AS/NZS ISO/IEC 18028.1:2008
ISO/IEC 18028-1:2006

AS/NZS ISO/IEC 18028.1:2008

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 1: Network security management

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT-012, Information Systems, Security and Identification Technology. It was approved on behalf of the Council of Standards Australia on 28 May 2008 and on behalf of the Council of Standards New Zealand on 31 May 2008.
This Standard was published on 25 June 2008.

The following are represented on Committee IT-012:

Attorney General's Office
Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Chamber of Commerce and Industry
Australian Electrical and Electronic Manufacturers Association
Certification Forum of Australia
Council of Small Business Organisations
Internet Industry Association
NSW Police
New Zealand Defence Force
Reserve Bank of Australia

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about joint Australian/New Zealand Standards can be found by visiting the Standards Web Shop at www.standards.com.au or Standards New Zealand web site at www.standards.co.nz and looking up the relevant Standard in the on-line catalogue.

Alternatively, both organizations publish an annual printed Catalogue with full details of all current Standards. For more frequent listings or notification of revisions, amendments and withdrawals, Standards Australia and Standards New Zealand offer a number of update options. For information about these services, users should contact their respective national Standards organization.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Please address your comments to the Chief Executive of either Standards Australia or Standards New Zealand at the address shown on the back cover.

This Standard was issued in draft form for comment as DR 07261.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

Australian/New Zealand Standard™

Information technology—Security techniques—IT network security

Part 1: Network security management

First published as AS/NZS ISO/IEC 18028.1:2008.

COPYRIGHT

© Standards Australia/Standards New Zealand

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Jointly published by Standards Australia, GPO Box 476, Sydney, NSW 2001 and Standards New Zealand, Private Bag 2439, Wellington 6020

ISBN 0 7337 8769 X

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012, Information Systems, Security and Identification Technology.

The objective of this Standard is to provide IT professionals and general line management with detailed guidance on the planning, installation and ongoing maintenance of IT networks.

This Standard is identical with, and has been reproduced from ISO/IEC 18028-1:2006, *Information technology—Security techniques—IT network security,* Part 1: *Network security management*.

As this Standard is reproduced from an international standard, the following applies:

(a) Its number appears on the cover and title page while the international standard number appears only on the cover.

(b) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

Reference to International Standard		*Australian/New Zealand Standard*	
ISO/IEC		AS/NZS	
17799	Information technology—Security Techniques—Code of practice for information security management	27002	Information technology—Security Techniques—Code of practice for information security management
		AS/NZS ISO/IEC	
18028	Information technology—Security techniques—IT network security	18028	Information technology—Security techniques—IT network security
18028-2	Part 2: Network security architecture	18028.2	Part 2: Network security architecture
18028-3	Part 3: Securing communications between networks using security gateways	18028.3	Part 3: Securing communications between networks using security gateways
18028-4	Part 4: Securing remote access	18028.4	Part 4: Securing remote access
18028-5	Part 5: Securing communications across networks using virtual private networks	18028.5	Part 5: Securing communications across networks using virtual private networks
18044	Information technology—Security techniques—Information security incident management	18044	Information technology—Security techniques—Information security incident management

Any international references not listed have not been adopted as Australian or Australian/New Zealand Standards.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

CONTENTS

Page

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

Page

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

AVA Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

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).

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

NOTES

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

Full document details: AS NZS ISO IEC 18028.1-2008

AUSTRALIAN/NEW ZEALAND STANDARD

Information technology — Security techniques — IT network security —

Part 1:
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*

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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/IEC 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/IEC 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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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
Telnet	Terminal 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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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,

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

— 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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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

