Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N14247
Date:	2010-03-22
Replaces:	
Document Type:	Liaison organization contribution
Document Title:	Liaison Statement from JTC 1/SC 27 to ISO/IEC JTC 1/SC 6
Document Source:	JTC 1/SC 27
Project Number:	
Document Status:	For your information.
Action ID:	FYI
Due Date:	
No. of Pages:	98

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE: liaison statement

TITLE: **ISO/IEC JTC 1/SC 27 liaison statement to JTC 1/WG 7**

SOURCE: 39th Meeting of ISO/IEC JTC 1/SC 27/WG 2 (November 2009)
7th Meeting of ISO/IEC JTC 1/SC 27/WG 4 (November 2009)
8th Meeting of ISO/IEC JTC 1/SC 27/WG 5 (November 2009)

DATE: 2009-11-06

PROJECT: 29192-1/4;
27033-1/7;
29100; 29101; 29190; 24760;
29115; 29146; 29191; 24761;

STATUS: As per resolutions 20 (SC 27 N299), 14 (SC 27 N7908) and 11 (SC 27 N8138) of the November 2009 SC 27/WG 2, 4 and 5 meetings held in Redmond, Washington (November 2009) this document has been sent to JTC 1/WG 7.
It is circulated within SC 27 for information.

ACTION ID: FYI

DUE DATE:

DISTRIBUTION: P, O, L Members
L. Rajchel, JTC 1 Secretariat
K. Brannon, ITTF
W. Fumy, SC 27 Chairman
M. De Soete, SC 27 Vice-Chair
M. Bañon, E. J. Humphreys, M.-C. Kang, K. Naemura, K. Rannenberg, WG-Conveners
J. Lee, Secretariat of JTC 1/WG 7

MEDIUM: Livelink-server

NO. OF PAGES: 1+2

Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1SC 27.din.de/en

ISO/IEC JTC 1/SC 27 Liaison Statement to ISO/IEC JTC 1/WG 7

Input from WG 2

Title: Liaison statement to ISO/IEC JTC 1/WG 7
Source: ISO/IEC JTC 1/SC 27/WG 2
Date: 2009-11-06

JTC 1/SC 27/WG 2 wishes to inform JTC 1/WG 7 of the development of a standard, ISO/IEC 29192 Lightweight cryptography, which is currently in working draft stage. Lightweight cryptography has applications in, amongst others, sensor networks where low power consumption is important.

JTC 1/SC 27/WG 2 requests JTC 1/WG 7 to give input to the criteria that sensor networks have for cryptographic algorithms and protocols that JTC 1/SC 27/WG 2 should consider when selecting suitable algorithms and mechanisms using asymmetric techniques for inclusion in ISO/IEC 29192. The current draft of ISO/IEC 29192 will be made available for comments from JTC 1/WG 7 preferably before the next SC 27 Working Group meetings in April, 2010.

Input from WG 4

Title: Liaison Statement from ISO/IEC JTC 1/SC 27/WG 4 to JTC 1/SC 6/WG 7 on potential collaborative work on Network Security and Sensor Networks

ISO/IEC JTC 1/SC 27/WG 4 thanks JTC 1/SC 6/WG 7 for providing the information on the work being done on Sensor Networks and forwarding the 1st CD ISO/IEC 29180, Security framework for sensor network.

ISO/IEC JTC1/SC 27/WG 4 sees that the work being done ISO/IEC 27033 documents on Network Security may be used in support of securing sensor networks.

ISO/IEC 27033: Information technology — Security techniques — Network security:

• Part 1: Overview and concepts (FDIS)
• Part 2: Guidelines for the design and implementation of network security (1st CD)
• Part 3: Reference network scenarios – Threats, design techniques and control Issues (FCD),
• Part 4: Securing communications between networks using security gateways – Threats, design techniques and control Issues (1st WD)

The latest drafts of these documents are attached for review and comments.

In addition the following parts of Network Security will be developed in the future, subject to national bodies contributions:

• Part 5: Securing virtual private network - Threats, design techniques and control issues
• Part 6: IP Convergence
• Part 7: Wireless

We look forward to further collaboration.

Input from WG 5

Liaison statement to JTC 1/WG 7 on Identity Management, Privacy Technology, and Biometrics

ISO/IEC JTC 1/SC 27/WG 5 would like to thank JTC 1/WG 7 for their continued interest in the work of ISO/IEC JTC 1/SC 27/WG 5.

ISO/IEC JTC 1/SC 27/WG 5 took note of the JTC 1/SGSN report on privacy (SC27 N7964) and equally considers privacy aspects of relevance to the work on sensor networks. ISO/IEC JTC 1/SC 27/WG 5 therefore would appreciate further exchange, especially with regard to the Reference Architecture for Sensor Networks. An overview of the progress of the different projects of ISO/IEC JTC 1/SC 27/WG 5 is attached to this document. ISO/IEC JTC 1/SC 27/WG 5 would like to especially draw the attention of ISO/IEC JTC 1/WG 7 on the progressed work in WD 29101 Privacy Reference Architecture and CD 29100 Privacy Framework.

Below is a short summary of the activities at the recent meeting on the different projects; the respective new documents will be provided upon their availability. The next meeting of ISO/IEC JTC 1/SC 27/WG 5 is scheduled for 19 – 23 April 2010 in Melaka, Malaysia. WG 5 would welcome comments and contributions by April 1.

ISO/IEC CD 29100 – Privacy Framework. ISO/IEC JTC 1/SC 27/WG 5 agreed on a split of the draft by moving Clause 7 on the implementation of privacy controls in ICT systems to WD 29101. By this the current document is expected to be more concise and consistent, while at the same time this will enrich WD 29101 bridging between the two documents explaining the implementation of privacy principles in ICT systems.

ISO/IEC WD 29101 – Privacy Reference Architecture. ISO/IEC JTC 1/SC 27/WG 5 received substantial input on the project, which resulted in the formation of a small work group that is developing improvements to the reference architecture and a classification of privacy-enhancing technologies that will be integrated into the next WD of the document. Further input results from the transferral of Clause 7 of CD 29100.

ISO/IEC CD 24760 – A Framework for Identity Management. ISO/IEC JTC 1/SC 27/WG 5 editing session on 1st CD 24760 discussed a proposed split of the document, which was supported by a number of NBs, but a formal decision was deferred to the next meeting of ISO/IEC JTC 1/SC 27/WG 5. As a result of a general discussion of the progress and perspective of the document, it was decided to install an ad-hoc group to support the editors. The mandate of this group is to restructure and reword Clause 6 of the document and advise the group on technical issues to be addressed at the next ISO/IEC JTC 1/SC 27/WG 5 meeting.

ISO/IEC WD 29146 – A Framework for Access Management. The document is still in an early state. ISO/IEC JTC 1/SC 27/WG 5 is therefore asking for further input and contributions.

ISO/IEC WD 29115 I X.eaa – Entity Authentication Assurance, common text project with ITU-T. ISO/IEC JTC 1/SC 27/WG 5 appointed Erika McCallister (US NB) as acting editor. The US NB contributed a significant revision to the 5th WD. It was agreed to use this contribution as a basis for the 6th WD of 29115. ISO/IEC JTC 1/SC 27/WG 5 also proposes a title change to “Entity Authentication Assurance Framework”, as well as a change in the scope to reflect the updated structure and content of the document.

ISO/IEC CD 24745 – Biometric Template Protection. ISO/IEC JTC 1/SC 27/WG 5 proposes a title change to ‘Biometric Information Protection’. The editing session concluded to call for a 2nd CD ballot.

ISO/IEC WD 29191 – Relative Anonymity with Identity Escrow. ISO/IEC JTC 1/SC 27/WG 5 considers a title change and will seek SC 27 approval in Malaysia. The current proposal is 'Requirements on partial anonymity', but WG 5 is welcoming further comments on this matter.

ISO/IEC WD 29190 – Privacy Capability Maturity Model. ISO/IEC JTC 1/SC 27/WG 5 is issuing a 2nd call for editors for this project. Input from the US NB has been provided as a starting point for the further development of the project. Robin Wilton was appointed acting editor and a 1st WD will be produced.

Committee Draft **ISO/IEC CD 27033-2 (revision of 18028-2)**	Reference number: ISO/IEC JTC 1/SC 27 **N7919**
Date:**2010-01-09**	Supersedes document SC 27 N6920
THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.	
ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-04-09** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC CD 27033-2

Title: Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security

Project: 27033-2 (revision of 18028-2) (1.27.58.02)

Explanatory Report

Status	SC 27 Decision	Reference documents	
		Input	Output
Study Period	1st WG 4 meeting, Nov. 2006, Resolution 2 (N5499).		Report Joint WG1/WG4 meeting (N5384); Report (N5484); Call f. Contr (N5568).
Revision approval of 18028-2:2006-02-01 (1st Ed)	SC 27 approval of revision as per SoV (N6094)	SoContr (N5652); JP[1)] contr. (N5760).	Termination of SP and recommendation on revision as per WG 4 resolution 5 (N5740); Report (N5930); DoC (N5938); 60-day LB (N5983).
	SC 27 approval of revision as per SoV (N6094)		
1st WD 18028-2* (revision) (27033-2) *** subject to SC 27 approval of renumbering to 27033-2**	Resolution 5 of 2nd WG 4 meeting (N5740), May 2007 and Resolution 2 of 19th SC 27 Plenary (N5939) May 2007.		Text f. 1st WD (N5912).
2nd WD 27033-2* * subject to JTC 1 endorsement of renumbering	3rd WG 4 meeting, Oct. 2007, resolutions 1 & 3 (N6017).	SoCom. (N6087rev1)	DoC (N6022); Text for 2nd WD (N6278); Proposed modif. (renumbering) (N6406); JTC 1 endorsm. (N6457).
3rd WD 27033-2	4th WG 4 meeting, Apr. 2008, resolutions 1, 5 & 7 (N6421); 20th SC 27 Plenary, resolution 2 (N6799); Deleg. of Auth. for 1st CD resolution 14 (N6799).	SoCom (N6513rev1);	DoC (N6425); Text f. 3rd WD (N6439)
4th WD 27033-2	5th WG4 meeting, Oct. 2008	SoCom (N6994)	DoC (N6911)N/A; Text f. 4th WD (N6920)N/A
	6th WG 4 meeting, May 2009, resolution 1 (N7551).		DoC (N6911); Text f. 4th WD (N6920).
1st CD 27033-2	7th WG 4 meeting, Nov 2009, resolutions 1, 3 (N7908).	SoCom (N8033)	DoC (N7918); Text f. 1st CD (N7919).

CD Registration and Consideration

In accordance with resolution 3 (see SC 27 N7908) of the 7th SC 27/WG 4 meeting held in Redmond, WA, USA (November 2009), the attached document has been registered with the ISO Central Secretariat (ITTF) as 1st CD and is hereby circulated for a 3-month CD letter ballot closing by **2010-04-09.**

[1)] Member body (for country code according to ISO 3166, e.g. CN for China.)

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10787 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 N7919

Date: 2010-01-04

ISO/IEC 1st CD 27033-2

ISO/IEC JTC 1/SC 27

Secretariat: DIN

Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Contents Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2. The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques – Network Security*:

— *Part 1: Overview and concepts,*

— *Part 2: Guidelines for the design and implementation of network security,*

— *Part 3: Reference networking scenarios – Risks, design techniques and control issues,*

— *Part 4: Securing Communications between networks using security gateways - Risks, design techniques and control issues,*

— *Part 5: Securing communications across networks using Virtual Private Networks (VPNs) - Risks, design techniques and control issues,*

— *Part 6: IP convergance*

— *Part 7: Wireless*

It should be noted that there may be further expansion on the parts mentioned above. This is due to the ever changing and evolving technology in the network security area.

Information Technology — Security techniques — Network security —

Part 2: Guidelines for the design and implementation of network security

1 Scope (and Objectives)

ISO/IEC 27033-2 provides guidance for organizations to ensure appropriate technical network security through a well-proven and consistent approach to the planning, design, documentation and implementation of network security.

2 Normative references

For the purposes of this document, the normative references given in ISO/IEC 27033-1 are applicable.

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), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27033-1.

4 Abbreviations

For the purposes of this document, the abbreviations used in ISO/IEC 27033-1 and the following are applicable.

IPS	Intrusion Prevention System
POC	Proof of Concept
RADIUS	Remote Authentication Dial-In User Service
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
TACACS	Terminal Access Controller Access-Control System
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

5 Document Structure

This document helps organizations understand what is needed for the design and implementation of network security to meet the associated controls in ISO/IEC 27001.

This document shows a process, but the document is technical in nature and uses the process as a way to provide a flow for the document. Unless otherwise noted within this document, references to architecture, design and implementation will represent the technical architecture, technical design and technical implementation. The scope includes existing and/or planned networks in an organization.

Initial items needed for preparation are discussed in Clause 6. These include:

- Project initiation
- Determine requirements of organization
- Identification of assets to be protected
- Review architecture, designs, or implementations
- Review any Security Risk Assessment and Risk Management results
- Determine performance, reliability and availability requirements

Once the initial items needed for preparation are compiled then there are guidelines on creating a Network Technical Security Design. The items discussed are technical design guidelines that can be used in most cases for any network security design. These guidelines include:

- Best Practice Design (includes defence in depth, network components, design resilience, network management, etc)
- Use of “Scenario” and “Technologies”
- Use of models and frameworks
- Product selection
- Proof of Concept
- Documentation of architecture
- Testing
- Implementation

The Annexes cover the mapping of ISO/IEC 27001 controls that are related to Network Security, documentation templates and an example of mapping a framework to ISO/IEC 27001.

6 Preparing for Design and Implementation of Network Security

6.1 Introduction

The security architecture for any networking project (i.e. the design of a network security infrastructure) should be fully documented and agreed, before finalizing the list of related security controls for implementation.

Further, the early documentation of the possible network 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 security requirements that will often arise, before agreement on the preferred network security architecture.

In documenting the options, due account must be taken of any particular organization/community networking and information security policy requirements, the relevant existing and/or proposed network architecture and network applications, security risk assessment and risk management results – including the list of potential security controls identified, and any existing network security architecture aspects. Once the options have been documented and reviewed, as part of the network architecture design process, the preferred technical security architecture should be agreed and documented in a network security architecture document (an example template for which is shown in Annex B.1). Changes might result to the network architecture to ensure compatibility between it and the agreed network security architecture, and/or the list of potential security controls, e.g. because it is agreed that the network security architecture can only be technically implemented in a particular way, necessitating an alternative to an identified security control.

The organization's business requirements and processes should be reviewed and considered as part of the overall design. The business requirements and processes should be considered equally important to the security requirements and processes.

6.2 Overview

The process flow used in this document to achieve an technical network security architecture is shown in Figure 1. Figure 1 illustrates each step in the process giving a summary of the inputs and outputs to each step. Information for each step is then detailed in Sections 6 and 7 of this document. Note that even as this process is shown as linear, network security design and implementation is a repetitive process to be re-examined as new assets and risks are identified or when significant architectural changes are implemented that impact the general security policy.

