS access only offers transfer of clear data.

13.2.8.2 Security Risks

There are a number of security risks that may be associated with RAS, including:

— unauthorized access to an organization's systems, services and information (including via eavesdropping), leading to the disclosure of, unauthorized changes to, or destruction of, information and/or service,

— the introduction of malicious code to an organization's systems, services and information, with resultant modification, unavailability and destruction,

— a DoS attack against an organization's services.

13.2.8.3 Security Controls

Remote access requires that the central services secure themselves against unauthorized access. Likewise, it is expected that the remote systems themselves have protection against a number of security threats. The controls that may be required include:

— firewalls (including personal firewalls),

— router ACLs,

— encryption of Internet access links,

— Calling Line Identifier,

— strong authentication,

— anti-virus software,

— audit management.

Further detail on security for remote access services is provided in ISO/IEC 18028-4.

13.2.9 Virtual Private Networks

13.2.9.1 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 may 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 securely over an insecure medium (for example, 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 and secure communications between sites can be established using VPNs.

13.2.9.2 Security Risks

The key security risk with communications over an insecure network is that sensitive information may be accessible to unauthorized parties, leading to unauthorized disclosure and/or modification. In addition to the risks typically associated with local and wide area networking (see Clauses 13.2.2.2 and 13.2.3.2 respectively), the typical risks associated with VPNs include:

— 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.

13.2.9.3 Security Controls

In VPNs, cryptographic techniques are commonly used in networking 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,

— authentication,

— intrusion detection,

— security gateways (including firewalls),

— 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 18028-5.

13.2.10 IP Convergence (data, voice, video)

13.2.10.1 Background

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

13.2.10.2 Security Risks

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

— 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 may be affected by viruses which may manage to enter the network through insecure VoIP systems that may degrade or even create a loss of service, and could spread to servers in the network, leading to damaged data storage,

— softphones on client PCs are a substantial risk as these could be an entry point for 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 may use up to eleven different ports,

— fraud is a key issue with telephony, and VoIP only adds to the risks if security is not addressed. 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 may 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 may not be operational in the case of power failure,

— there is a greater risk of failure of both voice and data services due to the use of common components, e.g. a LAN.

13.2.10.3 Security Controls

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

— 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 minimised,

— all VoIP servers should be configured with malicious software protection,

— PC supporting softphones should be fitted with personal firewalls and the virus checking software should be frequently updated,

— VoIP servers and VoIP management systems should be protected behind firewalls to safeguard them from attack,

— 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

— voice and data services should be segregated where possible,

— 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 the Ethernet hubs 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.

13.2.11 Enabling Access to Services Provided by Networks that are External (to the Organization)

13.2.11.1 Background

The opening up of e-mail and Internet services to an organization to meet legitimate business requirements brings with it a variety of threats which can be used to exploit vulnerable systems, and unless these services are well designed and operated they present a considerable risk to an organization. For instance, despite the barriers spammers face in reaching people at work, spam poses a big problem for enterprises and their staff. As spammers attempt to harvest worker names, most enterprises will need to deploy anti-spam technologies and educate users on protecting their e-mail addresses. In addition, users will need to be protected from accessing the Internet and bringing back malware, such as Trojans, into the organization, which could cause costly damage to information systems, and an organization's reputation. The key point to be kept in mind at all times is that the Internet is untrusted.

13.2.11.2 Security Risks

The key risk areas in enabling access to services provided by networks that are external to the organization, and where vulnerabilities in Internet and e-mail services can be exploited, include:

— the potential importation of damaging malware, such as Trojans,

— the receipt of overwhelming spam,

— loss of the organization's information,

— damage to the integrity, or loss, of information,

— DoS attacks,

— unauthorized use of Internet and e-mail services, including non-compliance with organization policy (e.g. using services for own benefits) and non-compliance with legislation and regulation (e.g. sending threatening emails).