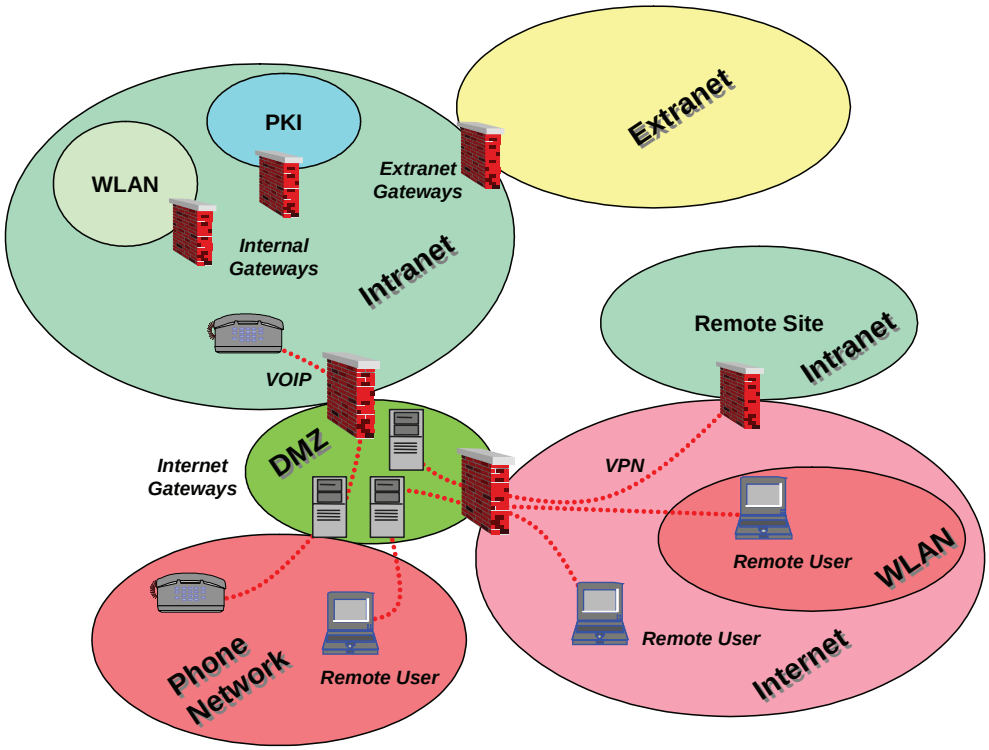

Figure 1 — Typical Networking Environment

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

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

- 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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

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).

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008

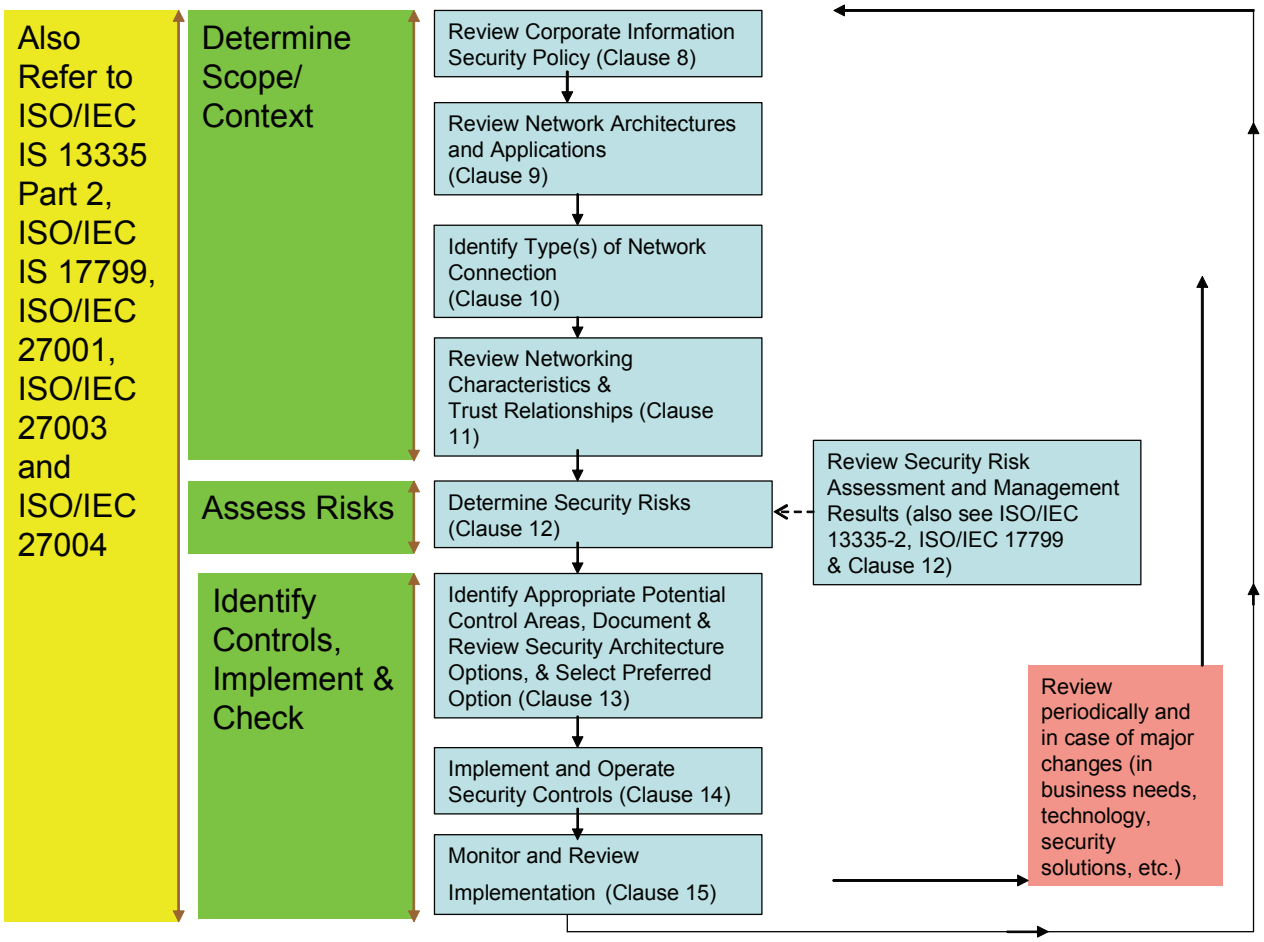

Figure 2 — Management Process in the Context of Network Security

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.

Accessed by MONASH UNIVERSITY LIBRARY on 15 Jun 2015 (Document currency not guaranteed when printed)

Documents
Document Sharing Hub

COPYRIGHT

Full document details: AS NZS ISO IEC 18028.1-2008