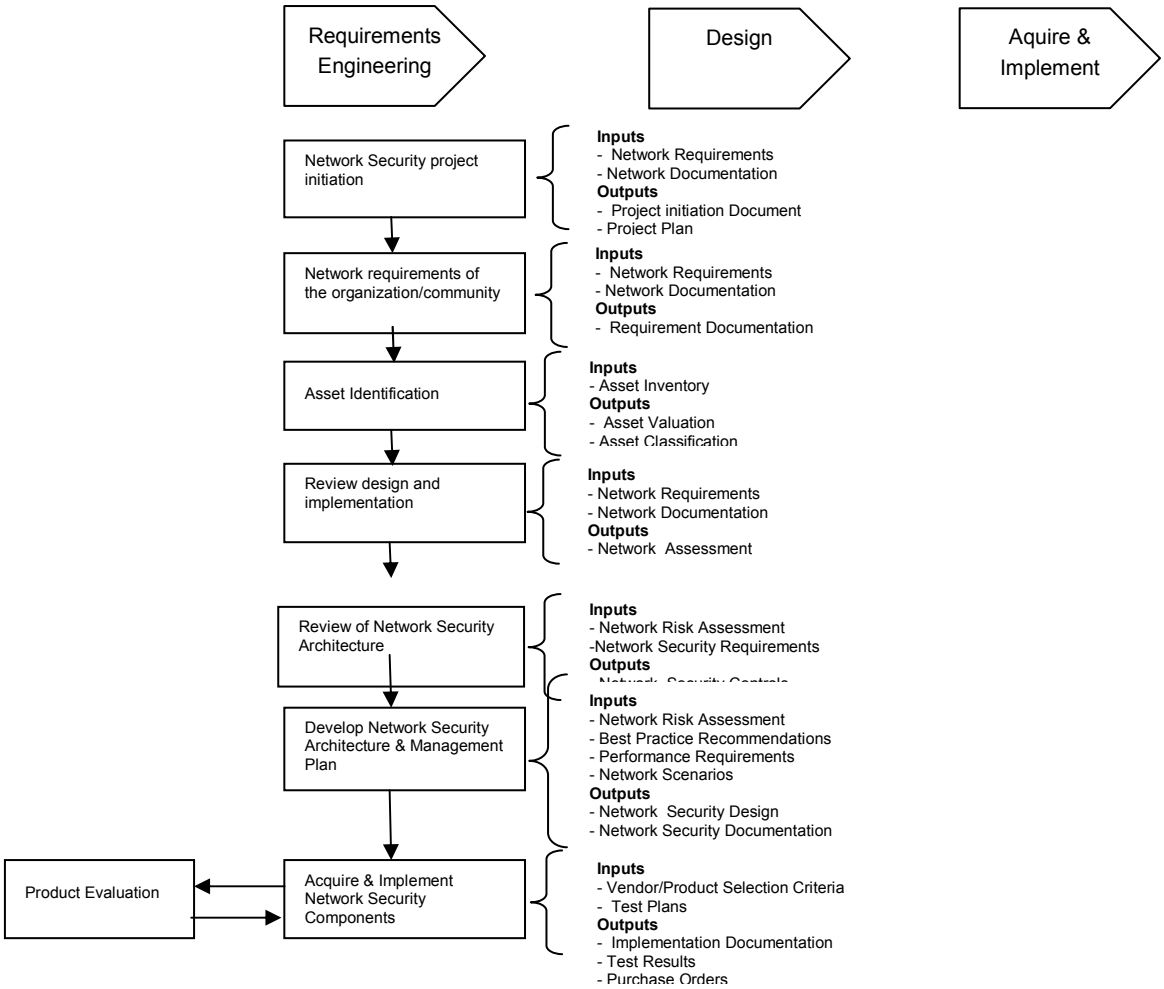

Figure 1. Process Flow

The inputs to the design process include:

- business requirements and processes;
- statement of service requirements, and other organization/community requirement documentation;
- network architecture/design documentation;
- current network security policy (or relevant parts of the associated information system security policy) – should be based on the results from a security risk assessment and risk management review;
- traffic requirements;
- current product information.

The outputs from the design process include:

- the network security architecture document (see Annex B.1 for an example template);
- service access (security) requirements documents for each security gateway/firewall system (which includes the firewall rule base(s) – see Annex B.2 for an example template);
- Security Operating Procedures;
- User guidelines for third party users, as relevant;
- Conditions for secure connection for third parties, as relevant.

Following implementation of the network security architecture, then security test plans should be produced and tested. Once acceptable test results have been achieved, with any adjustments made in the light of problems found during testing, then formal sign-off by the appropriate level of management should be obtained for the network security architecture.

Which ISO/IEC 27001 controls that this document can be used in support of are mapped in Annex A to describe the specific sections in this document to the specific controls that are applicable. Only the specific controls from ISO/IEC 27001 that are applicable to this document are listed.

6.3 Network security project initiation

An initial network security project meeting should be held to discuss how it should be managed, what information is required, what documentation is required, what tasks are to be conducted, who is to be involved, the timescales, formal sign-off requirements, and who will operate and maintain the controls once the project is implemented. The principal outputs from the networking project security initiation phase are the project initiation document and the project plan. Organizations that already have a project initiation process may find it useful at this stage.

6.4 Network requirements of the organization/community

The network requirements of the organization/community should be gathered and reviewed to ensure that they are still current and valid, including in terms of the types of access required and to what particular services, systems, facilities, etc. Examples of the network requirements may include (but are not limited to) reliability, bandwidth, and access

requirements. The review should include the constraints of the organization's environment, the ability to provision services, the physical limitations, (such as facilities, human factors, etc) and resources. Examples of access required could include requirements for simple mail transfer protocol (SMTP), outgoing access to the Internet, incoming access from the Internet, and access to other organizations (i.e. third party connections).

6.5 Asset Identification

Identification of assets is a critical first step in determining the information security risks to any network. Unless the key assets, particularly information, are properly identified their value to an organization cannot be properly measured (in terms of the potential adverse impacts on business operations were there to be breaches of confidentiality, integrity, non-repudiation and availability (by varying time periods)). The values of the assets need to be combined with the measures of likelihoods of identified threats and degrees of seriousness of identified vulnerabilities to those threats to calculate the measures of information security risks. Apart from the key information types, assets required to securely support management, control and user traffic and the features required for the functioning of the network infrastructure, services, and applications should be identified. This includes devices such as hosts, routers, firewalls, etc, interfaces (internal and external), information stored/processed and protocols used.

6.6 Review design & Implementation

. An assessment of the current capabilities and any planned technical network architecture changes needs to be reviewed and compared to the technical security architecture being developed to note any incompatibilities. Any incompatibilities need to then be reviewed and the appropriate architectures modified.

The information to be gathered during the assessment should include at a minimum the following:

- 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 technical security architecture and security controls, and the related designs
- network protocols to be used,
- network applications used on different aspects of the network

The information gathered should be accomplished in the context of the network capabilities. Detail should be obtained of the relevant network architecture and this shall be reviewed to provide the necessary understanding and context for 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 shall be adopted, should become more efficient and eventually result in 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.

6.7 Review of the network security architecture

The review of the security controls must be conducted in the light of the results from a security risk assessment and management review. The results of the security risk assessment may indicate which security controls are required commensurate with the assessed risks. Clause 6.8 covers confirmation of the results of the risk assessment. A gap analysis will need to be completed against the current network security architecture to determine what is not addressed in the existing network security architecture. The final network security architecture should encompass the existing controls and any missing controls.

6.8 Confirm security Risk Assessment and Risk Management Results

A review of information security controls must be conducted in the light of the results from the information security risk assessment and risk management review. Such a review should have addressed a number of key questions with regard to information security, including what:

- are the distinct types of network equipment and facility groupings that need to be protected?
- are the distinct types of network activities that need to be protected?
- what assets need to be protected?
- kind of protection is needed and against what threats?

In identifying the protection that is needed and against what threats, information security mechanism recommendations should be made for such as:

- protection against insider and outsider attacks,
- end-point security and compliance,
- authentication and integrity of signalling control and management traffic, such as user provisioning, network routing, and topology control data,
- encryption of sensitive data, such as user passwords, security configuration data, personally identifiable information, and lawful intercept configuration data,
- conformance with relevant organization's policies,
- conformance with relevant legal and regulatory compliance requirements, including:
  - intellectual property rights,
  - safeguarding of organizational records,
  - data protection/privacy,
  - prevention of misuse,
  - regulation of cryptography,
  - collection of evidence,

As stated earlier, the review of the information security risk assessment and risk management results will indicate what information security controls are required commensurate with the assessed risks, and that list will need to be matched against what exists and/or is planned to identify what additional information security controls are required, and maybe what are not and can be removed. Also part of the risk assessment and risk management results will be a prioritised list of assets to be protected. The required information security control list will include technical controls that need to be encompassed in the security architecture, and need to be accounted for in product selection.

6.9 Review performance requirements and confirm criteria

Traffic data is required to enable the configurations for the communication lines, servers and security gateways/firewalls to be documented such that on implementation a good level of service can be provided in accordance with user expectations – with no 'over-configuration' and related unnecessary costs. Information should be gathered on such as the speeds of any existing communication links, configuration/capacity of routers at any third party locations, the number

of users that will be allowed access via each link (concurrent access and number of users with access), minimum, average and maximum user connect time required, identity of what authorized users will access over the link, number of web page hits required, database access hits required, growth expected over one year and three/five years, and whether a Windows log-on is required. Use could be made of telecommunications table (queuing) theory for sizing the number of ports, channels required, particularly over dial-up links. These performance requirements should be reviewed, queries resolved and the performance criteria required to be met by the technical architecture and related technical security architecture formally agreed.

7 Network Security Design

7.1 Introduction

The network security architecture includes a description of the interfaces between an organization's/community's internal network and the outside world. Reflecting the requirements mentioned in clause 6.4 above and addressing how to protect the organization from the common threats and vulnerabilities as described in part 1.

Guidance on general best practice design is provided in clause 7.2 below, and guidance on the network security architecture aspects related to specific networking technologies to address the requirements of today and the near future is provided in ISO/IEC 27033-4 and onward. Guidance on specific scenarios that are possible for an organization are covered in ISO/IEC 27033-3.

Technical assumptions made during the requirements gathering should be documented, for example:

- only authorized IP communications should be allowed (firewalls normally only support IP communications, and if any other protocols were allowed then it could be difficult to manage them);
- if non-IP protocols are a requirement then they should be dealt with either outside the security architecture or by tunnelling the protocol.

A network security architecture would normally encompass services, such as the following but not limited to these:

- identification and authentication (passwords, tokens, smartcards, public key infrastructure (PKI), RAS/RADIUS/terminal access controller access control system plus (TACACS+), etc.);
- logical access controls (single sign on, role based access control, trusted databases, application controls, firewalls, proxy devices, etc.);
- security audit and accounting (audit logs, audit log analysis facilities, intrusion detection facilities, write once read many (WORM) devices, etc.);
- assured storage clearance/secure deletion (provable 'wipe' facilities);
- security testing (vulnerability scanning, network 'sniffing', penetration testing, etc.);
- secure development environment (separate development and test environments, no compilers, etc.);
- software change control (configuration management software, version control, etc.);
- secure software distribution (digital signing, SSL, transport LAN security (TLS) (RFC2246), short message service (SMS), etc.);
- secure maintenance and availability (good back-up/restore facilities, resilience, clustering, data vaults, diverse communications, etc.);
- transmission security (use of transport encryption, spread spectrum technology, Wireless LANS (WLANs), VPNs/extranets.

The timescale for the development of a network security architecture can vary considerably.

7.2 Best practice design

Common risk areas associated with networking security architectures are design failures due to poor design and/or the lack of appropriate consideration of business continuity planning. Fundamental elements are needed to develop network security architectures that encompass all the identified security controls and business requirements. Most of these elements can be covered by general network security design best practices. ISO/IEC 27033-4 and onward cover design and implementation in detail on some aspects of the network technical security architecture best practices. Additional detailed guidance on best practice implementations can be found in other publications.

The following sections provide general guidance on design best practices to be followed when considering a network security architecture.

7.2.1 Defence in depth

Organizations need to look at security not just from one perspective, but as a pervasive layered approach. Security must be comprehensive across all network layers. Adopting a layered approach is considered to be defence in depth. The components of security are a combination of policy, design, management and technology. Each organization needs to determine its needs and design a defence in depth based upon those needs.

Think of security as layers of defence. Each additional security level builds upon the capabilities of the layer above. Each additional security level provides finer and finer grained security. Figure 2 shows how there is perimeter security, with a more finer grain for infrastructure security, still more finer for the hosts, then applications and finally data. All of the layers are to protect the data. An example of the reasoning for layered security is that if you only have a firewall on the perimeter this does not protect a host from an attacker on the inside of the perimeter; the infrastructure security would be needed for that.

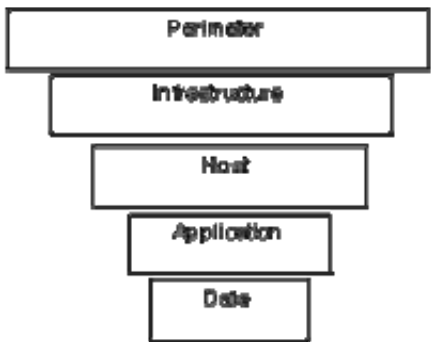

Figure 2. Defence in Depth Approach

Security solutions based on the layered approach are flexible and scalable. The solution is adaptable to the security needs of the organization.

7.2.2 Common network components

For any secure network design there is a combination of common components that can be used. These components are used in a combination that will create a technical network security design. The remainder of clause 7 and ISO/IEC 27033-3 and onward go into technical detail on some of the components listed below. These components will be used in some combination to secure the requirements reflected in clause 6.4. Some of these components may include:

- Segmentation and compartmentalization
- Security Management systems
- Basic Security technologies, such as Identity management, cryptography, etc.
- Network admission control devices
- Threat mitigation techniques, such as Quality of Service, etc
- Perimeter devices
- Firewalls
- Remote-access devices
- Intrusion detection systems/Intrusion prevention systems
- Endpoint protection
- Routers and switches
- Extranet connections

7.2.3 Design resilience

For any system where the availability has to be at a constant state of availability, the resilience of the security network infrastructure configuration has to be considered. There are two approaches to the design –infrastructure can be designed for load sharing or failover. If the requirements merit the use of load sharing then the clustering of devices must be considered as this will allow more than two devices to be included in the configuration. For example the design of security gateways in the infrastructure can be through load sharing (this would include clustering) or failover. Regardless of the approach used, each security gateway may need an additional interface to support the transfer of state information to allow the changeover of the security gateway in the event of a failure.

Servers should be configured within clusters for resilience. For example, there could be three front end web servers which should be configured in a cluster with a single IP address enabling the actual addresses of the servers to be hidden behind the firewalls. Application servers should be similarly clustered for resilience.

With regard to the infrastructure, including wide area connections and the internal LANs:

- the wide area connections should be duplicated and physically alternately routed for resilience, with care taken to ensure that the specification states that physical cables use diverse duct routes;
- LAN communications could include the Ethernet communications between devices, i.e. switches
  - Ethernet subnets that are configured on switches using VLAN configurations, the key design criteria should include:
    - VLANs not configured across different systems/services, or projects;
    - where there is a requirement for VLANs to be configured either side of a firewall, i.e. in different security sub-domains, the VLANs configured on different physical switches;
    - management communications should be segregated from data LANs;

- Where VLANs pass through one sub security domain to another, then the communication path should be via a security gateway.

Where possible, there should be dual power feeds to each equipment cabinet to ensure continuity of the mains electricity supply, and critical devices (such as firewalls, switches, and servers) should be fitted with a minimum of two power supplies. Many major hosting sites will have full building uninterruptible power supply (UPS) systems to ensure the continuity of the electricity supply to equipment. However, experience shows that there can be catastrophic failures of these protected supplies which can damage equipment. Thus, where there are devices such as servers that support critical services there should be an additional UPS device installed and configured with automatic shut down in the event of an electricity failure. A restart plan may also be required for servers after a power failure.

7.2.4 Securing network management

Network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance and provisioning of networked systems.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.

- Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.

- Maintenance is concerned with performing repairs and upgrades - for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.

Malconfiguration of network related components, either liberate or deliberate, impose significant risks, not only regarding availability, but often also regarding integrity and confidentiality.

Therefore controls to address these risks are necessary. Such controls can be categorized in organizational controls and technical controls.

Organizational controls do e.g. include proper entitlement of administrative personal, operational principles such as four eyes principle or appropriate separation of duties as wells as procedures and policies to avoid default or weak passwords.

Technical controls include the use of administration interfaces and tools which provide appropriate authentication and authorisation quality and confidentiality. Technical management is required for a number of networking related components. Security gateways could be managed locally or remotely, but remote management should use tools which ensure strong or two-factor authentication or at least technically avoid default or weak passwords and which provide adequate integrity and confidentiality functions would be used whenever possible. Examples are the use of encrypted VPN tunnels configured with appropriate levels of encryption or SSH terminal emulation. Servers could also be managed locally or remotely. Where the servers support sensitive information then again the remote management must use tools which ensure strong or two-factor authentication or at least technically avoid default or weak passwords and which provide adequate integrity and confidentiality functions would be used whenever possible.

Infrastructure components, such as switches and routers, could be managed locally from the console port, remotely from a central management station, using terminal emulation program to work online on a remote computer or from distributed management system. However, it is recognized that these protocols are not secure unless they can be configured with a method that can fully encrypt the connection. One example of secure remote connection which can fully encrypted and includes a secure file transfer facility is SSH. Further, access to infrastructure components should be controlled by an authentication server.

Networks that are outsourced to a provider normally have their own management systems. However, they should be managed from a central management station using secure remote management methods. Remote management

methods should include encryption and authentication using public key cryptography. Examples of secured methods that could be used are, Telnet and TFTP via a VPN tunnel, or SSH, which is controlled by an authentication server.

Many organizations use simple network management protocol (SNMP) management traps to directly monitor such networks. There are significant risks with SNMP version 1 and version 2 that have weak or no security. Therefore if an organization decides to use SNMP the use should be using version 3 with full security controls.

7.2.5 Authentication & authorisation

Several methods can be used for authentication and identity. These techniques include (but are not limited to): password, onetime passwords, biometric techniques, smart cards and certificates. Password based authentication should use strong passwords conform to current best practices (e.g. at least 8 characters, including alphanumeric and special characters). Further a special interest should be put on the frequency of change of passwords (e.g. at least every 6 months). Password authentication alone may not be sufficient. Based on risk assessment it may be necessary to combine password authentication with other authentication and authorization process such as certificates.

