International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 3

(04/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security

ITU-T X-series Recommendations – Supplement 3

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339

For further details, please refer to the list of ITU-T Recommendations.

Supplement 3 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security

Summary

Network security is designed around a strong security framework, available tools, and standardized protocols. In complex multi-vendor environments, standards-based security solutions can ensure interoperability and operational efficiencies in realizing end-to-end security. Network providers depend upon security information available to them to help plan, design and implement and maintain their networks in order to meet the security objectives. Standards-based systematic methodology and guidelines identify and address critical security challenges of network and information security.

This supplement establishes guidelines for implementing system and network security with a focus on telecommunications networks. This supplement provides security guidelines for critical activities during the network life-cycle. These guidelines address four areas: 1) technical security policy, 2) asset identification, 3) threats, vulnerabilities and mitigations, and 4) security assessment. The guidelines and associated templates help in systematically addressing the security of networks.

Source

Supplement 3 to ITU-T X-series Recommendations was agreed on 18 April 2008 by ITU-T Study Group 17 (2005-2008).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

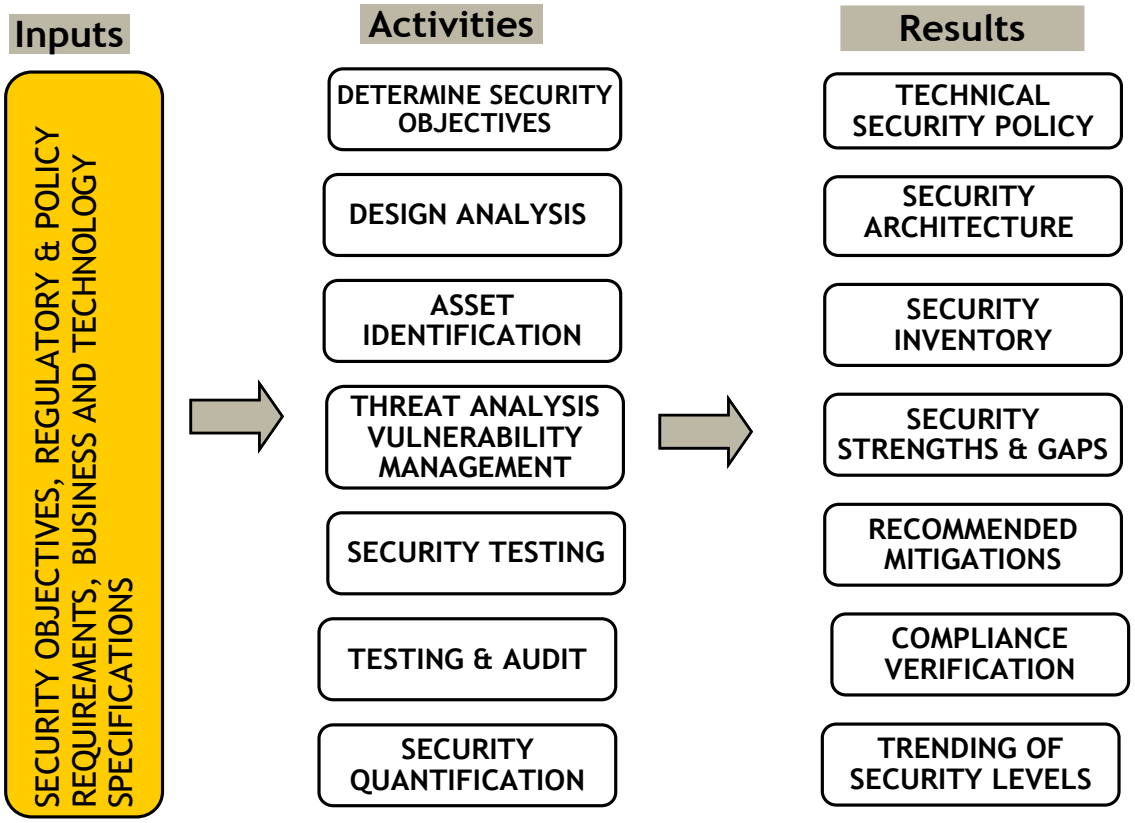
ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

Network security is designed around a strong security framework, the available tools, and standardized protocols. In complex multi-vendor environments, standards-based security solutions can ensure interoperability and operational efficiencies in realizing end-to-end security. Network operators depend upon key security information to plan/design, implement and maintain secure networks to meet the organization's business and technical goals. The figure below shows the key security activities and associated results needed during the security life-cycle. Standards-based systematic methodology and guidelines help in identifying and addressing critical security information challenges of systems and networks. A systematic assessment can provide a baseline of the current level of security and mitigations that are required to support the security life-cycle.