13.2.11.3 Security Controls

The technical security controls to manage the risks from identified threats for Internet/e-mail solutions include:

— use of firewalls with assurance levels appropriate to the assessed risks, and firewall rulesets that cover:
  - default 'deny all' policy,
  - outgoing Web only (for example, http/https),
  - e-mail both ways,

— use of ACLs and NAT on routers to limit and hide the IP addressing structure,

— enablement of anti-spoofing to prevent external attacks. Anti-spoofing controls take the form of not accepting the message from outside (for example, from the Internet) if it claims to have originated from inside the organization, and vice versa,

— enablement of web and e-mail proxies to act as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. Security is enforced by comparing the requested URL against 'black' and 'white' lists (for Internet access), scanning

the data for known patterns, translating between internal and external addresses, creating an audit log of requests and requesters, and having anti-virus facilities based at the proxies.

— anti-virus controls on web and e-mail proxies. Typical controls include facilities to quarantine suspicious files (for example, by content type), and screening of requested URLs or e-mail addresses against a 'black list. (It should be noted that 'black' lists cannot be regarded as foolproof, particularly where such list are obtained from others. There could be a danger of false positives.). Further information on anti-virus controls is provided in Clause 13.9 below,

— anti-relay on e-mail servers and reverse DNS look-ups. Anti-relay controls detect if an incoming e-mail is from the correct sending organization; if not, the e-mail is logged (or quarantined) and the e-mail server takes no further action,

— enablement of alerts and SNMP traps. 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,

— network audit logging and monitoring (see Clause 13.7 below),

— institute OOB management, which relates 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,

— ensure that vulnerabilities in the client software used to access the Internet Services (e.g. the web browser) are proper threaded with appropriate vulnerability and patch management processes.

13.2.12 Web Hosting Architecture

13.2.12.1 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 in the architecture. 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 risk of being defaced.

13.2.12.2 Security Risks

The key risk areas include those shown below:

— 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,

— 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).

13.2.12.3 Security Controls

The technical security controls to manage the risks from identified threats for web sites, 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 13.2.7 above and ISO/IEC 18028-3.),

— 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,

— anti-virus controls on uploads to prevent the import of malware. (Further information on controls to detect and prevent malicious code is provided in Clause 13.9 below.),

— 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,

— 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 18028-4 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. (Further information on network audit logging and monitoring is provided in Clause 13.7 below.),

— 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 17799, Clause 10.6.),

— 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. (For more information on business continuity management reference should be made to Clause 13.11 below.)

13.3 Secure Service Management Framework

13.3.1 Management Activities

A key security requirement for any networking is that it is supported by secure service 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's or a community's information systems. With regard to network connections, management activities should include:

— definition of all responsibilities related to the security of networking, and designation of a security manager with overall responsibility,

— documented networking security policy, and accompanying documented technical security architecture,

— documented SecOPs,

— the conduct of security compliance checking, including security testing, to ensure security is maintained at the required level,

— documented security conditions for connection to be adhered to before connection is permitted by outside organizations or people,

— documented security conditions for users of network services,

— a security incident management scheme,

— documented and tested business continuity/disaster recovery plans.

It should be noted that this clause builds upon aspects described in ISO/IEC 17799, and which will be described in ISO/IEC 13335-2 when published. Only those of the above topics that are especially important with regard to the use of networking are further described in this document. Thus for further information, for example on the content of networking security policy and security operating procedures, and on topics not mentioned further here, the reader should thus consult ISO/IEC 17799. ISO/IEC 13335-2, when published, will also provide further information.

13.3.2 Networking Security Policy

It is the responsibility of management to visibly accept and support the organization's networking security policy (as referred to in ISO/IEC 17799). 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 may 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 networking security policy should usually include a summary of the results from the security risk assessment and management review (s) (which provide the justification for spend on controls), including detail of all security controls selected commensurate with the assessed risks (see Clause 12 above).

13.3.3 Security Operating Procedures

In support of the networking security policy, SecOPs documents should be developed and maintained, covering each network connection as appropriate. They should contain details of the day-to-day operating procedures associated with security, and who is responsible for their use and management.

13.3.4 Security Compliance Checking

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

— networking 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 connection, 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. Normally 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.

13.3.5 Security Conditions for Connection

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 may include those related to privacy/data protection, where a connection may 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.

13.3.6 Documented Security Conditions for Users of Network Services

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

13.3.7 Incident Management

Information security incidents are more likely to occur, and more serious adverse business impacts to result, where there are network connections (as opposed to where there are none). Further, with network connections to other organizations in particular there could well be significant legal implications connected with 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 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 18044.