Once authenticated, authorisation mechanisms control user access to appropriate system resources. Authorization can be categorized according to the granularity of access that is required. Fine-grained authorization refers generally to a system where access is controlled in very fine increments.

Authorisation is often “role based” whereby access to the system resources is based on a person’s assigned role in the organization.

7.2.6 Security auditing, accounting, and monitoring

An audit server should be configured with all security gateway systems, located on a DMZ that is secure from both the outside and the inside networks as well as any other security relevant devices located inside or outside the DMZ. The audit server should not be part of the internal network domain and should only be directly accessible by an assigned security officer for the security gateway/firewall system. However, write access will be needed to allow audit logs to be uploaded by a secure protocol (for example Secure Copy (SCP)) from infrastructure components, servers and firewalls. All firewall and associated audit logs should be directed to this audit server for later examination by security staff, with audit analysis software provided to allow review and manipulation of the audit log files.

Security information management includes the collection and standardization of information collected so that decisions can be made based on that information. Information collected may include syslogs, SNMP information, IDS/IPS alerts, and flow information.

7.2.7 System Hardening

All operating systems should be hardened relative to the use of the server. There are many existing best practices for various operating systems that should be referenced based on operating system that is being used. Some of the best practices that should be used for any operating system include:

- removal of un-needed/un-used software
- removal of unnecessary accounts
- changes to any default accounts
- closure of all unused ports
- installation of latest patches

7.3 Use of "Scenario" and "Technology" guidance

A network environment under review can often be characterized by particular network scenario(s) and 'technology' topic(s) that are associated with well defined risks, design considerations and control issues. Such information is very useful when reviewing technical security architecture/design options and selecting and documenting the preferred technical security architecture/design and related security controls.

ISO/IEC 27033 Part 3 references such scenarios, and for each scenario provides detailed guidance on the security risks and the security design techniques and controls required to mitigate the risks.

7.4 Use of models/frameworks

Historically a component of security system engineering includes selection, use or development of a security model or framework.

The security model is used to describe the entities (subjects governed by an organization's security policy) and define the access rules necessary to instantiate said policy. The security model typically focuses on either confidentiality via access controls or information integrity, where some are formally defined and others informally defined.

Security frameworks typically provide an organization a way to form a general outline of how to form a secure system. An example of a framework would be ITU-T X.805. This overarching framework for the ITU-T X.800 series of recommendations to fit into to provide end-to-end network security. To this end, X.805 defines the concept of security dimensions that are containers for tools, technologies, standards, regulations, procedures, etc. that span either aspects of security. X.805 recognizes that redundant security mechanisms are avoided by identifying security capabilities in one layer that protect another layer, (Layer here is used in the context of X.805) thus reducing the overall cost of a security solution. X.805 is a generic security framework and as such does not provide a specification for any particular information system or component. Rather it specifies security principles and target security capabilities facilitating end-to-end network security. An example of how ITU-T X.805 can be applied in support of ISO/IEC 27001 controls can be found in Annex C.

7.4.1 An Example Reference Architecture

The Reference Architecture was created to address the global security challenges of Service Providers, enterprise, and consumers and is applicable to wireless, optical and wire-line voice, data and converged networks. In context of this section the work "reference" in conjuncture with the worked "architecture" is used to convey that the specification presents an example of high-level security architecture that could serve as a base for designing more detailed security solutions for various networks. This Reference Architecture addresses security concerns for the management, control, and use of network infrastructure, services, and applications. The Reference Architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to predict, detect, and correct security vulnerabilities.

The Reference Architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The Reference Architecture addresses the network security needs covering the following essential questions:

1. What kind of information needs to be protected
2. What are the security risks, and what kind of protection is needed to manage these risks?
3. what are the distinct types of network activities that need to be protected?
4. What are the distinct types of network equipment and facility groupings that need to be protected?

A risk analysis should be conducted to prioritize the protection requirements and help to determine the appropriate security measures for security architecture.

The principles described by a multifaceted Reference Architecture can be applied to a wide variety of networks independent of the network's technology or location in the protocol stack.

The reference architecture can be applied to all aspects and phases of a Security program. A security program consists of policies and procedures in addition to technology, and progresses through three phases over the course of its lifetime: (1) the definition and planning phase, (2) the implementation phase, and (3) the monitoring phase and (4) the maintenance phase. The reference architecture along with guidelines of ISO/IEC-13335 can be applied to security policies and procedures, as well as technology, across all phases of a security program.

Based on business requirements, the network architecture, policy definitions, incident response and recovery plans are determined. In this process the reference architecture can guide the development of comprehensive security policy definitions, incident response and recovery plans, and technology architectures by taking into account each Security Dimension at each Security Layer and plane during the definition and planning phase. The reference Architecture can also be used as the basis for a security assessment that would examine how the implementation of the Security Program addresses the security dimensions, layers and planes as policies and procedures are rolled out and technology is deployed. Once a security program has been deployed it must be maintained in order to keep current in the ever-changing security environment. The Reference architecture can assist in the management of the security policies and procedures, incident response and recovery plans, and technology architectures by ensuring that modifications to the security program address each security dimension at each security layer and plane.

7.5 Product selection

Product selection should not be undertaken in isolation, but conducted as an iterative process associated with the design of the network security architecture.

Some examples of what product selection should be based on include:

- technical suitability and merit of the product;
- performance;
- protocol support;
- resilience;
- compatibility;
- extensibility;
- network management facilities;
- audit capability;
- compliance, and approved, to recognized standards;
- technical documentation;
- maintenance;
- remote diagnostic facilities;
- logical security;

- vendor ‘characteristics’ (capability, track record, commitment to quality, market position, size, overall competence including for the products under consideration, organizational/financial stability, references, and training facilities);
- timescales for delivery;
- costs.

7.6 Network technical security architecture and related documentation

The network security architecture document is one of the critical technical security document and, as stated earlier, should be compatible with the related security risk assessment and risk management review results, organization/community networking and information security policies, and other security policies as relevant. As with any critical documentation these documents should be kept under change control. An example template is given in Annex B.1. It should reference the related technical architecture documentation and other technical security documents. Key related documents include:

- the service access (security) requirements document for each security gateway/firewall ‘system’ (that include the firewall rule base(s) – see Annex B.2 for an example template);
- audit log analysis software requirements documentation;
- product analysis reports.

7.7 Test plans and conducting testing

A security testing strategy document should be produced that describes the approach to be taken with testing to prove the networking technical security architecture. It should concentrate on how the key technical security controls should be tested to verify that the requirements defined are met, and that policies are implemented as designed. To verify these viewpoints, system test and checklist-based checking are conducted.

The testing strategy document should include areas such as:

– identification and authentication mechanisms

– resilience of design

– authorisation mechanisms

– implementation of policy controls

– verification of hardened operating systems

– verification of audit log solution

The testing strategy should also include unit and usability testing to ensure suitability of design.

Before conducting system test, Testing plan should be prepared. The testing plan should include testing-data with testing-scenarios for its evidence. The testing plan should also include appropriate testing term. The testing-data should be carefully prepared to be able to examine the functionality of the technical security controls.

7.8 Formal network design and implementation sign-off

When testing has been completed successfully, the network security architecture should be formally signed off by the design team, operations management, and the appropriate level of management involved in the project.

Annexes

ANNEX A
(informative)
Cross-references Between ISO/IEC 27001/27002 Network Security Related Controls and ISO/IEC 27033-2 Clauses

A.1 By ISO/IEC 27001/27002 Clause

ISO/IEC 27001/27002 Clause		ISO/IEC 27033-2 Clause
10.4.1 Controls against malicious code	Detection, prevention and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.	7.2.7 System Hardening
10.6.1- Network Controls	Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.	See below against ISO/IEC 27001/27002 clauses 10.6.1 IG a) to e).
10.6.1 IG a)	Operational responsibility for networks should be separated from computer operations where appropriate.	7.2.4 Securing network management
10.6.1 IG d)	Appropriate logging and monitoring should be applied to enable recording of security relevant actions.	7.2.6 Security auditing, accounting and monitoring
10.6.1 IG e)	Management activities should be closely coordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.	7.2.4 Securing network management
10.6.2 – Security of Network Services	Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.	6.4 Network requirements of the organization/community 7.7 Network technical security architecture and related documentation

ISO/IEC 27001/27002 Clause		ISO/IEC 27033-2 Clause
10.8.1 Information exchange policies and procedures	Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.	7.7 Network technical security architecture and related documentation
11.4.1 Policy on use of network services	Users should only be provided with access to the services that they have been specifically authorized to use.	7.2.5 Authentication and authorisation
11.4.2 User authentication for external connections	Appropriate authentication methods should be used to control access by remote users.	7.2.5 Authentication and authorisation

Annex B
(informative)
Example Documentation Templates

B.1 An example network security architecture document template

B.1.1 Introduction

Including sections such as:

- purpose/objectives/scope,
- assumptions, both technical and otherwise,
- document status,
- document structure.

B.1.2 Business related requirements

Including sections such as:

- introduction,
- context,
- networking and other IT services.

B.1.3 Technical architecture

Including sections such as:

- introduction,
- technical overview,
  - summary,
  - major domain 1,
  - major domain 2,
  - major domain 3,
  - etc.,
  - servers,
  - workstations,
  - logging,

  - management,
  - authentication and access control,
  - service coverage and resilience,
- system locations,
- system components,
- interconnections,
- component 1,
  - overview,
  - configuration,
  - logging,
  - management,
- component 2,
  - overview,
  - configuration,
  - logging,
  - management,
- component 3,
  - overview,
  - configuration,
  - logging,
  - management,
- component ‘x’ etc.,
- server management,
  - introduction,
  - monitoring of services,
  - extended system administration (XSA),
  - enterprise security manager (ESM),
  - any other manager,

- firewalls,
  - introduction,
  - overview,
  - firewalls,
  - firewall configuration back-up,
  - design criteria and configuration,
  - rule bases,
- firewall management,
  - configuration,
  - firewall alerts,
  - remote access,
- logging,
- back-up system,
  - introduction,
  - firewalls,
  - servers,
  - applications,
- network communications,
  - local area networking, e.g. VLANs, WLANs,
  - routers,
  - switches,
  - IP addressing,
- management responsibilities,
  - servers,
  - firewalls,
  - infrastructure,
  - application management.

B.1.4 Network services

Including sections such as:

- introduction,
- services at location x,
- services at location y,
- etc.

There should be a list of all network services by location, including such as:

- KiloStream services,
- MegaStream services,
- frame relay services,
- ATM,
- IP Clear/ MPLS,
- broadband services,
- Wi-Fi/WiMax,
- LAN connect services,
- GSM,
- primary rate ISDN (up to 30 of 64 Kbps channels delivered over a MegaStream),
- ISDN basic rate interface (BRI), (2 × 64 Kbps channels),
- analogue direct exchange lines (DELs),
- intranet/extranet services,
- ISPs,

with all lines and services included.

If the list is extensive then it should be included in an annex with references to it from the main body of the document.

B.1.5 Hardware/physical layout

Including sections such as:

- introduction,
- location.

There should be a list of all hardware, with floor plans and cabinet layouts – by location, including coverage of, for example, servers, routers, switches, firewalls and other communications equipment. As all hardware should be labelled, the labelling plan should be included or at least referenced.

Table B.1 shows an example hardware list table. There should be a table for each type of hardware – the example table covers server components.

Table B.1 — Example Hardware List Table

Server component	Hardware	Software	Comment
Name and manufacturer of server	Part number	Software and version	Specific comments as required, such as. scaled vertically, or clustered.

B.1.6 Software

Including sections such as:

- introduction,
- list of software,
  - software at location x,
  - software at location y,
  - etc.The list of all software, including version numbers, should include such as:
- Novell,
- Windows software,
- firewalls,
- RAS/RADIUS,
- router software,
- switch software,

- proxy,
- audit management,
- mail servers,
- SMTP mail relay,
- content management,
- Java/ActiveX screening,
- web servers,
- FTP servers,
- domain controllers,
- back-up software,
- other software.

The list should be included in an annex with references to it from the main body of the document.

B.1.7 Performance

Expected performance details should be included, including for ‘subsystems’ such as:

- desktop,
- servers,
- LAN,
- WAN,
- gateways,
- external services.

B.1.8 Known issues

Details of known issues, including regarding areas of non-compliance, should be included under such headings as technical, physical and environmental, including sections such as:

- introduction,
- areas of non-compliance.

B.1.9 References

References should be included to all related documentation, including:

- security risk assessment and management review results,
- networking security policy,

- information security policy,
- other security policies as relevant,
- the technical architecture documentation,
- the service access (security) requirements documents for each firewall system (that include the firewall rule base(s)),
- (audit) log analysis software requirements documentation,
- product analysis reports,
- generic testing strategies and plans,
- the information security incident management scheme,
- SecOPs,
- conditions for secure connection for third parties,
- user guidelines for third party users.

B.1.10 Appendices

Include details of such as:

- hardware configuration,
- server/console configurations,
- firewall configurations,
- router configurations,
- software configuration,
- firewall configurations,
- router configurations,
- database configuration,
- IP addressing plan,
- SNMP configuration,
- system traps,
- application traps,
- standards.

B.1.11 Glossary

B.2 An example template for a service access (security) requirements document

NOTE. One document should be produced for each firewall system.

B.2.1 Introduction

Including sections on such as:

- background/scope/objectives,
- firewall system name,
- firewall location,
- firewall role,
- name of person/group responsible for firewall operation,
- record of revisions to document content,
- references.

B.2.2 Firewall configuration

Including sections on such as:

- introduction,
- identity of links via firewall system,
- firewall architecture overview,
- firewall system details:
  - hardware,
  - software,
  - firewall architecture,
  - firewall service,
  - firewall management,
  - inner router,
  - outer router,
  - DMZ hub,
  - anti-malicious code server,
  - SMTP mail,
  - web pages,
  - SMTP mail server,
  - (audit) logging server,
  - UPS,
  - other components,
  - other controls required,
- description of links to, and of, other systems,
- information types involves and their sensitivity,

- user types and numbers etc.

B.2.3 Security risks

Including sections on such as:

- introduction,
- potential adverse business impacts (sometimes known as asset valuations),
- threat assessments,
- vulnerability assessments,
- risk assessments,

in the context of the firewall usage.

B.2.4 Security management

Including sections on the responsibilities of such as:

- security officer/group,
- network personnel,
- firewall support personnel,
- network management,
- other IT management,
- users.

B.2.5 Security administration

Including sections on such as:

- SecOPs,
- security compliance reviews,
- availability,
- maintenance,
- configuration control,
- capacity management,
- problem management,
- service level management,
- expiry of this document.

B.2.6 Authentication and access control

Including sections on such as:

- introduction,
- logical access controls for such as firewall administrators, internal and remote users,
- external access control measures such as network to firewall rule base, secure platform and application proxy servers,
- network level protection.

B.2.7 (Audit) Logging

Including sections on such as log:

- information to be recorded,
- analysis to be conducted and with what tools,
- security.

B.2.8 Information Security incident management

Including sections on such as log related:

- introduction,
- incident reporting,
- incident handling,
- etc.

B.2.9 Physical security

Including sections on the responsibilities of such as control of access to the:

- firewall system,
- cabling.

B.2.10 Personnel security

Including sections applicable to firewall related personnel on such as:

- recruitment screening/checking,
- security awareness and training.

B.2.11 Appendices

Including on such as service and protocol details:

- access outwards and inwards,

- remote management,
- firewall management,
- DMZ server management,
- any other relevant service and protocol details.

B.2.12 Glossary

Annex C
(informative)
ITU-T X.805 Framework and ISO/IEC 27001 Control Mapping

C.1 ITU-T X.805 and ISO 27001

ITU-T X.805 can also be used for technical augmentation of controls in the ISO 27001 standard. In particular, as depicted in Figure E-1, ITU-T X.805 can augment four controls in ISO 27001: security policy, asset management, access control, and information security incident management. The specific X.805 layer, planes, dimensions applicable to each of these controls is depicted in the Figure. For example, for asset management, the infrastructure and service layers, and the control, and management planes are the most applicable, with the access control and availability dimensions being the most prominent concerns.

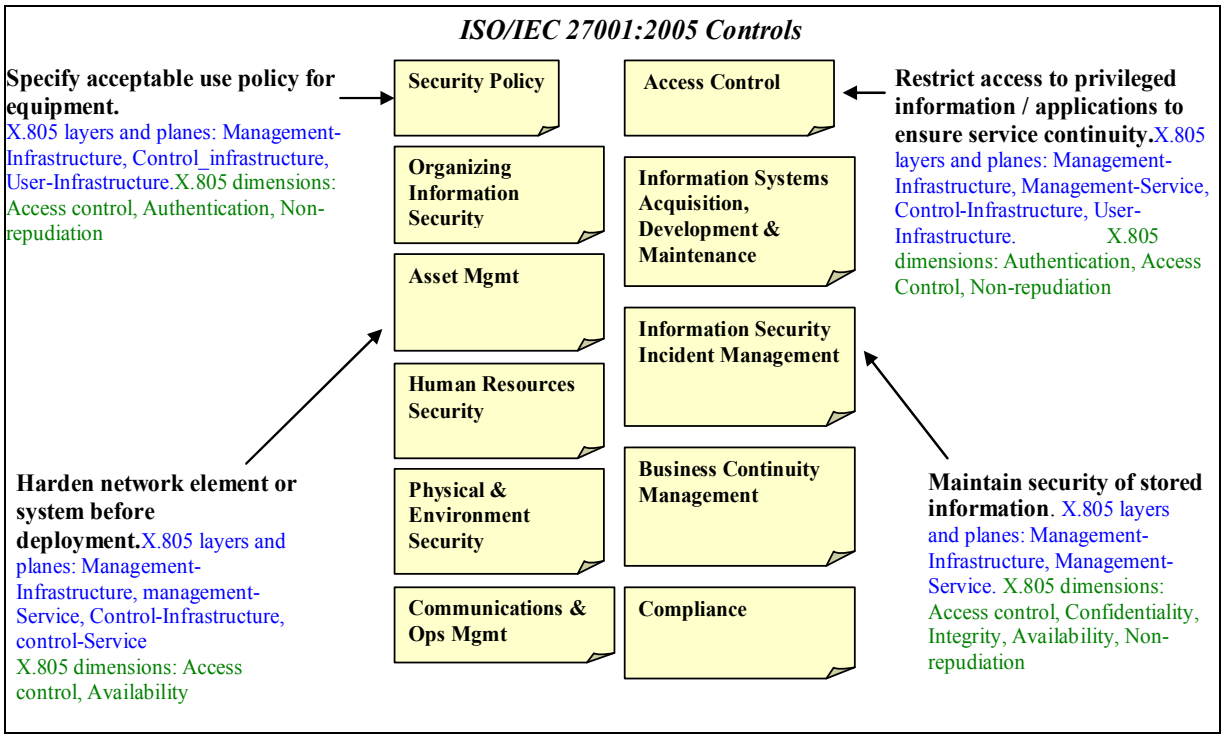

Figure C-1 : ITU-T X.805 Augmentation for ISO 27001 Controls

As an example, the augmentation can be used to systematically assess and design the security for an enterprise data center that stores its employee information, specifically personal information that should be restricted to authorized users only. The employee information is accessed by several support organizations employed by the enterprise, one of which is the help desk; in addition, the data center and systems contained therein are maintained by the corporate IT organization. As seen in Figure E-2, the Help Desk accesses the employee information for handling complaints, supporting orders for new IT services, resolving problems employees are having with IT services (e.g., remote access), etc. In addition, the Corporate IT organization accesses the employee information as part of its maintenance activities of file system maintenance, system updates, patch management etc..

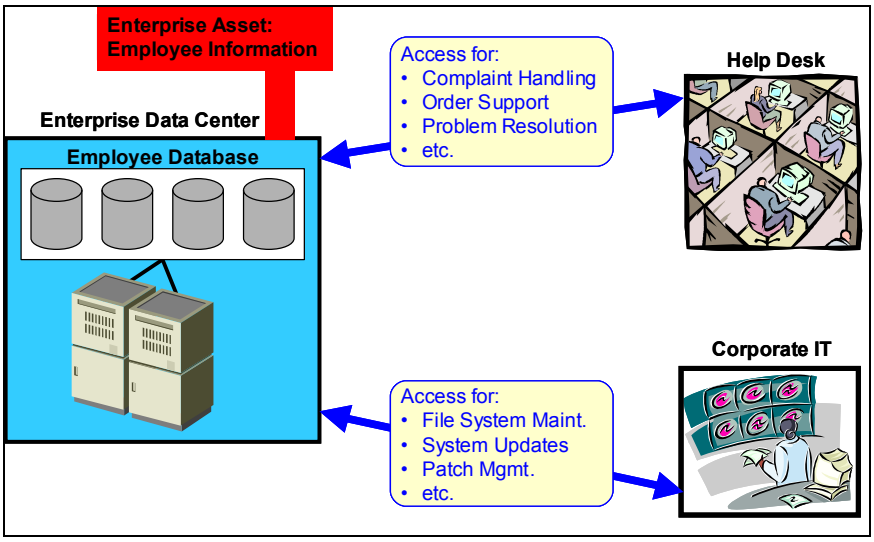

Figure C-2: Access Scenario for Enterprise Asset

An ITU-T X.805 threat/vulnerability analysis reveals that members of the corporate IT organization can view and modify the employee information thereby making it vulnerable to disclosure and corruption in the infrastructure layer (see E-3). In addition, as part of performing problem resolution, employee information is transmitted in the clear between the data center and the help desk; thereby making it vulnerable to disclosure, corruption and interception in the services layer. Thus, controls must be identified and selected to protect employee information against threats and vulnerabilities in the management plane of its infrastructure and services layers. It should be noted that a step-by-step ITU-T X.805 analysis is not presented in this paper. Only the result of such an analysis is assumed for brevity.

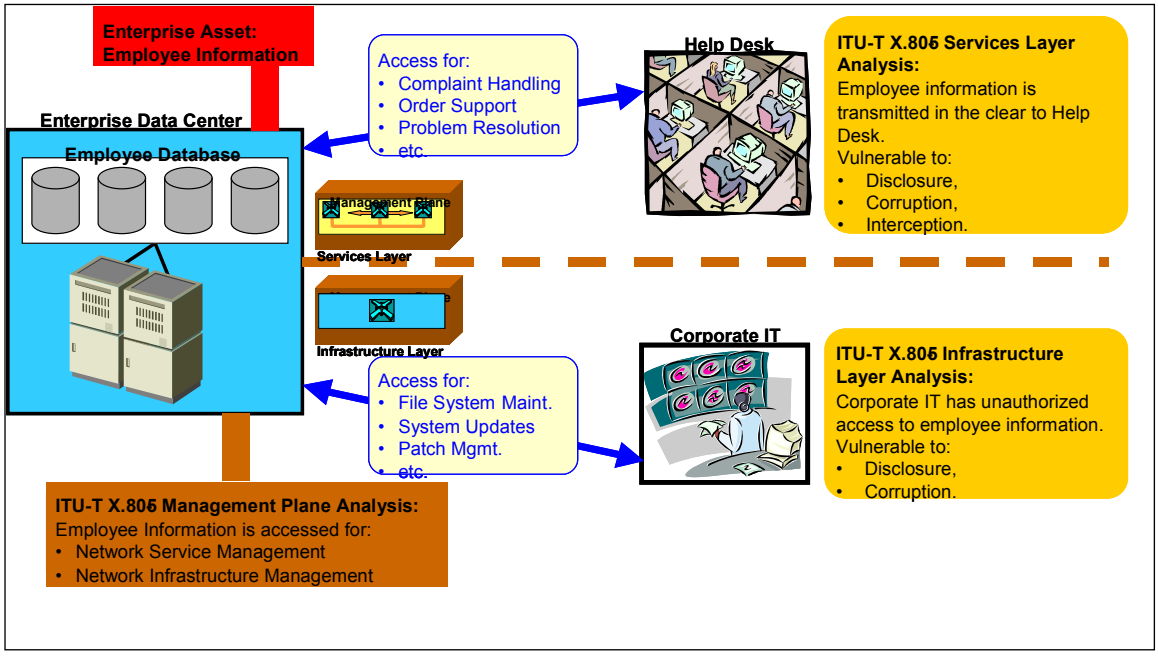

Figure C-3: ITU-T X.805 Threat and Vulnerability Analysis Results for Enterprise Asset

ISO 27001 Control A.10.9.2 is identified and selected as being required to protect the management of employee information in the services and infrastructure layers due to the vulnerabilities and threats identified there by the ITU-T X.805 analysis (E-4). ISO 27001 Control A.10.9.2 states that information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

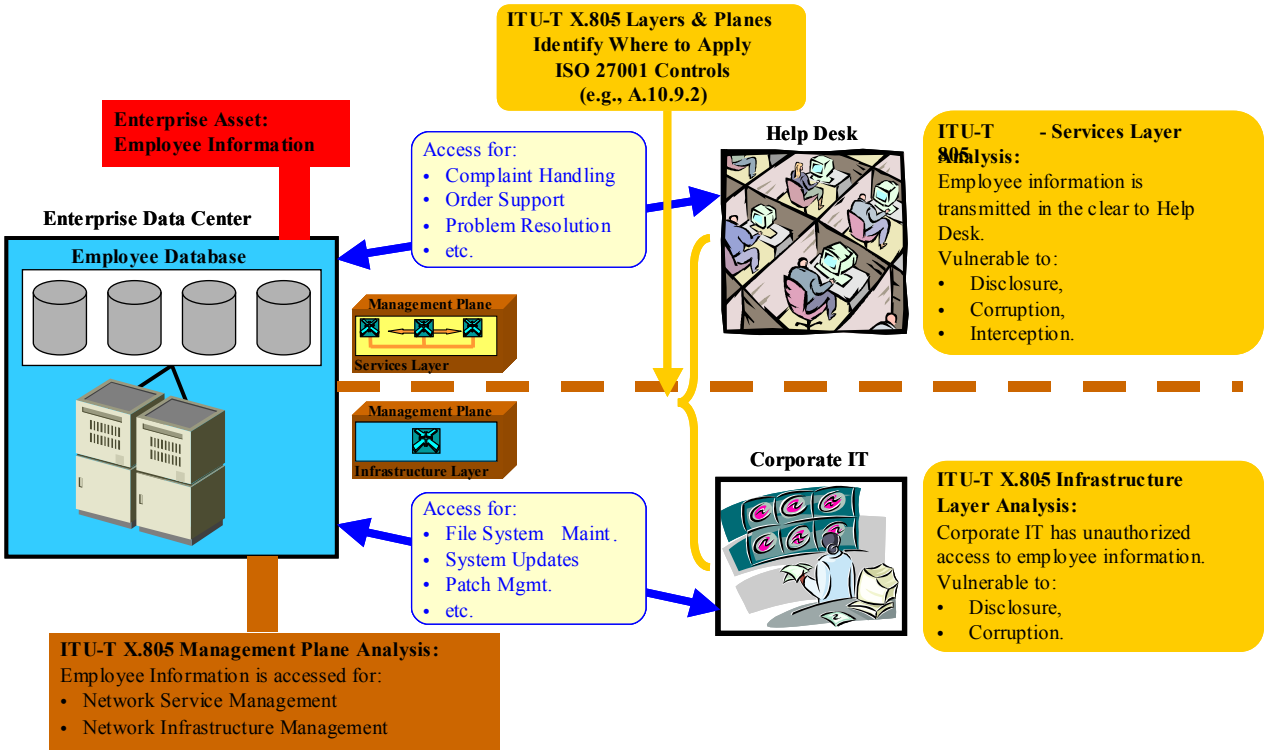

Figure C-4: ISO 27001 Controls

The ITU-T X.805 dimensions provide implementation and operation details for Control A.10.9.2 in the services and infrastructure layers for the employee information asset. In the services layer, Communications Security dimension provides for the use of VPNs to prevent misrouting. The Data Integrity dimension provides for the use of IPSec AH to prevent incomplete transmission, unauthorized message alteration and duplication as well as prevent message replay. The Data Confidentiality dimension provides for the use of IPSec ESP to prevent unauthorized disclosure. In the infrastructure layer, the Data Integrity dimension provides for the use of file checksums to prevent unauthorized alteration, the Data Confidentiality dimension provides for file encryption to prevent unauthorized disclosure, and the Access Control dimension provides for the use of file system access control lists (ACLs) to prevent unauthorized duplication. Figure C-5 depicts how the ITU-T X.805 dimensions provide for the implementation and operation of control A.10.9.2 to protect the employee information asset.

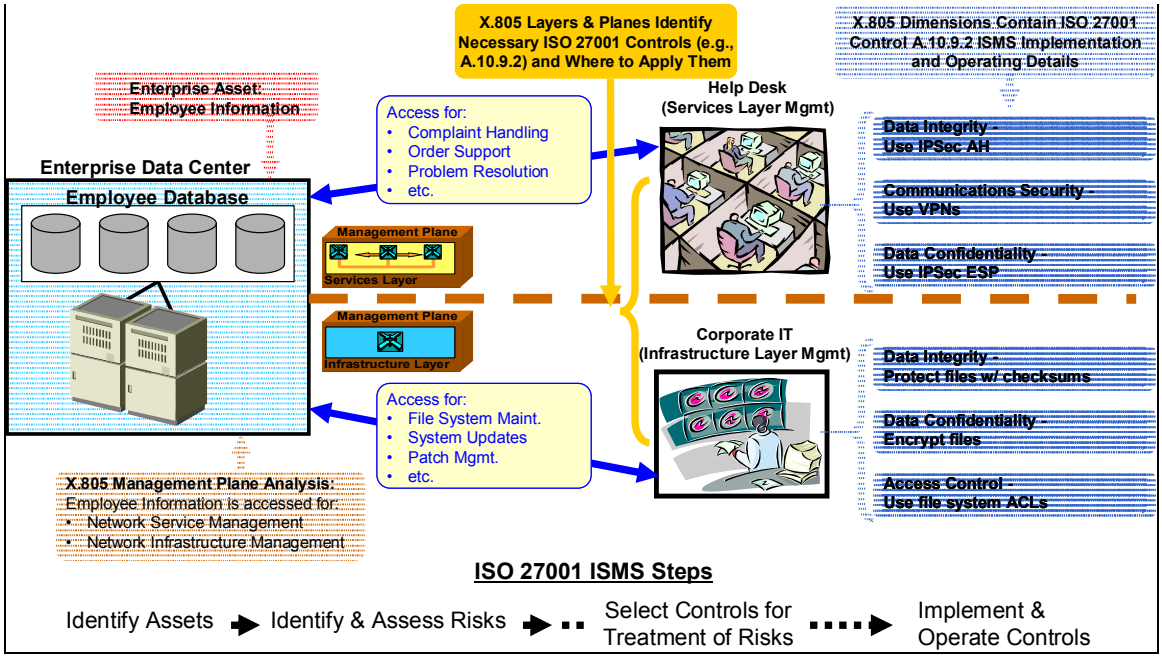

Figure C-5: ITU-T X.805 for ISO 27001 Implementation

ISO/IEC JTC 1/SC 27 **N7923**

ISO/IEC JTC 1/SC 27/WG 4 **N47923**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	text for Working Draft
TITLE:	**Text for ISO/IEC 1st WD 27033-4 (revision of ISO/IEC 18028-3:2005) Information technology -- Security techniques - Network security - Part 4: Securing communications between networks using security gateways – Threats, design techniques and control issues**
SOURCE:	Project Editor (Heung Youl YOUM)
DATE:	2010-1-4
PROJECT:	27033-4 (revision of 18028-3)
STATUS:	In accordance with resolution 2 (contained in SC 27 N7908) of the 7th SC 27/WG 4 meeting in Redmond on 2nd - 6th November 2009 this document is being circulated to the National Bodies and liaison organizations for **STUDY AND COMMENT**. The National Bodies and liaison organizations of SC 27 are requested to send their comments / contributions on the hereby attached document directly to the SC 27 Secretariat as soon as possible but no later than **2010-04-01.**
PLEASE NOTE:	For comments please use THE SC 27 TEMPLATE separately attached to this document.
ACTION ID:	**COM**
DUE DATE:	**2010-04-01**
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice Chair E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners Heung Youl YOUM, Project Editor
MEDIUM:	Livelink-server
NO. OF PAGES:	1 + 17

Secretariat ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut für Normung e.V., Burggrafenstraße 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 **N7923**

Date: 2010-01-4

ISO/IEC WD 27033-4

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues

Technologies del'information — Techniques de sécurité — Partie 4: Sécurité de réseaux TI

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (20) Preparatory
Document language: E

D:\HOD_South_Africa\Eigene Dateien\PROJECT_admin\27033\27033-4_(18028-3_revision_Oct2008)\02_01_1stWD_27033-4_(18028-3_revision)\SC27N7923_1stWD_27033-4_20100106\SC27N7923_1stWD_27033-4_20100104.doc STD Version 2.3

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This 1st edition of ISO/IEC 27033-4 cancels and replaces the first edition of ISO/IEC 18028-3:2005 which has been technically revised.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Overview and concepts (revision of ISO/IEC 18028-1:2006),*

— *Part 2: Guidelines for the design and implementation of network security (revision of ISO/IEC 18028-2:2006),*

— *Part 3: Reference network scenarios – Threats, design techniques and control Issues,*

— *Part 4: Securing communications between networks using security gateways – Threats, design techniques and control Issues (revision of ISO/IEC 18028-3:2005),*

— *Part 5: Securing virtual private networks – Threats, design techniques and control issues (revision of ISO/IEC 18028-5),*

— *Part 6: IP convergence,*

— *Part 7: Wireless*

(Note that there may be other Parts in the future. Examples of possible topics to be covered by future Parts include local area networks, wide area networks, broadband networks, web hosting, Internet email, and routed access to third party organizations. The main clauses of all such Parts should be Risks, Design Techniques and Control Issues.) Part 4: Securing communications between networks using security gateways – Threats, design techniques and control issues

Introduction

In today's world, the majority of both commercial and government organizations have their information systems connected by networks, with the network connections being one or more of the following:

• within the organization,

• between different organizations,

• between the organization and the general public.