13.4 Network Security Management

13.4.1 Preface

The management of any network should be undertaken in a secure manner, and indeed provide support for the overall management of network security. This should 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 controls, the majority of which can be identified through using ISO/IEC 17799, and ISO/IEC 13335-2 when published. In addition, remote diagnostic ports, whether virtual or physical, should be protected from unauthorized access.

13.4.2 Networking Aspects

The various aspects of networking can be categorized as follows:

Network Users - personnel who are users and /or administrators of networks. The spectrum of users ranges from individuals accessing remote resources via the Internet, dial-up or wireless connections, to individuals using workstations or personal computers that are attached to a local network. Users connected to local networks may also be able to connect to remote resources via inter-network connections that may exist between their local network and other networks. Such underlying connections may be transparent to the user,

End-Systems - computers, workstations and mobile devices (for example, smartphones and PDAs) that are connected to networks. This includes devices used to access networked facilities (e.g. client systems) and devices used to provide services (e.g. servers, host computer systems). This category encompasses the hardware, operating system software, and any local applications software, including software used to access the network.

Networked Applications - applications software, running on networked servers or host systems, and accessed via computer network connections, to provide, for example:

— financial transaction services,

— enterprise software services (e.g. CRM, EIS, MRP, etc.),

— web-based services,

— on-line database services,

— on-line storage facilities.

Network Services - services provided by the network, usually implemented in software on end-host or server systems that form part of the network infrastructure, for example:

— connectivity,

— e-mail,

— file transfer,

— directory services.

Network services may be:

— owned and operated by the organization,

— owned by the organization but operated by external agencies under contract,

— leased from external agencies,

— purchased ad-hoc from external providers,

— a combination of the above.

Network Infrastructure - the underlying hardware and software facilities, for example:

— premises,

— cabling,

— wireless facilities,

— network devices (e.g. routers, switches, modems, etc.).

As reflected in Clause 12 above, these aspects of network security should be modeled as network facets. These facets build upon each other in effect to form a network security management framework, as shown in Figure 4 below:

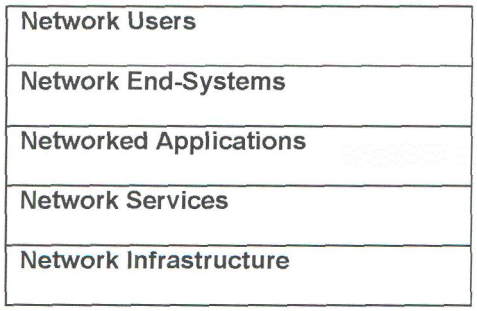

Figure 4 — Facets in a Network Security Management Framework

There is inevitably some overlap, with some systems performing multiple roles in any realistic network scenario. However, these conceptual facets of functionality should assist the necessary systematic process of assessment required to determine the security risks present in any particular network scenario. Each facet in this conceptual security framework should be managed individually, and all the facets should be managed collectively, to ensure that the overall objectives are met for a secure network.

13.4.3 Roles and Responsibilities

The roles and responsibilities that should be instigated associated with network security management are as follows. (It should be noted that, depending upon the size of the organization, these roles may 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,

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,

Network Security team:

— acquire, develop, test, check and maintain security components and tools,

— maintain security tools and components to follow closely the evolution of threats (e.g. updating virus signature files),

— update 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 security specifications, rules, and parameters required by the 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 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 of systems with network security policy,

— check and test compatibility of operating security rules with the current business requirements and legal restrictions (e.g. lists granted for network accesses).

13.4.4 Network Monitoring

Network monitoring is a very important part of network security management. This is dealt with in Clause 13.7 below.

13.4.5 Evaluating Network Security

Network security is a dynamic concept. Security staff should keep up to date with developments in the field and ensure that any network 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.

13.5 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 a network, most often observed in the areas of availability and confidentiality. Thus technical vulnerability management should be present covering all components of a network, and should include:

— obtaining timely information about technical vulnerabilities,

— evaluating the exposure of the network to such vulnerabilities,

— defining appropriate controls to address the associated risks, and

— the implementation and verification of the defined 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 the technical vulnerability management for network components into the overall task should be the preferred solution. (Further information on technical vulnerability management, including implementation guidance, can be found in ISO/IEC 17799.)