Further, with the rapid developments in publicly available network technology (in particular with the Internet) offering significant business opportunities, organizations are increasingly conducting electronic business on a global scale and providing online public services. The opportunities include the provision of lower cost data communications, using the Internet simply as a global connection medium, through to more sophisticated services provided by Internet Service Providers (ISPs). This can mean the use of relatively low cost local attachment points at each end of a circuit to full scale online electronic trading and service delivery systems, using web-based applications and services. Further, the new technology (including the integration of data, voice and video) increases the opportunities for remote working (also known as 'teleworking' or 'telecommuting') that enable personnel to operate away from their home work base for significant periods of time. They are able to keep in contact through the use of remote facilities to access organization and community networks and related business support information and services.
However, whilst this environment does facilitate significant business benefits, there are new security threats to be managed. With organizations relying heavily on the use of information and associated networks to conduct their business, the loss of confidentiality, integrity, and availability of information and services could have significant adverse impacts on business operations. Thus, there is a major requirement to properly protect networks and their related information systems and information. *In other words, implementing and maintaining adequate network security is absolutely critical to the success of any organization's business operations.*
In this context, the telecommunications and information technology industries are seeking cost-effective comprehensive security solutions, aimed at protecting networks against malicious attacks and inadvertent incorrect actions, and meeting the business requirements for confidentiality, integrity, and availability of information and services. Securing a network is also essential for maintaining the accuracy of billing or usage information as appropriate. Security capabilities in products are crucial to overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall security solution.
The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements. Its main objectives are as follows:

- in ISO/IEC 27033-1, *Guidelines for Network security,* to define and describe the concepts associated with, and provide management guidance on, network security. This includes the provision of an overview of network security and related definitions, and guidance on how to identify and analyze network security threats and then define network security requirements. It also introduces how to achieve good quality technical security architectures, and the threat, design and control aspects associated with typical network scenarios and network 'technology' areas (which are dealt with in detail in subsequent parts of ISO/IEC 27033). In effect it also provides an overview of the ISO/IEC 27033 series and a 'road map' to all other parts,

- in ISO/IEC 27033-2, *Guidelines for the design and implementation of network security,* to define how organizations should achieve quality network technical security architectures, designs and implementations that will ensure network security appropriate to their business environments, using a

consistent approach to the planning, design and implementation of network security, as relevant aided by the use of models/frameworks. (In this context, a model/framework is used to outline a representation or description showing the structure and high level workings of a type of technical security architecture/design.),

- in ISO/IEC 27033-3, *Reference network scenarios – Threats, design techniques and control issues*, to define the specific threats, design techniques and control issues associated with typical network scenarios,

- in ISO/IEC 27033-4, *Securing communications between networks using security gateways – Threats, design techniques and control issues*, to define the specific threats, design techniques and control issues for securing information flows between networks using security gateways,

- in ISO/IEC 27033-5, *Securing virtual private networks – Threats, design techniques and control issues,* to define the specific threats, design techniques and control issues for securing connections that are established using virtual private networks (VPNs),

- in ISO/IEC 27033-6, *IP convergence* - to define the specific threats, design techniques and control issues for securing IP convergence networks, i.e. those with the convergence of data, voice and video,

- in ISO/IEC 27033-7, *Wireless* – to define the specific threats, design techniques and control issues for securing wireless and radio networks.

(As noted in the Foreword, there may be other Parts in the future*,* to define the specific threats, design techniques and control issues for 'technology' topics (other than those covered by Parts 4 to 7).)
It is emphasized that the ISOI/IEC 27033 series provides further detailed implementation guidance on the network security controls that are described at a basic standardized level in ISO/IEC 27002.

ISO/IEC 27033-1 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. It is also relevant to anyone involved in the planning, design and implementation of the architectural aspects of network security.

ISO/IEC 27033-2 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

ISO/IEC 27033-3 is relevant to all personnel who are involved in the planning, design and implementation of the architectural aspects of network security (for example network architects and designers, network managers, and network security officers).

ISO/IEC 27033-4 is relevant to all personnel who are involved in the detailed planning, design and implementation of security gateways (for example network architects and designers, network managers, and network security officers).

ISO/IEC 27033-5 is relevant to all personnel who are involved in the detailed planning, design and implementation of VPN security (for example network architects and designers, network managers, and network security officers).

ISO/IEC 27033-6 is relevant to all personnel who are involved in the detailed planning, design and implementation of security for IP convergence networks (for example network architects and designers, network managers, and network security officers).

ISO/IEC 27033-7 is relevant to all personnel who are involved in the detailed planning, design and implementation of security for wireless and radio networks (for example network architects and designers, network managers, and network security officers).

(If there are other Parts in the future, these will be relevant to all personnel who are involved in the detailed planning, design and implementation of the network aspects covered by those parts (for example network architects and designers, network managers, and network security officers).)
It should be noted that this standard is not a reference or normative document for regulatory and legislative security requirements. Although the standard emphasizes the importance of these influences, it cannot state them specifically, since it is dependent on the country, the type of business, etc.
Unless otherwise stated throughout this document the guidance referenced is applicable to current and/or planned networks, but will only be referenced as “networks” or “the network”.

Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways — Threats, design techniques and control issues

1 Scope

ISO/IEC 27033-4 provides an overview of securing communications between networks using security gateways (e.g., firewall, Intrusion Protection System, application firewall) in order to protect the organization's internal network against malicious attacks and manage and control the traffic flowing across it in accordance with a documented information security policy of the security gateways. It defines specific security threats associated with security gateways, provides security controls and specific design techniques and control issues for security gateways.

ISO/IEC 27033-4 also:

• provides guidance on how to identify and analyze network security threats and the definition of network security requirements based on that analysis for security gateways,

• introduces how to achieve good quality network technical security architectures, and the threat, design and control aspects associated with typical network scenarios and network 'technology' areas using security gateway, and

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

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 27033-1, *Information technology -- Security techniques -- Network security – Part 1: Overview and concepts* (ISO/IEC 18028-1:2006)

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), ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, 27033-1 and the following apply.

4 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 27033-1 and the following apply.

5 Structure

The structure of ISO/IEC 27033-4 comprises:

- an overview of security gateway(see clause 6),

  - security threats associated with security gateway(see clause 7),

  - security requirements based on that analysis for security gateways(see clause 8),

  - security controls associated with typical network scenarios and network 'technology' areas using security gateway(see clause 9),

  - various design techniques for security gateways(see clause 10).

6 Overview

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.

7 Security threats

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 threat productivity losses, liability exposure, and misallocation of bandwidth due to non-productive Web surfing. Thus the key security threats to be addressed include those associated with:

− the connections to the outside world becoming unavailable,

− data becoming corrupted,

− valuable company assets being subject to unauthorized disclosure,

− data placed on websites or otherwise transmitted without proper authority incurring legal penalties, e.g. insider trading.

8 Security requirements

Security gateways control access to a network (OSI model layer 2, 3, and 4), or to an application (OSI model layers 5 to 7).

Examples include firewalls being used to protect:

• an internal organizational network from the Internet,

• two internal organizational networks from each other,

• an internal organizational network from an external organisation's network, or

• an internal organizational network from external networks including telephone network through the application-level security gateway.

Security gateways are used to fulfill the following security requirements:

• separate logical networks,

• provide restricting and analysing functions on the information which passes between the logical networks,

• provide means of controlling access to and from the organization´s network, by inspection of connections or by proxy operations on selected applications,

• 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 and auditing,

• provide network address translation to hide internal networks,

• provide port mapping (including dynamic port opening), and application-level attack detection and protection (including content filtering).

9 Security controls

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

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

It is emphasized that the connection to a network should only take place after it is checked that the selected security gateway suits the requirements of the organization and/or community, and that all threats 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 threats, 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.

Note that whilst the network security aspects of personal firewalls, a special type of firewall, are not discussed in 27033-4, they should also be considered.

Unlike most central sites which are protected by dedicated firewalls, remote systems may not warrant the expense and specialist skills to support these devices. Instead, a personal firewall can be used, which controls the flow of communications into (and sometimes out of) the remote computer. The administration of the rules (policies) of the firewall can be carried out remotely by personnel at the central site, relieving the remote system user of the requirement of technical understanding. However if this is not possible, care should be

taken to ensure effective configuration, especially if those at the remote site are not IT literate. Some personal firewalls can also restrict the ability to transmit over the network to authorized programs (or even libraries), restricting the ability of malware to spread.

9.1 Packet filtering

9.1.1 Description of packet filtering

Packet filtering means that network traffic is blocked or passed by comparing the information found in the header of each incoming or outgoing packet against a table of access control rules. The filtering device looks at the header of each packet individually as it enters and compares the IP address and port of the source and destination against its rule base. If the address and port information are permitted, the packet proceeds

through the firewall directly to its destination. If a packet fails this test, it is dropped.

The IP packets can be checked selectively as to whether the data flow between two hosts or networks should be allowed or not. Criteria upon which the decision to allow or deny this data flow is taken can include:

- IP source address;
- IP destination address;
- Protocol (e.g., TCP, UDP, ICMP);
- Source port;
- Destination port;
- Direction of the communication (incoming, outgoing).

Packet filtering gateways are fast because they operate at the network and transport layer and make only cursory checks into the validity of a given connection.

9.2 Stateful packet inspection

9.2.1 Description of stateful packet inspection

Based upon packet filtering technology, the stateful packet inspection approach adds more security checks in an attempt to simulate the secure checks of an application proxy firewall. Instead of simply looking at the address of each incoming packet individually, the stateful packet inspection firewall intercepts incoming packets at the network layer until it has enough information to make some determination as to the state of the attempted connection on upper layers. These packets are then inspected in a proprietary inspection module inside the operating system kernel. State-related information required for the security decision is examined in this inspection module, then maintained in dynamic state tables for evaluating subsequent connection attempts. Packets that are cleared are then forwarded inside the firewall, allowing direct contact between the internal and external systems.

Because most of the examination occurs in the kernel, stateful packet inspection firewalls are often faster than application proxy firewalls. Although the stateful packet inspection approach has significantly enhanced the security of simple packet filtering firewalls, it will fail security checks that require collecting packets into larger units like URLs or files. Above that it must make security decisions without information of the application layer of the protocol stack in the same way that an application proxy handles this. Packet filters with stateful inspection still allow external users direct access to business applications and systems that may very well have poorly configured operating systems with well-known security vulnerabilities.

Application proxies mask these same vulnerabilities by limiting the access to an application or a computer

system to a finite set of identifiable tasks within the proxy itself.

9.3 Application firewall

9.3.1 Description of application firewall

The application proxy approach offers superior security control because it provides application-level awareness of attempted connections by examining everything at the highest layer of the protocol stack. Because it has full visibility at the application layer, an application proxy service can easily see the granular details of each attempted connection up front and implement security policies accordingly. Application proxy services also feature a built-in proxy function – terminating the client connection at the application gateway and initiating a new connection to the internal protected network. The proxy mechanism provides added security because it separates the external and internal systems and makes it more difficult for hackers on the outside to exploit vulnerabilities on systems inside.

Secure gateways using the application proxies provide the strongest security with the only drawback being that the added security can negatively impact the performance. Furthermore, for new services it often takes time before the proxy for this service becomes available.

9.4 Content filtering

9.4.1 Description of content filtering

Security gateways with application level proxies often implement content filtering too. Content filtering comprises the protection against malicious code (like viruses, worms and Trojan horses) and also mobile code (like Java, JavaScript, ActiveX, or any other executable code) which can cause damage to networks, applications, and data.

As most of this malicious code is distributed over the Internet via email or HTTP-based communication (e.g. downloads from a web site or a FTP site), the protection should start at the point where the security gateway interfaces to the Internet. Therefore a virus scanner or more generally, a content scanner is added to the screened subnet or the demilitarized zone (DMZ). In most of the installations, the content scanner is linked directly to the firewall with a network interface so that the SMTP-based email traffic and the HTTP-based communication is routed to the content filtering scanner.

The predominant technologies for content analyzing are as follows:

• Signature-based scanning (searching for known patterns);

• Investigative analysis (analyzing code for functions and behavior known to be associated with malicious code)

• Sandbox technology (essentially a content monitoring program, which quarantines suspect code in a “sandbox”).

As the difference between content scanning and intrusion detection is small, especially regarding networkbased intrusion detection, an intrusion detection system (IDS) can also be combined with the firewall by implementing an IDS agent on the firewall device. See ISO/IEC TR 15947:2002, Information technology —Security techniques — IT intrusion detection framework.

NOTE Selection, deployment and operations of intrusion detection systems will form the subject of a future

International Standard (ISO/IEC 18043).

Content filtering technology also has some limitations. If data is encrypted on the transport or application layer (e.g., SSL/TLS or S/MIME), content screening is no longer possible unless the encrypted data are decrypted and re-encrypted again on the firewall. N.B. this could pose security threats such as “man in the middle” attacks.

There are legal implications regarding content scanning and filtering, especially where a strong data protection legislation is required. In such a scenario, only automatic scanning for malicious code is allowed, but not the scanning for specific content of an email because this would influence the privacy of the sender and of the recipient.

9.5 Intrusion protection system

9.5.1 Description of intrusion protection system

The intrusion is an 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. The intrusion prevention is a formal process of actively responding to prevent intrusions. The intrusion prevention system is a variant on intrusion detection systems that are specifically designed to provide an active response capability.

10 Design techniques

10.1 Security gateway components

The section provides an overview of four distinct categories of security gateways by component, e.g. switches, routers, and firewalls.

10.1.1 Switches

Switches are used to allow high-speed communications delivering full network bandwidth to each physical port. Generally switches are layer 2 devices which are extensively used to segment local area networks. Further, they can provide subnet isolation when VLAN techniques are implemented. Through the use of access control lists (ACLs) applied to different OSI model layers 2, 3 and 4, the traffic between a switch and the nodes connected to that switch can be controlled. Access control functionality provided by switches makes them useful for inclusion as components of security gateway architectures, especially for the implementation and structuring of any screened subnets’ respective demilitarized zones. Switches used in a security gateway environment should not be connected directly to a public network, due to various threats, e.g., denial-of service-like attacks that can cause the exposed switch to flood connected networks with packets.

10.1.2 Routers

Routers are normally designed to connect different networks by supporting multiple network protocols and to optimize the network traffic and the routes between communicating hosts. In addition, routers can be used as components for security gateways as they are able to filter the respective data communication data packets based on packet filtering techniques. A router that utilizes this checking of packet information to control network traffic is often referred to as a screening router (see 8.1.1). Routers normally work on the layer 3 of the OSI model, the network layer, where only a control of the low level information of the data packets is possible in so far that no check of the user data is performed. Routers can perform NAT and packet filtering.

10.1.3 Application level gateway

An application level gateway is a hardware and software based device or set of devices. Application level gateways are specifically designed to restrict access between two separate networks. Primarily two techniques are used for implementing application level gateways:

• Stateful Packet Inspection;

• Application Proxy.

Combinations and variations (e.g., circuit-level firewalls) of these techniques may also be used. In addition NAT can be performed by application level gateways.

10.1.4 Security appliances

Network devices (routers, switches, modems etc.) equipped with hardened operating systems, all dedicated to security purposes are called Security Appliances. These devices can be a base for security software (firewall, IDS/IDP, anti-virus protection etc). Security appliances are offered on a wide range of platforms to meet diverse security needs, from the smallest remote locations to large corporate networks, and data centres as well. Appliances dedicated to protect remote locations or single computers are called Personal Firewall Appliances although they may include other security functions, e.g. anti-virus protection. All techniques mentioned in Clause 6 can be implemented by using security appliances.

10.2 Deploying security gateway controls

[Editor's note] The intention of Editor is to update clause 8, security gateway architecture, of ISO/IEC 18028-3-2005(E).

10.3 Guidelines for network security gateway architecture

[Editor's note] The intention of Editor is to update clause 9, guideline for selection and configuration, of ISO/IEC 18028-3-2005(E).