13.6 Identification and Authentication

13.6.1 Background

It is important to ensure that the security of network service and related information is preserved by restricting access through connections to authorized personnel (whether internal or external to the organization). Requirements for these are not exclusive to the use of network connections, and thus detail appropriate to the use of a network connection should be obtained by using ISO/IEC 17799. ISO/IEC 13335-2, when published, will also provide relevant detail.

Four control areas that could be relevant to the use of network connections, and the information systems directly related to such connections, are introduced in Clauses 13.6.2 to 13.6.5 below.

13.6.2 Remote Log-in

Remote log-ins, whether from authorized personnel working away from the organization, from remote maintenance engineers, or personnel from other organizations, 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 controls appropriate to the nature of the connection type. Control examples are:

— not allowing direct access to system and network software from accounts used for remote access, except where additional authentication has been provided (see Clause 13.6.3 below), and perhaps end-to-end encryption,

— 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.

13.6.3 Authentication Enhancements

The use of user id/password pairs is a simple way to authenticate users, but they can be compromised or guessed. There are other more secure ways to authenticate users, particularly remote users. Authentication enhancements should be required when a high possibility exists that an unauthorized person may gain access to protected and important systems. This may be, for example, because the access may be initiated using public networks, or the accessing system may be out of the direct control of the organization (e.g. via a laptop).

Where authentication enhancements over network connections are required (for example, by contract) or justified by the risks, an organization should consider strengthening the person authentication process by implementing relevant controls.

Simple examples are using:

— CLID, which may be thought of as the originating telephone number seen by the receiving equipment. Although CLID has some value as being the claimed ID of the calling party, it is open to spoofing and should not be used as a proven ID without further authentication. CLID is often used as a quick identifier in the establishment of backup links (especially over ISDN) between sites,

— links via modems that are disconnected when not in use, and only connected after verification of the caller's identity.

More complex, but very important, 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 (e.g. through readers attached to PCs), hand held one time pass key generation devices, and biometric based facilities,

— 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. If tokens are used, a user is required to know a PIN which with the token enables the production of a unique authentication value. With regard to smartcards, these can be viewed as automating the use of token access. In order to be 'opened', the user should supply the PIN to the card after inserting it into the smartcard reader. Then, whenever authentication is required by the central or remote systems, the smartcard may be 'called' directly to 'sign' data (proving authentication) using a key embedded in the smartcard.

13.6.4 Remote System Identification

As implied in Clause 13.6.3 above, where relevant authentication should be enhanced by verification of the system (and its location/access point) from which external access is made.

It should be recognized that different network architectures can offer differing identification capabilities. Thus, the organization may achieve enhanced identification by choosing an appropriate network architecture. All security control capabilities of the chosen network architecture should be considered.

13.6.5 Secure Single Sign-on

Where network connections are involved, users are likely to encounter multiple identification and authentication checks. In such circumstances users may 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 of 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, it should be noted 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 may 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.

13.7 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 connections, 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 networking 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 may 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 may be that there are substantial "drops" in the firewall logs, indicating probing activity against a potential target. An IDS system may also detect this in real time against an attack signature. Thus, it is emphasized that great care should be taken in selecting the right audit log analysis tools, to provide quick, focused and readily understandable outputs.

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 may 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.

Ongoing monitoring should include coverage of the following:

— 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, etc.,

— output from IDS,

— results from network security scanning activities,

— information on events and incidents reported by users and support personnel,

(as well as results from security compliance reviews).

Events may turn out to be a security incident but have been prevented, e.g. a 'bad' logon, or have actually caused an incident but have now been detected, e.g. recognition of which user has carried out an unauthorized database change.

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, 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 network audit logging and monitoring controls required in relation to network connections and related information systems can be determined by using ISO/IEC 17799 and with ISO/IEC 13335-2, when published.

13.8 Intrusion Detection

As network connections increase, it becomes easier for intruders to:

— find multiple ways to penetrate an organization or community's information systems and networks,

— disguise their initial point of access, and

— 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 an intrusion detection capability. Such a capability provides the means by which to predict intrusions, and identify intrusions in real-time and raise appropriate alarms. 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.

In many situations it may be clear that some unauthorized or unwanted event is happening. It could be a slight degradation in services for apparently unknown reasons, or it could be an unexpected number of accesses at unusual times, or it could be the denial of specific services. In most situations it is important to know the cause, severity and scope of the intrusion as soon as possible.

It should be noted that this capability is more sophisticated than the audit log analysis tools and methods that are implied in Clause 13.7 above and the related clauses of ISO/IEC 17799, and ISO/IEC 13335-2 when published. The more effective intrusion detection capabilities use special post-processors that are designed to

use rules to automatically analyze past activities recorded in audit trails and other logs to predict intrusions, and to analyze audit trails for known patterns of malicious behavior or behavior which is not typical of normal usage.

Thus, an IDS is a system for detecting intrusion into a network. There are two types of IDS:

— NIDS,

— HIDS.

NIDS monitor packets on a network and attempts to discover an intruder by matching the attack pattern to a database of known attack patterns. A typical example is looking for a large number of TCP connection requests (SYN) to many different ports on a target machine, thus discovering if someone is attempting a TCP port scan. A network intrusion detection system sniffs network traffic, by promiscuously watching all network traffic.

HIDS monitor activity on the hosts (servers). It does this by monitoring security event logs or checking for changes to the system, such as changes to critical system files, or to the systems registry. There are two types of HIDS:

— system integrity checkers, which monitor system files and systems registry for changes made by intruders,

— log file monitors (that monitor the system log files). Operating systems generate security events about critical security issues, such as a user acquires root/administrator level privileges.

In some cases responses to detected intrusions can be automated in IPS>

Further detail on intrusion detection is provided in ISO/IEC 18043.

13.9 Protection against Malicious Code

Users should be aware that malicious code, including viruses, may be introduced into their environment 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 may 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 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 viruses, worms and Trojans (which sometimes are collectively termed '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-virus software should be run on the remote systems and also on the servers on the central system - especially Windows and e-mail servers.

Users and administrators of systems with network connections 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 17799, and will be in ISO/IEC 13335-2 when published.

13.10 Common Infrastructure Cryptographic Based Services

13.10.1 Preface

The need for security and enhanced privacy is increasing as electronic forms replace their paper-based counterparts. The emergence of the Internet and the expansion of corporate networks to include access by customers and suppliers from outside an organization have accelerated the demand for solutions based on cryptography, to support authentication and VPNs, and to ensure confidentiality.

13.10.2 Data Confidentiality over Networks

In circumstances where preservation of confidentiality is important, encryption controls should be considered to encrypt information passing over network connections. The decision to use encryption controls should take account of relevant government laws and regulations, the requirements for key management, and the suitability of the encryption mechanisms used for the type of network connection involved and the degree of protection required.

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.

13.10.3 Data Integrity over Networks

In circumstances 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 (see Clause 13.10.4 below). The decision to use digital signature or message integrity controls should take account of relevant government laws and regulations, relevant public key infrastructures, the requirements for key management, the suitability of the underlying mechanisms used for the type of network connection 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.

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.

13.10.4 Non-Repudiation

Where there is a requirement to ensure that substantive proof can be provided that information was carried by a network, 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 should it be contested, 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.

Further information on non-repudiation is provided in ISO/IEC 14516 and ISO/IEC 13888.

13.10.5 Key Management

13.10.5.1 Overview

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.

Whereas in very small environments with only a few connections this can be achieved with manual organizational procedures (e.g. the manual exchange of symmetric encryption keys), in bigger environments pre-defined and automated procedures are necessary, and the use of public/private key encryption technologies will in most cases provide benefits.

Public/private key encryption technologies do solve one major problem with symmetric encryption technologies. Symmetric technologies require the same key to be present at both sides of the communication (they are also referred to as shared secret technologies), and therefore imply a transfer of the symmetric encryption key. Since the symmetric encryption key itself has to be kept confidential, an already established secure data channel for exchanging the key is necessary. Public/Private key encryption technologies overcome this problem by providing two keys and requiring only one of them to be transferred to the other communication entity. Since this one is not confidential (it is referred to as a public key) it can be transmitted over public communication channels. The other, not to be transferred, key still has to be treated confidentially (and is referred to as a private key).