Bibliography

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall, Bonn 1997

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Firewall Studie II, Bonn 2001

[3] Chapman, D. Brent, Zwicky, Elizabeth D.: Building Internet Firewalls, Cambridge 2000 (O'Reilly)

[4] Cheswick, William R.; Bellovin, Steven M.: Firewall and Internet Security. Repelling the Wily Hacker.Reading, a.o. 1994 (Addison-Wesley)

[5] Ellermann, Uwe: Firewalls. Isolations- und Audittechniken zum Schutz von lokalen Computer-Netzen.Berlin 1994 (DFN-Bericht Nr. 76)

[6] Siyan, Karanjit; Hare, Chris: Internet Firewalls and Network Security. Indianapolis 1995 (New Riders Publishing)

[7] Wack, John; Cutler, Ken; Pole, Jamie: Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology, 2001 (National Institute of Standard and Technology (NIST) Special Publication 800-41)

[8] ISO/IEC TR 15947:2002, *Information technology — Security techniques — IT intrusion detection framework*

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

[10] ISO/IEC 18028-2, *Information technology — Security techniques — IT network security — Part 2: Network security architecture* 1)

[11] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security*

incident management

[12] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

Final Committee Draft **ISO/IEC FCD 27033-3**	Reference number: ISO/IEC JTC 1/SC 27 **N7921**
Date:**2009-12-15**	Supersedes document SC 27 N7562

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2010-04-02** Please submit your votes and comments via the online balloting application by the due date indicated.

ISO/IEC FCD 27033-3

Title: Information technology -- Security techniques -- Network security -- Part 3: Reference network scenarios – Threats, design techniques and control issues *)

Project: 27033-3 (1.27.58.03)

Explanatory Report

Status	**SC 27 Decision**	**Reference documents**	
		Input	**Output**
27033-3* (18028-6) by subdivision ** subject to SC 27 approval of renumbering to 27033-3*	19th Plenary, April 2007, resolution 17 (N5939).		Proposed modif. (subdivision) (N5995); JTC 1 endorsm. (N6118)
1st WD 27033-3* ** subject to JTC 1 endorsement of renumbering*	3rd WG 4 meeting, Oct. 2007, resolutions 1 & 3 (N6017).		Text for 1st WD (N6283); Proposed modif. (renumbering) (N6406); JTC 1 endorsm. (N6457).
2nd WD 27033-3	4th WG 4 meeting, Apr. 2008, resolutions 1, & 13, 4 (N6421); 20th SC 27 Plenary, April 2008, resolution 2 (N6799), Deleg. of Auth. for 1st CD resolution 14 (N6799).	SoCom (N6514); CH com. (N6601).	Editor's appoint. (res. 13) DoC (N6426); Text f. 2nd WD (N6746).
3rd WD 27033-3	5th WG 4 meeting, Oct. 2008, resolutions 1 & 2 (N6904).	SoCom. (N6995)	DoC (N6912); Text f. 3rd WD (N6921).
1st CD 27033-3	7th WG 4 meeting, May 2009, resolutions 1, 3 & 7 (N7551); 21st SC 27 Plenary, May 2009, resolution 8 (N7777), Deleg. of Auth. for FCD resolution 16 (N7777).	SoCom. (N7530)	DoC (N7561); Text f. 1st CD (N7562).
FCD 27033-3	8th WG 4 meeting, November 2009, resolutions 1, & 7 (N7908).	SoV (N8034)	DoC (N7920); Text f. FCD (N7921).

FCD Registration and Consideration

In accordance with resolution 7 (contained in SC 27 N7908) of the 7th SC 27/WG 4 meeting held in Redmond (WA, USA) 2nd – 6th November 2009, the attached document has been registered with the ISO Central Secretariat (ITTF) as Final Committee Draft (FCD) and is hereby circulated for an FCD letter ballot closing by

2010-04-02

PLEASE NOTE: The FCD ballot period is four months but has been shortened by two weeks in order not to delay the further development of this project and to close in time to the editing meeting for ISO/IEC FCD 27033-3 (revision) scheduled to be held during the next WG 4 meeting in Melaka, Malaysia, 19th – 23rd April 2010.

**) subject to JTC 1 endorsement on the title change*

Secretariat ISO/IEC JTC 1/SC 27
DIN Deutsches Institut für Normung e.V., Burggrafenstrasse 6, 10787 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

ISO/IEC JTC 1/SC 27 N7921

Date: 2009-12-15

ISO/IEC FCD 27033-3

ISO/IEC JTC 1/SC 27/WG 4

Secretariat: DIN

Information technology — Security techniques — Network security — Part 3: Reference network scenarios -- Risks, design techniques and control issues

Technologies de l'information — Techniques de sécurité — Partie 3: Sécurité de réseaux T

Warning

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: International Standard
Document subtype:
Document stage: (40) Enquiry
Document language: E

X:\TA3\TG3-3\NA043\NA043_Sekretariate\JTC1_SC27\03_Projekte\PROJECT_admin\27033\27033-3_Revision_Oct2007)\03_02_FCD_27033-1_20091215\SC27N7921_FCD_27033-3_20091215\SC27N7921_FCD_27033-3_20091215.doc STD Version 2.3

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27033-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

ISO/IEC 27033 consists of the following parts, under the general title *Information technology — Security techniques — Network security*:

— *Part 1: Guidelines for network security*

— *Part 2: Guidelines for the design and implementation of network security*

— *Part 3: Reference network scenarios -- Threats, design techniques and control issues*

— *Part 4: Securing Communications between networks using security gateways - Risks, design techniques and control issues,*

— *Part 5: Securing virtual private networks - Risks, design techniques and control issues*

(It should be noted that there may be other Parts in the future. Examples of possible topics to be covered by future Parts include local area networks, wide area networks, wireless and radio networks, broadband networks, voice networks, Internet Protocol (IP) convergence (data, voice, video) networks, web host architectures, Internet email architectures (including outgoing online access to the Internet, and incoming access from the Internet), and routed access to third party organizations. The main clauses of all such Parts should be Threats, Design Techniques and Control Issues.)

Information technology — Security techniques — Network security — Part 3: Reference network scenarios -- Risks, design techniques and control issues

1 Scope

ISO/IEC 27033 Part 3 describes the threats design techniques and control issues associated with reference network scenarios. For each scenario, Part 3 provides detailed guidance on the security threats and the security design techniques and controls required to mitigate those risks. Where relevant, Part 3 includes references to Parts 4 to 6, to avoid duplicating the content of those documents.

The information in Part 3 should be used when reviewing technical security architecture/design options and selecting and documenting the preferred technical security architecture/design and related security controls, in accordance with ISO/IEC 27033 Part 2. The particular information selected (together with information selected from Parts 4 to 6) will depend on the characteristics of the network environment under review, i.e. the particular network scenario(s) and 'technology' topic(s) concerned.

Overall, Part 3 will aid considerably the comprehensive definition and implementation of security for any organization's network environment.

2 Normative references

For the purposes of this document, the normative references given in ISO/IEC 27033-1 are applicable.

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 27033-1 and the following apply: accountability, asset, authenticity, availability, baseline controls, business continuity management, confidentiality, data integrity, impact, information security event, information security incident, information security incident management, 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 27033

3.2.1
opacity
protection of information that might be derived by observing network activities, such as deriving addresses of end-points in a voice-over-IP call. Opacity recognizes the need to protect actions in addition to information

3.2.2
social engineering
act of manipulating people into performing actions or divulging confidential information

4 Abbreviated terms

AAA	Authentication, Authorization and Accounting
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DNSSEC	Security Extensions for DNS
DoS	Denial of Service
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPsec	IP Security Protocol
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open Systems Interconnection
PDA	Personal Data Assistant
PSTN	Public Switched Telephone Network
QoS	Quality of Service
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer (Encryption and authentication protocol)
VoIP	Voice over IP
VPN	Virtual Private Network

5 Structure

The structure of ISO/IEC 27033-3 comprises of:

- an overview of the approach to addressing security for each reference scenario listed in this document (clause 6)
- a clause for each reference scenario (clause 7-15), which describes:
  - risks associated with the reference scenario
  - a presentation of the security controls and techniques based on the approach in clause 6

The scenarios in the document are ordered per the following framework where the objective is to evaluate a given scenario as a function of the:

- **type of user access**, whether the user is inside an enterprise, or the user is an employee who is accessing enterprise resources from outside, or the user is a consumer, vendor or business partner, and,
- **type of information resources accessed**, open, restricted or outsourced resources.

Thus, the framework helps present a consistent structure, and makes addition of new scenarios manageable, as well as justifies the need for the various scenarios presented in this document.

Table 1 — Framework for Ordering Network Scenarios

		Users		
		Inside	**Employees from outside**	**Outside**
Accessed information resources	**Open**	- Internet access services for employees - Business to business services		- Business to customer services
	Restricted	- Enhanced collaboration services - Business to business services - Network segmentation - Networking support for home and small business offices	- Mobile communication - Networking support for travelling users	- Enhanced collaboration services - Business to business services - Business to customer services
	Outsourced	- Outsourcing services		- Outsourcing services

Thus, the order in which the scenarios are listed in this document is as follows:

- Internet access services for employees (clause 7)
- Business to business services (clause 8)
- Business to customer services (clause 9)
- Enhanced collaboration services (clause 10)
- Network segmentation (clause 11)
- Networking support for home and small business offices (clause 12)
- Mobile communication (clause 13)
- Networking support for travelling users (clause 14)
- Outsourcing services (clause 15)

6 Overview

The guidance presented in this document for each of the identified reference network scenarios is based on the following approach:

- Review the background information and scope of the scenario
- Describe the threats and risks relevant to the scenario
- Perform risk analysis on discovered vulnerabilities and
- Analyse the business impact of addressing the vulnerabilities.
- Determine the implementation recommendations for securing the network

In order to address the security of any network, an approach that is systematic and provides an end-to-end evaluation is desirable. The complexity of such an analysis is a function of the nature and size of the network in scope. However, a consistent methodology is important to managing security, especially due to the evolving nature of technology.

The first consideration in a security assessment is the determination of assets that require protection. These can be largely categorized into infrastructure, services or application assets. However, an enterprise can chose to define their own categories, but the distinction is important because the exposure to threats and attacks is unique to each asset category or type. For instance, if a router is categorized an infrastructure asset, and Voice over IP as an end-user service, then a Denial of Service (DoS) attack requires a different consideration in each case . Specifically, the router requires protection against a flood of bogus packets on the router's physical port that can prevent or impede the transmission of legitimate traffic. Similarly, the VoIP service requires protection of the subscriber's account/service information from deletion or corruption such that a legitimate user is not prevented from accessing the service.

Network security also entails protection of the various activities supported on the network, such as management activities; control/signaling messages; and end-user data (resident and in-transit). For example, a management GUI can be subject to disclosure as a result of unauthorized access (easy to guess administrator ID and password). The management traffic itself is subject to corruption due to forged OA&M commands with spoofed IP addresses of the operations systems, or disclosure by sniffing, or interruption due to a packet flood attack.

The approach of identifying assets and activities enables a modular and systematic consideration of threats. Each reference network scenario is examined against a known set of threats to ascertain which threats are applicable. Annex B provides a list of known industry threats. Although the list should not be viewed as exhaustive, it provides a starting point for any analysis. Once the threat profile for the network is derived, the vulnerabilities are analyzed to determine how the threats may be realized in the context of the specific asset under consideration. Such an analysis will help determine what mitigations are missing and what countermeasures need to be deployed to achieve the protection objectives. A countermeasure will reduce the likelihood of the threat being successful and/or reduces its impact. Risk analysis that analyzes the risk represented by discovered vulnerabilities. Business impact analysis consists of arriving at a business decision regarding how to address each vulnerability: remediate, accept risk, or transfer risk.

Designing countermeasures and implementing controls for protecting vulnerabilities against threats is part of any security assessment methodology. Per the ISO/IEC 27000 series standard, the selection and implementation of relevant controls is critical to asset/information protection. The standard requires the preservation of confidentiality, integrity and availability of information, and specifically states that in addition, other properties such as authenticity, non-repudiation and reliability can also be involved.

The following is a set of security properties that is used in this document to develop mitigations and countermeasures in an objective manner. The rationalization for the need for each security property (in addition to confidentiality, integrity and availability) is described below:

- Confidentiality is concerned with protecting data from unauthorized disclosure.
- Integrity is concerned with maintaining the correctness or accuracy of data and protecting against unauthorized modification, deletion, creation, and replication
- Availability is concerned with ensuring that there is no denial of authorized access to network elements, stored information, information flows, services, and applications.
- Access Control provides, through the use of authentication and authorization, control to enforce access to network devices and services, and ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. For example, in an IPTV deployment, one of the known security recommendations, disabling the debugging interface on subscriber set top boxes, is derived from a consideration of the access control property. A review of confidentiality, integrity or availability will not result in some other recommendations.
- Authentication is concerned with confirming or substantiating the claimed identity of a user or communicating parties when used by access control for authorization, and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication. For instance, an individual may gain access to a network management system, but will need to be authenticated in order to update subscriber service records. Thus the ability to perform network management activities cannot be assured by simply addressing confidentiality, integrity, availability, or access control.

Note: In Role-Based Access Control, authorization takes place by virtue of the user being assigned to a role. Access control then verifies the user has the role prior to granting access. Similarly, access control lists grant access to anything that satisfies the policy, so if you satisfy the policy requirements you are authorized access. The authentication and authorization functions are null in this case.

- Communication or Transport Security is concerned with ensuring that information only flows between authorized end-points without being diverted or intercepted.
- Non-repudiation in concerned with maintaining an audit trail, so that the origin of data or the cause of an event or action cannot be denied. Identifying the authorized person that performed an unauthorized action on protected data has nothing to do with the data's confidentiality, integrity, availability.
- Opacity is concerned with protecting information that might be derived from the observation of network activities. Opacity recognizes the need to protect actions in addition to information. Protecting information is addressed by confidentiality. Protecting the conversation in a phone call between Person A and Person B protects their confidentiality. Protecting the fact that Person A and Person B had a phone call ensures opacity.

In all the scenarios described in this document, the above-stated security properties are reviewed as part of the security design technique and control phase. Table 2 below shows examples of network security mechanisms that can be implemented for security properties that are selected for mitigating the potential risk.

Table 2 — Example Network Security Techniques

Security Considerations	Security Mechanisms / Techniques
Access Control	Physical badge system, Access Control Lists (ACL), Separation of duties
Authentication	Simple log-in/password, Digital certificates, Digital Signatures, SSLv3, SSO, CHAP
Availability	Redundancy & back-up, DoS mechanisms, Firewalls, IDS/IPS (for blocking DoS), Business continuity, Managed network & services with SLAs

Security Considerations	Security Mechanisms / Techniques
Communication Security	IPsec / L2TP / MPLS tunnels, Private Lines, Separate networks
Confidentiality	Encryption (3DES, AES), Access control lists, File permissions
Integrity	IPsec HMACs (e.g. MD5, SHA-1), Cyclic redundancy checks, Anti-Virus Software, Patching
Non-repudiation	Logs, Role based access control, Digital signatures
Opacity	Encryption of IP headers(for example: IPsec VPNs), NAT

In this document, the above considerations are inherent in the design and implementation discussed in the context of each reference network scenarios. Typically, an organization will select the relevant ISO/IEC 27002 controls to meet their business objectives, and the guidelines in this document are intended to provide the network level considerations required for the implementation of the chosen controls.

7 Internet access services for employees

7.1 Background

Organizations that need to provide Internet access services for their employees should consider this scenario so as to ensure access for clearly identified and authorized purposes, not general open access. Organizations need to be concerned about managing that access to avoid loss of network bandwidth and responsiveness as well as exposure to legal liability when employees have uncontrolled access to Internet services.

Controlling employee access to the Internet is a growing concern given the number of emerging Internet case laws. Thus an organization is responsible for establishing, monitoring and enforcing an unambiguous Internet Use Policy by evaluating the following scenarios, and providing relevant claims in the policy:

- Internet access is allowed for business reasons,
- if Internet access is also allowed in (limited) form for private purposes, which services are allowed to be used,
- if enhanced collaboration services are allowed,
- if employees are allowed to participate in chat channels, forums etc.

Even though often a written policy acts as a significant deterrent to unacceptable Internet usage, the organization is still subject to substantial information security risks. In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

7.2 Security threats

Information security risks related to Internet access services for employees are associated with:

- Virus attacks and introduction of malware:

- o employees using the Internet are also a prime target for malware which may lead to, loss or corruption of information and loss of control of IT infrastructure, and a huge risk to an organization's network security,
- o user downloaded files or programs may contain malicious code. Given the ubiquity of applications such as instant messaging, peer-to-peer file sharing, and IP telephony, employees can inadvertently download and install a malicious application that can evade network defences using such techniques as port agility (jumping around among open ports) and encryption. In addition, peer-to-peer applications can be exploited to serve as covert channels for botnets,
- o vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans. Once infected, availability can be severely impacted due to virus propagation activities leading to network overload. Trojans can enable unauthorized external access leading to confidentiality violations.