However, some problems still remain, mainly:

— the authentic transfer of the public key, or how to obtain the public key of the other communication entity authentically,

— the appropriate protection of the private key.

The transfer of the public key has to ensure that the receiving entity gets the public key the sending entity did send. In other words the transfer needs to be authentic, otherwise a possible attacker observing the public key transfer may be able to exchange an unrecognized key with another one (sometimes termed a 'men in the middle attack').

Several techniques are available to check the authenticity of a transferred public key. The most obvious way is to check for the equality of the sent and the received public key. This is usually done by comparing a hash value (in this context often referred to as a 'fingerprint') of the key sent and the key received in an interactive way. The sending and the receiving entity of the key may therefore use a separate channel (e.g. a telephone line), and it is important that this channel allows a proper authentication of the sending and the receiving entities (e.g. if the receiving entity can authenticate the sending entity by recognizing his/her voice).

Whereas this bilateral way of public key exchange works if only a small number of communicating entities are involved, it does not scale up. This can be solved by introducing infrastructures providing every entity's public key and certifying the authenticity of the provided public keys. Such infrastructures, typically named a PKI, are composed of various components. New entities joining are registered by a Registration Authority, which has the main task to verify the proper identity of the entity. Based on this Registration, the Certification Authority is then able to certify the entity's public key, and Directory Services are typically present to make the certified public keys (usually referred to as just 'certificates') available to all entities designated to use the system. Technically a certificate consists of a well defined set of the entity attributes (examples are name and e-mail address for user entities) and the entities public key, and the authenticity of this information is assured by digitally signing of this information by the Certification Authority.

Since the security of all cryptographic services using public keys provided and managed by a PKI rely on the authenticity of these keys, PKIs have very high security requirements. As an illustration, if an attacker gains access to the Certification Authority infrastructure he/she may be able to issue certificates which enables the possibility to impersonate entities.

Most PKI need to be attached to a network for functionality reasons, and therefore specific attention has to be drawn to proper network security controls in order to be able to fulfill the high security requirements of PKI. In many cases these security controls include the setting up of a dedicated network for the core PKI components, and to protect this network by appropriate security gateways or firewalls.

With regard to the appropriate protection of the private keys, this protection is crucial to security as well, since if an attacker has access to an entity's private key he/she has the possibility to impersonate the entity. Usually, depending on the security requirements of specific organizations, environments or applications, several solutions are available.

The simplest solution is to protect the private key by storing it in symmetric encrypted form on the entity's systems or, a little bit better, on a removable media. The entity has then typically to key in a password (which constructs the symmetric encryption key) to unlock the private key and make it available to services and applications for further usage. This solution has the significant benefit of being fully software based and can therefore be implemented in most environments relatively easily. However, from a security perspective, there are major drawbacks, as protection:

— is dependent on the quality of the chosen password, and

— relies on the integrity of the system used by the entity. If an attacker gains control of this system he/she may copy the private key which is stored in memory in unencrypted form during processing of cryptographic functions, or he/she may achieve the same result by getting the entity's password and the public key in an encrypted form.

Smartcard based solutions are available to overcome these drawbacks. They provide a two factor authentication for accessing the private key (typically possession of the smartcard and knowledge of a password or PIN to unlock it), and their architecture does ensure that the private key never leaves the smartcard, which implies that all core cryptographic computations requiring the private key are processed on the smartcard itself. As a significant advantage this solution protects the private key even in situations when the integrity of the system used by the entity is compromised. The major drawback of smartcard based solutions is the need to distribute and integrate the specific smartcard related hardware to the entities and their systems. Although there are technical standards available in this area, this is usually a quite complex and cost intensive process.

It is emphasized that this clause only provides a brief overview of the topic of key management. For further information on the topic, 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 IS 11568 - Banking - retail key management,

— ISO IS 11649 - Banking - multicenter key management,

— ISO IS 13492 - Retail key management data elements,

— ISO IS 21118 - Banking Public Key Infrastructure.

13.10.5.2 Security Considerations

There are a number of security considerations to be made in the context of key management, in particular when using or implementing PKI services.

These considerations include topics such as:

— scope and usage - the intended usage of a PKI has significant influence on the actual security required. As an example, the usage of the issued certificates do mainly influence the security requirements of a PKI,

— policies - provided PKI services and their purpose, the level of protection implemented in a PKI, and interaction processes need to be documented appropriately in a Certificate Policy (CP) and a Certificate Practice Statement (CPS),

— implementation issues - an organization may choose to implement a PKI in-house ('insourced PKI') or may decide to just buy PKI services ('outsourced PKI'), or may choose to implement a combination of both (e.g. just buy the core certification services, but implement other services, such as a roaming directory, locally),

— specific functional requirements, e.g. for roaming users - many functional requirements require specific security controls. One example is how to provide protection of the private keys and access to certificates for roaming users; one solution therefore is the use of smartcards (see below),

— use of smartcards - smartcards may be used to fulfill higher security requirements (e.g. as mentioned in Clause 13.10.5.1 above) or to solve issues in the context of roaming users. However, the use of smartcards does require many further considerations, such as a lifecycle process for smartcards, physical distribution and handling of smartcards, fail back processes (e.g. when a user forgets his/her smartcard), security issues with the used reader hardware and the appropriate integration software on the client system,

— operational issues, e.g. online/offline operation of the root Certification Authority - specific operational measures can be used to fulfill the specified security requirements. As an example, taking the root Certification Authority offline when its services are not used, combined with adequate physical protection, can be used to provide a higher level of protection for the most sensitive parts of the system.

13.11 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 - establishing business recovery priorities, timescales and requirements (supported by business impact analysis review), 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/IEC 17799. ISO/I EC 13335-2, when published, will also provide guidance.

From the networking perspective, it is the maintenance of network connections, the implementation of alternative connections of sufficient capacity, and the recovery of connections subsequent to an unwanted

event, 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 a 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.

14 Implement and Operate Security Controls

Once the technical security architecture and the security controls have been identified, documented and agreed, the network security controls should be implemented. Before networking operations are permitted to commence, the implementation should be reviewed, tested, and any identified security deficiencies dealt with (see also Clause 15 below). Then, once the security has been 'signed off', live operations should commence. Over time, and if significant change occurs, then further implementation reviews should be conducted (see also Clause 15 below).

15 Monitor and Review Implementation

As reflected in Clause 14 above, the first implementation should be reviewed for compliance with the documented technical security architecture and required security controls specified in the following documents:

— technical security architecture,

— networking 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 is complete when all deficiencies have been identified, fixed, and signed off by senior management. Post live operation, ongoing monitoring and review activities should also be conducted, particularly including prior to a major new release related to significant changes in business needs, technology, security solutions, etc., and otherwise annually.

It is emphasized that 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. Normally 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 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, with an addendum confirming that all agreed fixes have been applied. Such reports should be signed off by senior management.

Bibliography

[I] ISO/IEC TR 14516:2002, *Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*

[2] ISO/IEC 13888 (all parts), *IT security techniques — Non-repudiation*

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

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

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

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

[7] ISO/IEC 27005, *Information technology — Information security risk management* [1o])

[8] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[9] ITU-T X.810 | ISO/IEC 10181-1:1996, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Overview*

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

[II] IETF IP Security Document Roadmap (RFC 2411), November 1998.

[12] IETF Security Architecture for the Internet Protocol (RFC 2401), November 1998. [13]

IETF Address Allocation for Private Internets (RFC 1918), February 1996. [14] IETF

SNMP Security Protocols (RFC 1352), July 1992.

[15] IETF Internet Security Glossary (RFC 2828), May 2000.
http://www. ietf. org/rfc/rfc2828.txt

[16] NIST Special Publications 800 series on Computer Security, including:

— NIST Special Publication 800-10: Keeping Your Site Comfortably Secure: An Introduction to Firewalls.

10) To be published. (Revision of ISO/IEC TR 13335-3:1998 and ISO/IEC TR 13335-4:2000.)

ICS 35.040
Price based on 59 pages