- Information leakage:
  - o applications that allow upload of information to web-based servers, may lead to uncontrolled transfer of data from inside an organization to the Internet. If encrypted sessions are used (e.g. TLS) then even logging of such activity may not be possible. Similar security risks are introduced when unauthenticated portable code is executed on systems inside an organization.
- Unauthorized usage and access
  - o Loss of control of infrastructure, systems and applications can result in fraud, denial of service, and abuse of facilities
- Regulatory non-compliance
  - o legal liability due to non-compliance to legislation or regulatory obligations,
  - o non-conformance to an organization's use policy can lead to regulatory non-compliance
- Reduced network availability due to inadequate bandwidth or stability problems
  - o excessive use of high bandwidth services such as streaming media or peer to peer file sharing may lead to network overload

7.3 Security design techniques and controls

Security design techniques and controls related to employee internet access services are discussed in the Table below:

For a given security risk, each security property is reviewed for applicability in reducing the risk, and then a corresponding technical implementation example is presented in the second column. For example, integrity, access control, and authentication are applicable for protecting against malicious code.

Table 3 — Security Controls for Employee Internet Access Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Only provide the business relevant internet services towards the employee. Use of blacklists for authorized services, so as to not allow chat channels or web mail services, or peer-to-peer networking protocols. • Use of virus checking software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. Ensure that anti-virus updates are automatically installed or the user is

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
	alerted to the fact that updates are available • Use of antivirus software on all client systems, especially those used for internet access by employees. • Scan files and all stored information for viruses and Trojans and other forms of malware • Data/file integrity verification using algorithms such as hash/checksums, certificates • Blocking pop-ups and web advertisements, • Routing of traffic used for Internet access services through a small number of controlled security gateways • Active content authentication.
Information Leakage	
• Communication security • Integrity • Access Control	• Implementing Filters for mobile code on the gateways to the Internet. • Accept mobile code only from uncritical, white listed sites. • Accept only digital signed mobile code signed from approved Certification Authorities or from approved vendors, enable the respective configuration options on the client side, e.g. by actively manage and implement a white list of allowed code signing Certification Authorities.
Reduced Network Availability	
• Integrity • Availability	• Proper vulnerability management and patching of known system vulnerabilities within timeframes based on vulnerability criticality. • Focus of vulnerability management should be all systems receiving internet traffic, either on transport or application level, which includes all systems used in the context of the gateways used towards the Internet as well as end user systems used for accessing internet services, especially if they use a windows operating system. • Throttle bandwidth for streaming media (only if permitted per business policy) • Network and system resources should be monitored (IDS, logs, audits, etc.) to detect system, security, and operational events.
Unauthorized Access	
• Access Control • Non-Repudiation	• Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols. • Restrict the use of services which easily enable the transfer of big amounts of data. • Ensure that proper logging and monitoring is in place for all services which allow the possibility to transfer data towards the Internet.
Unauthorized Usage	
• Access Control	• Cleary define authorized and unauthorized usage of internet access in a dedicated policy (see sample template in Annex A

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
	• Ensure user awareness through adequate education and training • Only provide the business relevant internet services towards the employee. Use of blacklists for unauthorized services, e.g. chat channels or web mail services. Implementation of filters for non authorized protocols, e.g. peer-to-peer networking protocols.
Regulatory Non-Compliance	
• Non-Repudiation	• Usage logs, time stamps • User awareness and training

8 Business to business services

8.1 Background

Organisations that conduct transactions with other organizations, such as manufacturer, wholesaler, retailer, should consider this scenario

Traditionally business to business services have been implemented by using dedicated leased lines or network segments. The Internet and the related technologies do provide more options, but also introduce new security risks associated with the implementation of such services. The evolved business-to-business e-commerce model allows organizations to conduct business over the Internet, and the applications focus on using the Internet, extranet, or both to improve business partnerships in which the entities are known to each other and all users are registered, unlike the business to consumer scenario.

Typically business to business services have their own requirements. For example, availability and reliability are very important requirements as frequently organizations are directly dependent on working business to business services.

When using the Internet as a base network connection to implement business to business services, requirements such as availability and reliability need to be handled differently than before. Proven measures such as quality of service assumptions used, e.g. in conjunction with leased lines, do not work any more. The new security risks need to be mitigated by appropriate design techniques and controls. The focus is on reinforcing trust between organizations by preventing access to unauthorized data and maintaining separation of business systems.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

8.2 Security threats

Information security risks related to business-to-business services are associated with:

- Virus attacks and introduction of malware
    - o malware exploits leading to infiltration of systems leading to disruptions or unauthorized access to sensitive information,

- vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks on business to business portals or extranets,
- insider attacks by authorized business partners,
- Forgery of transaction contents (messages not reaching the intended recipient or data is tampered during transmission).

8.3 Security design techniques and controls

Information security design techniques and controls related to business-to-business services are associated with:

Table 4 — Security Controls for Business to Business Services Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus Attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Use of virus checking software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available • Scan files and all stored information for viruses and Trojans and other forms of malware • Data/file integrity verification using algorithms such as hash/checksums, certificates • Routing of traffic used for Internet access services through a small number of controlled security gateways • Active content authentication.
Denial of Service	
• Availability • Opacity	• Disable unused protocol ports and services to prevent them from responding to unauthorized scans/probes, which has the potential of causing a traffic flood DoS • Excluding descriptive information from warning banners prevents providing targeting information to attackers
Insider Attacks	
• Access Control • Non-Repudiation	• Well defined security policy for access management (for business relationship management) • Clearly identified roles and responsibilities • Customised warning banners • Limit on privileges • Logging of all critical/non-critical transactions by users
Forgery of Transaction Contents	
• Non-Repudiation	• Detailed logs of transactions • Use of digital signatures

9 Business to customer services

9.1 Background

Organisations that conduct transactions with consumers should consider this scenario.

Business to customer services, also referred to as e-business services includes services such as e-commerce, e-banking, and e-government. **In business to customer services, security must balance enabling transactions with preserving brand and business value**

The information security requirements include those associated with:

- confidentiality (especially regarding e-banking),
- authentication,
- integrity,
- data communications security where the end user expects the business service provide to protect the transaction path between the user and the provider. Resistance against sophisticated attacks (e.g. 'man in the middle' or 'man in the browser' attacks),
- Availability is an important dimension for the e-business provider.

The information security characteristics include:

- security only 'guaranteed' on the end platform typically under the control of an organization, providing a good environment for implementing controls and maintaining a good platform level security,
- security on the customer platform, often a PC, can typically be poor. It is harder to get controls implemented in such an environment, and thus customer platforms would present significant risks in this scenario (without a 'conditions for secure connection' set of requirements in a contract, which may be difficult to impose in such an environment).

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

9.2 Security threats

Information security risks related to business to customer services are associated with:

- Virus attacks and introduction of malware
  - malware exploits leading to infiltration of systems leading to disruptions or unauthorized access to sensitive information,
  - vulnerabilities in web browsers or other web applications may be exploited by malware, and result in virus infections and installation of trojans
- Unauthorized access:
  - Unauthorized access of back-end databases (e.g. SQL injection attacks, cross-site scripting attacks)
- Loss of sensitive data (stored and in-transit)
  - Account harvesting which is the ability to derive valid account information depending on how a web application responds to user's authentication attempts. Automated scripts are often used to harvest valid user ids and account names.
  - online identity theft using successful social engineering attacks (through the use of deceptive techniques), such as phishing attacks and DNS-based attacks that connect users to fraudulent web-servers that look legitimate but are not

- o unauthorized access to systems or networks with malicious intent to copy, modify or destroy data
- o illegal content decryption leading to copyright violations and theft of content
- DoS and DDoS attacks
- Forgery of transaction contents (messages not reaching the intended recipient or data is tampered during transmission).

9.3 Security design techniques and controls

Security design techniques and controls related to business to customer services are discussed in the table below.

Table 5 — Security Controls for Business to Customer Services Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Virus Attacks and Introduction of Malware	
• Integrity • Access Control • Authentication	• Use of virus checking software on the gateways to the Internet for scanning all traffic from and to the Internet. Scanning should include all network protocols authorized for use. • Scan files and all stored information for viruses and Trojans and other forms of malware • Data/file integrity verification using algorithms such as hash/checksums, certificates • Routing of traffic used for Internet access services through a small number of controlled security gateways • Active content authentication.
Protection against Unauthorized Access	
• Access Control • Authentication	• Limit permissions of web applications when accessing backend databases • Network segmentation and security tiers within a Demilitarized Zone (DMZ) to prevent direction connection paths to corporate data assets. • Secure user registration to ensure that access credentials are only issued to authentic users – such as using an independent Registration Authority for the process, • Authentication using digital certificates, passwords, biometrics or smartcards, • Firewalls and access control lists to prevent unauthorized user access, • Role based access control to limit the function the user is permitted to perform. • Web application log reviews for attack identification and containment
Protection of Sensitive Data (In-transit and Stored)	
• Confidentiality • Communication Security • Integrity • Opacity	• Suitable levels of encryption of stored information, • Ensuring security between web browsers and web servers using technologies such as SSLv3/TLS • Securing basic Web Service communication using for example SOAP messages • Data/file integrity verification using algorithms such as

Applicable Security Properties for Identified Threats	Implementation Design and Technologies

	hash/checksums, certificates
	• For web application level data integrity of URLs, cookies or hidden form elements:
	  o encrypt all data (even if SSLv3 is being used)
	  o Use timestamps with the variables
	  o Digitally sign or use keyed hash for sensitive data
	• Use of reverse proxy between the web server and the external network

Denial of Service	
• Availability • Opacity	• Disable unused protocol ports and services to prevent them from responding to unauthorized scans/probes, which has the potential of causing a traffic flood DoS • Excluding descriptive information from warning banners prevents providing targeting information to attackers
Forgery of Transaction Contents	
• Non-Repudiation	• Detailed logs of transactions • Use of digital signatures

10 Enhanced collaboration services

10.1 Background

Organisations that utilize services involving multiple employees should consider this scenario. Examples of such services are:

- Groupware
- File servers
- Mailing List
- Web-based services

Enhanced collaboration services, which integrate various communication and document sharing possibilities, are gaining importance in today's business environments.

Such collaboration services typically integrate video telephony, voice communication with chat channels, e-mail systems, as well as document sharing and online co-working environments.

There are two basic ways how to use such services for an organization:

- use them as internal services only, but with the disadvantage that the services cannot be used with external partners, etc.,
- use them as internal services and services external to an organization. This offers much more benefit from using such services, but at the same time has more associated security risks compared with only internal usage.

Regarding implementation, the services may be:

- implemented in-house, or
- from a third party.

If the services are to be used internally and externally, then buying in collaboration services from a third party may be a more appropriate solution.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage. The security controls apply to management, signalling and user traffic.

10.2 Security threats

Information security risks related to enhanced collaboration services are associated with:

- Unauthorized access and disclosure of sensitive information
  - misuse of collaboration tools to illegally share copyrighted material, obtain confidential data, and expose users to undesirable content or propaganda,
  - violation of Opacity by monitoring usage patterns, spamming and identity attacks
- Introduction of malware
  - distribution and execution of malware by exploiting shared resources
- Reduced Network Availability
  - overloading the network with legitimate traffic,
  - exploiting protocol vulnerabilities used in the collaboration services.

10.3 Security design techniques and controls

Information security design techniques and controls related to enhanced collaboration services are associated with:

If managed services are involved, then it is expected that the organization's security policy will address additional server segmentation and non-disclosure agreement clauses in addition to the technical controls discussed above.

Table 6 — Security Controls for Enhanced Collaboration Services

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Unauthorized access and disclosure of information	
• Access Control • Authentication • Confidentiality • Communication Security • Non-Repudiation	• Role-based access to applications, networks, and storage • Assigning users in different roles to different VLANs with different permissions • Role based policies for usage rights and access to resources, such as applications that a user can run, • Access control lists • Strong authentication and authorization • VLANs for network virtualization • Host-based IDSs • Encryption of data
Introduction of malware	
• Integrity	• Use of screen transferring software such as Terminal Servers to minimize the data and potential malware to enter the

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
	corporate environment
Reduced Network Availability	
• Availability	• using virtual storage area networks to improve availability and security of data at rest, • prevention of information removal by using software tools to prevent copy/paste of information, block attempts to write to removable media, or printing, • monitoring software to detect policy violations – such as access violations of applications and other network resources

11 Network segmentation

11.1 Background

Organisations that wish to divide their internal network into multiple domains in to align with the organizational structure should consider this scenario.

Segmenting networks is a technique that can be used to augment system and application access controls. Network segmentation can be used to group certain types of activity, application, or systems in a way that access is only possible to those with access to the network segment. In this way, network access controls augment other end-point access controls and provides an additional level of defence in depth. For example, network segmentation can be used to:

- segregate administrative and maintenance capabilities from routine user access to business applications
- segregate critical applications from other applications
- segregate databases from most users
- For multi-national organizations country specific legislation has a great influence on information security requirements. To cover the different information security requirements for the countries an international organization is doing business in, segmentation of a network in effect in line with country borders can be an effective approach. For example, a particular country's legislation may require specific protection of customer/client data, and does not allow the transfer of such data to another country. This typically requires additional information security controls to guarantee compliance with such legislation.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

11.2 Security threats

Information security risks related to network segmentation for fulfilling country-specific compliance requirements in international organizations are associated with:

- Non compliance to country specific legislation, which may be associated cost liability,
- Data Leakage
    - o breach of confidentiality, e.g. when customer/client data is accessible from countries from which it should not,
    - o breach of country specific privacy requirements,
    - o reputation related risks implicated by not meeting customer/client expectations regarding confidentiality or opacity.

11.3 Security design techniques and controls

Information security design techniques and controls related to network segmentation for fulfilling country-specific compliance requirements in international organizations are associated with:

Table 7 — Security Controls for Network Segmentation

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Regulatory Non-compliance	
• Opacity • Confidentiality	• Policy and User Awareness: o Privacy laws o Allowable encryption technologies o Data storage, transfer laws o Laws for lawful intercept
Data Leakage	
• Access Control • Authentication • Integrity	• Security Gateways • Application Level Proxies • Data Encryption

12 Networking support for home and small business offices

12.1 Background

Organisations that need to provide access to internal resources to their employees at home or small offices should consider this scenario.

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

In many home or small business scenarios the infrastructure may also be used for private as well as for business purposes – which may result in additional information security risks.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

12.2 Security threats

Information security risks related to networking support for home and small business offices are associated with:

- Unauthorized access:
  - weak configuration settings in network access equipment, e.g. of SOHO routers (Small Office and Home Office),
  - use of split-tunneling,
  - missing or weak physical security controls,
  - longer window of opportunity due to “always-on” nature of network connectivity,

- o use of guest accounts and default settings

- Virus attacks and introduction of malware:
  - o equipment, including PCs used in the home or small office network and operated with inadequate security controls, e.g. missing or weak malware protection etc.,
  - o problems introduced by mixing private and business environments, e.g. by the private usage of protocols with inherent high risks, such as peer to peer file sharing protocols,
  - o patching failure

- Reduced network availability
  - o Once infected, availability can be severely impacted due to virus propagation activities leading to network overload

- Disclosure of sensitive information
  - o lack of encryption of data stored on systems and transmitted in the home or small business network,
  - o misuse of access possibilities such as WLAN access in the home or small business network,
  - o lack of awareness and security best practices training of end-users
  - o invalidation of assumptions regarding the protection of Intranets, since the network gateways in home or small office environments do not provide the same protection level as gateways used to interconnect office branches.

12.3 Security design techniques and controls

Information security design techniques and controls related to networking support for home and small business offices are associated with:

Table 8 — Security Controls for Networking for Home and Small Business Office Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Unauthorized Access	
• Access Control • Authentication • Communication security	• Disable network interfaces and services that are not used • Install host-firewall - drop or reject all incoming connections from outside • Design and technology protections for split tunnelling • Systems should not utilize blank, null, or default passwords. • Strong passwords should be enforced for all users. Anonymous/ guest access should not be permitted. • Technical compliance checks to ensure proper configuration and setup of all security sensitive equipment, e.g. router or WLAN access points • Secure Virtual Private Network technologies in network access components such as network access routers
Virus Attacks and Introduction of Malware & Reduced network availability	
• Integrity • Availability	• Maintain current software versions and patch levels • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available • Use host based Intrusion Detection System (HIDS) at least to detect software/database integrity (as applicable) • Scan files and all stored information for viruses and Trojans and other forms of malware

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
	• Backup of configuration data, and files for incident response and recovery
Disclosure of Sensitive Information	
• Confidentiality • Opacity	• User awareness and training for security best practices • Encryption of stored and transmitted data

13 Mobile communication

13.1 Background

Organizations that permit the use of mobile devices for employees should consider this scenario.

This scenario focuses on the security concerns of enterprises using and deploying mobile devices and applications. Although the main driver for the fast development of new features of mobile devices, such as smart phones or personal data assistants (PDAs), comes from the consumer market, these are also used in business environments. Often such devices are personally owned and used in both for business purposes and privately. Sometimes the devices may be company provided and are used for personal use. Thus, devices directed at the business market need to have features introduced for the consumer market, as the vendors want to gain as much business as possible in a competitive market.

The mobile communication devices allow remote users to synchronize personal databases, and provide access to network services such as wireless e-mail, Web browsing, and Internet access. When a person uses the same device for private as well as business purposes, there is a tendency to circumvent or disregard use policies, thus introducing significant information security risks to the enterprise.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

13.2 Security threats

Information security risks related to mobile communication devices are associated with:

- Unauthorized access of information stored on mobile devices due to:
  - inadequate access control or protection of sensitive information,
  - lack of awareness and inadequate passwords
  - weak configuration
  - hijacking attacks by rogue devices,
  - missing end user awareness of information security protection requirements, e.g. with mixing of private and business information,

- Unauthorized disclosure of sensitive data and location information
  - location-based services can disclose user position information to unauthorized third parties, thus leading to privacy concerns,
  - eavesdropping,

- o involvement of inadequately protected third parties in the communications flow,
- o usage of plaintext or inadequately protected transmission protocols
- o improper disposal procedures

- Unauthorized modification/deletion of stored information (including software) due to:
  - o introduction of malware by installation of software from unauthorized sources
  - o exploitation of vulnerabilities in the underlying operating system

- Spam leading to
  - o increased service charges
  - o enabling phishing attacks
  - o DoS attacks

- Theft or accidental loss, both of which could lead to:
  - o loss of sensitive data whenever data stored on the device is not mirrored or backed up somewhere else,
  - o confidentiality issues when sensitive data stored on the device is not adequately protected,
  - o secure data backup

13.3 Security design techniques and controls

Information security design techniques and controls related to personal mobile communication devices are associated with:

Table 9 — Security Controls for Mobile Communication Scenario

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Unauthorized access of information stored on mobile devices	
• Access Control • Authentication • Non-Repudiation	• User awareness for physical control • Avoiding default configurations • Strong authentication • Enabling logging options • Inactivity timer lock • Firewall • Organization security policy for passwords and business usage (restricting personal use for enterprise-owned devices)
Unauthorized disclosure of sensitive data and location information	
• Confidentiality • Authentication • Communication Security • Opacity	• Encrypting stored and transmitted (wireless) data • Password protection • Avoidance of third party services which require clear text access to transmitted data or, if not feasible, requesting

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
	assurance that confidentiality of processed data is as required, • Ensure secure synchronization procedures, • Secure VPN for remote access connections, • Proper disposal procedures for erasing sensitive data • User consent for location use
Unauthorized modification/deletion of stored information (including software)	
• Confidentiality • Availability • Integrity	• Disable unused wireless interfaces, services and applications, • Up-to-date patching of OS, • Proper disposal procedures for erasing sensitive data, • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available • Software downloads only from enterprise software distribution system (avoiding installation of unlicensed software) • Digital signatures to verify download sources
Spam	
• Access Control	• Content filtering • Increasing user awareness
Theft or accidental loss	
• Confidentiality • Availability	• Remote asset management (disable/lock device) • Periodic secure backup • Centralized management for asset tracking and policy compliance

14 Networking support for travelling users

14.1 Background

Organizations that permit travelling employee to access the enterprise resources should consider this scenario.

Solutions and offerings in this area often focus on the functionality side and are targeted primarily to the consumer market. From an information security viewpoint, the offered functionality levels introduce new risks, e.g. by affecting or invalidating assumptions regarding information security. For example, an assumption of maintaining a well controlled and (from the outside) protected Intranet may be questioned substantially if travelling user access to the Intranet is not implemented with appropriate controls.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

14.2 Security threats

Information security risks related to networking support for travelling users are associated with:

- Unauthorized Access

- misuse of travelling user network support to gain unauthorized access to the Intranet of an organization,
- compromise of security gateways used on the Intranet network border,
- unauthorized access to data stored on travelling user devices.

- Reduced availability
  - availability problems introduced when user expectations regarding network support cannot be met, e.g. when this is dependent on the availability of Internet Service Providers

14.3 Security design techniques and controls

Information security design techniques and controls related to networking support for travelling users are associated with:

Table 10 — Security Controls for Networking Support for Travelling Users

Applicable Security Properties for Identified Threats	Implementation Design and Technologies
Unauthorized Access	

• Access Control
• Authentication
• Communication Security
• Confidentiality
	• enhanced authentication techniques (certificate based authentication, two-factor or challenge response authentication)
	• dedicated services for travelling users based on TLS/SSLv3 protected Web interfaces
	• using Secure Virtual Private Network technologies combined with appropriate security gateways on the client systems (e.g. personal firewalls):
	  o layer 2/3 implementations, e.g. IPsec,
	  o application level VPN's, e.g. based on TLS/SSLv3
	• encryption of stored user data

15 Outsourcing services

15.1 Background

Organizations that use outsourcing services should consider this scenario.

Organizations use outsourced services because it is viewed as a viable business strategy, but it also introduces organizational and operational complexities, specifically for ensuring the quality and security of outsourced services.

The extended enterprise inherits additional risk because of the dependency on the service provider. For instance, service providers or vendors can require direct access to assets inside an enterprise for support and/or incident management issues, thus exposing critical assets to security risks. Whilst many support services require permanent access rights to the supported infrastructure, others may only need temporary access. Often support services need highly privileged access rights in order to fulfil their tasks.

Regardless of the type of outsourcing scenario, security considerations and oversight is required in all such contractual arrangements.

In the clauses below, the security threats and advice on security design techniques and controls to mitigate those risks are described for internal, and internal plus external, usage.

15.2 Security threats

Information security risks related to outsourced IT support services are associated with:

- Unauthorized access to other internal systems (when supplier accesses internal systems for remote support and maintenance)
  - abuse of remote maintenance ports
  - abuse of administrator rights
- Unauthorized disclosure of sensitive data by service provider
  - lack of respect for intellectual property rights,
  - lack of separation of multi-customer environments
  - lack of information security best practices (for example, password sharing may be rampant),
  - mis-handling of storage media
  - use of non-secure communications methods,
- Introduction of malware (in software development environments)
  - inadequate security in software development and software release procedures,
  - insecure transfer of files and data,
  - insecure online collaboration practices
- Lack of legal or regulatory compliance
  - lack of understanding of country specific regulatory and liability laws if the service provider is based in a different country
  - Insufficient legal data privacy and protection requirements applicable in the country where the supplier is located. It may have a substantial adverse effect on the data privacy and protection requirements applicable to the acquirer.

15.3 Security design techniques and controls

Information security design techniques and controls related to external or outsourced IT support services are associated with:

The first step of conducting an in-depth risk assessment of an outsourcing partner prior to execution of any contract, with the outsourcing partner assessed for its:

Table 11 — Security Controls for Outsourcing Services

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies** (implementation can be assumed by the outsourcing organization or outsourced enterprise depending on statement of work)
Unauthorized Access to internal systems	
• Access Control • Authentication	• Strict assignment of individual user ids • Strong authentication (e.g., two-factor authentication) for

Applicable Security Properties for Identified Threats	**Implementation Design and Technologies** (implementation can be assumed by the outsourcing organization or outsourced enterprise depending on statement of work)
• Non-Repudiation	root/admin login • On-site console port or craft port protected by userID and password (in case service provider requires on-site physical access) • Comprehensive logging of access activities, and log reviews
Unauthorized Disclosure of Sensitive Data	
• Confidentiality	• Client data protection best practices through encryption • Security awareness and training • Monitoring and audit facilities and procedures • Contractual security policy and procedures directives
Introduction of malware	
• Integrity	• Secure coding practices • Change management processes • Ensure that anti-virus updates are automatically installed or the user is alerted to the fact that updates are available
Legal or regulatory liabilities	
• Confidentiality • Opacity	• Awareness of local regulations • Use of compliant encryption software • Opacity mechanisms (IPsec VPNs)

1 1

Annex A
(informative)
An Example Internet Use Policy

A.1 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name>'s established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

A.2 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

A.3 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

A.4 Policy

A.4.1 General Use and Ownership

1. While <Company Name>'s network administration desires to provide a reasonable level of opacity, users should be aware that the data they create on the corporate systems remains the property of <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company Name>.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.
4. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.
5. <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

A.4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly, user level passwords should be changed every six months.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the “Laptop Security Tips”.
6. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.
7. All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company Name>, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

A.4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

A.4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any <Company Name> account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

A.4.3.2 Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

A.4.4 Blogging

1. Blogging by employees, whether using <Company Name>’s property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of <Company Name>’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate <Company Name>’s policy, is not detrimental to <Company Name>’s best interests, and does not interfere with an employee's regular work duties. Blogging from <Company Name>’s systems is also subject to monitoring.
2. <Company Name>’s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any <Company> confidential or proprietary information, trade secrets or any other material covered by <Company>’s Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of <Company Name> and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or

otherwise engaging in any conduct prohibited by <Company Name>'s Non-Discrimination and Anti-Harassment policy.

4. Employees may also not attribute personal statements, opinions or beliefs to <Company Name> when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of <Company Name>. Employees assume any and all risk associated with blogging.
5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, <Company Name>'s trademarks, logos and any other <Company Name> intellectual property may also not be used in connection with any blogging activity

A.5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A.6 Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

A.7 Revision History

Annex B
(informative)
Catalogue of Threats

B.1 Misrepresenting Authority & Rights:

- Presentation of a false authority as if it were true with the intent to mislead.
- Presentation of a password, key or certificate of another (e.g., system administrator).
- Unauthorized acquisition and use of subscriber service-related authentication information (e.g., user id/password, session keys). Limited to individual subscribers.
- Unauthorized acquisition and use of administrative authentication information (e.g., user id/password).
- Replay attacks involving signaling.

B.2 Theft of Service:

- Unlawful taking of a benefit of a service provider intended to deprive the service provider of lawful revenue.
- Defrauding service provider.
- Unauthorized deletion or alteration of billing information.
- Device cloning.
- Circumvention of conditional access systems (CAS).
- Massive replication/dissemination of information enabling theft of service.

B.3 Invasion of Subscriber Privacy and Eavesdropping:

- Call Pattern Tracking to discover identity, affiliation, presence and usage.
- Traffic Capture - unauthorized recording of traffic including packet recording, packet logging and packet snooping. Includes mangement and signaling traffic.
- Unauthorized access to subscriber media stream.
- Unauthorized access to operations, administration, management & provisioning (OAM&P) traffic.
- Unauthorized access to signaling traffic.
- Information Harvesting - unauthorized means of capturing identity that enables subsequent unauthorized communication and theft of information. Consists of the collection of IDs, which may be numbers, strings, URLs, etc.
- Media Reconstruction - unauthorized monitoring, recording, storage, reconstruction, recognition, interpretation, translation, and/or feature extraction of any portion of a video communication including identity, presence or status.
- Unauthorized disclosure of subscriber service capabilities.
- Unauthorized disclosure of subscriber's previous or current usage or activities (e.g., subscriber viewing history of broadcast or VoD content, on-line gaming activities, etc.).
- Replay attacks involving media (re-playing captured media for malicious gains, or invading privacy by replaying media for personal use).

B.4 Interception & Modification:

- Conversation Impersonation & Hijacking - the injection, deletion, addition, removal, substitution or replacement or other modification of any portion of a communication with information that alters any of its content and/or the identity, presence or status of any of its parties. Includes management and signaling traffic.
- Unauthorized access, modification or deletion of digital information.
- Hijack data stream; insertion, modification and deletion data stream in an unauthorized manner.
- Any form of SPAM.
- Unauthorized transmission of material (for political or other reasons).

B.5 Traffic/Packet Flooding:

- DoS attack on a user endpoint by sending a large number of valid packets causing interruption of service, some of which may impact network elements as well. Application stops due to overload.
- Endpoint packet flooding scenarios cause network element, or server to crash, reboot, or exhaust all resources.
- DOS - bandwidth consumption or resource consumption; high volume of traffic (e.g., to a multicast group).
- Potentially impacting thousands of subscribers (e.g., DSLAMs, servers that support thousands of subscribers).

B.6 Malformed Packets & Messages:

- Disabling Endpoints with Invalid Messages - DoS attack on the endpoint (e.g., server) by sending a number of invalid messages that could cause the endpoint to crash, reboot, or exhaust all resources.
- Malformed Protocol Messages - sending of malformed protocol messages (e.g., messages with overflow or underflow) to the device that degrades its performance to the point of being unable to process normal messages.
- Malformed messages that cause buffer overflow.
- Potentially impacting thousands of subscribers (e.g., servers that support thousands of subscribers).

B.7 Spoofed Messages:

- DoS attack that disrupts service by causing a session to end prematurely.
- Spoofing of control messages. Malicious control traffic - injected into the communications causing applications or servers to malfunction or traffic sent to the wrong destination. Forged control messages used to alter the structure of multicast distribution trees and affect the data distribution across them. DOS - bogus broadcast message claiming there is a high loss rate on the channel or high congestion; source will reduce the transmission rate affecting other subscriber.
- Forged end-use messages and application or server responses.
- Change IP and MAC addresses to spoof other users MAC and IP address to capture data streams.

B.8 Underlying Platform DoS:

- Vulnerabilities of the underlying operating system or firmware that the application or service runs on.
- "Point-and-shoot" exploits freely available for download on the Internet.
- DoS attacks which reduce the device's performance.

Exploitation of these vulnerabilites has the potential to propagate to thousands of devices (e.g., client devices). Potentially resuting in redeployment of or maintenance to thousands of devices.

B.9 Compromise of Installed Software, Service-Related Data, or System Configuration:

- Malware, spyware, rootkit insertion.
- Unauthorized duplication, installation, alteration of deletion of production software and configuration files.
- Unauthorized duplication, disclosure, creation, modification, or deletion of service-related data (e.g., system logs, billing information, decryption keys, storage containers for decryption keys, etc.).
- D-DoS using compromised devices to crash the service.
- Unauthorized creation or modification of subscriber service-related information (e.g., authentication info, session keys).
- Unauthorized or unnecessary activation/deactivation of logical (protocol) ports.

B.10 Resource Exhaustion:

- Deficiencies in software or hardware that cause depletion of memory resource (e.g., buffers) in a system.
- Deficiencies in software or hardware that consumes most of CPU resources in a system.
- Hardware or software errors that limit available bandwidth of a communication link.
- Deficiencies in software or hardware that generate unnecessary messages reducing bandwidth resources.
- E.g., infinite software loops, routing loops.

B.11 Unauthorized Network Scans and Probes:

- Port scanning/ping sweeps. Attacker can run publicly available scanning software on host that has connectivity to the network. Host services on devices monitoring the ports will respond, potentially providing information to the attacker.
- Vulnerability scanning (e.g., nessus), network mapping (e.g., NMAP). Attacker can run publicly available software on host that has connectivity to the network that queries the device configuration and network topology.
- Unauthorized remote access to software or functions resident on the device (e.g., utilizing a rootkit to provide a backdoor).

B.12 Compromise of Subscriber Application Data:

- Unauthorized disclosure, creation, modification, duplication, deletion of data created and/or used by subscriber-accessible applications.
- Includes information stored in the Service Provider's network on behalf of subscribers (e.g., video content recorded by nDVR).

B.13 Theft of Content:

- Capturing digital certificate to order content and even broadcast/redistribute the stream to other subscribers.
- Packet capture on home network and IP subnet.

- Output from an analog output port to an external recording device.
- Output from a digital port to an external recording device.
- Implement playing more than then number of allowed plays.
- Accessing illegitimate content (e.g., pirated content).
- Circumvention of conditional access systems (CAS).
- Copying content from disk storage on server or end-user device.

B.14 Access to Inappropriate Content:

- Accidental access.
- Deliberate access.

B.15 Compromise of Subscriber Information:

- Social engineering to obtain subscriber information.
- Unauthorized disclosure, creation, modification, duplication or deletion of subscriber information (e.g., address, phone no., account no., credit card info, DNS/ENUM entries, etc.).
- Limited to individual subscribers.

B.16 Session Hijacking and Service Masquerading:

- Impersonation of legitimate service provider. Capturing digital certificate from provider to modify streams and include any information they want.
- Impersonation of legitimate network device, video server, gaming server, DRM server.
- Man-in-the-Middle attack.
- Redirection of video stream to unauthorized device.

B.17 Unauthorized Management:

- Unauthorized use of on-board management application or execution of management commands. For example, manipulation of modem configuration to block specific services.
- Forged/modified management protocol messages. For example, manipulation of modem configuration to block or allow specific protocols (e.g., SNMP).
- Modification of remote managment messages (e.g., MITM).
- Illegitimate subscriber self-provisioning actions. For example, reconfiguring STB to remove bandwidth limitations in order to produce slow connections for other subscribers or increase bandwidth for yourself.
- Authorized management agent performing unauthorized activities.
- Unauthorized content management; e.g., loading, deleting content or modifying the trigger date (the date that content becomes available to the viewing public).
- Unauthorized subscriber management; e.g., unauthorized subscriber provisioning activities including upgrade/downgrade of subscriber viewing privileges.