This supplement establishes guidelines for implementing system and network security with a focus on telecommunications networks. This supplement provides security guidelines for critical activities during the network security life-cycle. These guidelines address four areas: 1) technical security policy, 2) hierarchical-asset identification, 3) threats, vulnerabilities and mitigations based on hierarchical assets, and 4) security assessment. The guidelines and associated templates will help in systematically addressing the security of networks.

1) *Guidance to organizations on technical security policies*

This clause describes the value of a security policy and provides guidance on the components of a technical security policy. Recommendation ITU-T X.1051| ISO/IEC 27011 provides details of ISMS security policy. This supplement leverages existing standards on security policy to build and manage the technical policy. The guidelines in this supplement show key components required to build and continuously manage the technical policy.

2) *Guidance on hierarchical-asset identification*

Guidelines are provided on how to comprehensively identify assets that need to be protected. These guidelines can be used to identify critical security assets regardless of the technology or industry vertical.

3) *Guidance on understanding threats, vulnerabilities and mitigations*

Guidelines on how to identify potential threats to the assets are provided. As part of the threat analysis, guidelines on recognizing the potential vulnerabilities within the hierarchical-assets and the resulting impact of potential threat materialization are provided in this clause. It is important to also recognize the mitigations needed and their implementation priority.

4) *Guidance on security assessments*

Guidelines are provided on network security assessment in the three stages of the security life-cycle that are shown in Figure 1. Securing activities related to management, control and users for the network infrastructure, services and applications is the focus of this clause. The assessment guidelines cover plan/design, implementation and maintenance phases of a system or network life-cycle. It leverages the guidelines and results from technical policy, hierarchical-asset identification, and threat/vulnerability mitigation guidelines to secure a network.

Benefits of system and network security implementation guidance:

The industry needs a uniform set of security guidelines that can be consistently applied to relevant phases of system and network life-cycle to realize the following benefits:

- A common approach leads to shared understanding and interoperability in multi-supplier networks.
- An identification of hierarchical assets and what is needed to protect them.
- A consistent way to look at threats, vulnerabilities for products, regardless of technology.
- A systematic analysis assures efficient coverage of network security.

Supplement 3 to ITU-T X-series Recommendations

ITU-T X.800-X.849 series – Supplement on guidelines for implementing system and network security

1 Scope

This supplement provides system and network security implementation guidelines. These guidelines can be utilized to realize a network security program. The guidelines are applicable to management, control, and user activities to secure assets belonging to infrastructure elements, network services and applications. These guidelines are independent of the underlying technology and focus on telecommunications networks security. This supplement focuses on four different areas as described in the paragraphs below:

1.1 Guidance to organizations on technical security policies

This clause shares the need and value of a security policy and then provides guidance on the components needed for a technical security policy. [b-ITU-T X.1051] provides details of ISMS security policy. This supplement leverages existing standards on security policy to build and manage the technical policy. The guidelines in this supplement show key components required to build and continuously manage the technical policy.

1.2 Guidance on hierarchical-asset identification

Guidelines are provided on how to comprehensively identify assets that require protection. These guidelines can be used to identify critical security assets, regardless of the technology or industry vertical.

1.3 Guidance on understanding threats, vulnerabilities and mitigations

Guidelines on identifying potential threats to the assets, recognizing the potential vulnerabilities within the assets, and the resulting impact and mitigations of potential threat materialization are provided in this clause. These guidelines leverage the policy and hierarchical-asset identification.

1.4 Guidance on security assessments

Guidelines are provided on network security assessment for three stages of the life-cycle, which include the planning and definition, design and implementation and maintenance phases. Securing activities related to management, control and users for the network infrastructure, services and applications is the focus of this clause. In this clause, the assessment addresses the implementation of policy, hierarchical-asset identification, and threat/vulnerability guidelines and baselines of the security of the system or network.

The selection of protocols for specific technologies is not within the scope of this supplement. Protocol details are covered by other Recommendations and standards. This supplement does not cover all aspects of the security life-cycle, including product end-of-life. Security domain experts, depending on the operating environment and objectives, will have to select the relevant Recommendations and standards. The guidelines in this supplement, together with the domain expertise, will help in achieving comprehensive security.

2 References

None.

3 Definitions

This supplement uses the following terms defined elsewhere:

3.1 attack [b-ITU-T H.235.0]: The activities undertaken to bypass or exploit deficiencies in a system's security mechanisms. By a direct attack on a system they exploit deficiencies in the underlying algorithms, principles, or properties of a security mechanism. Indirect attacks are performed when they bypass the mechanism, or when they make the system use the mechanism incorrectly.

3.2 information asset [b-ISO/IEC 13335-1]: An information asset is defined as a physical or logical (tangible or intangible) entity that is of value to an organization or institution and characterized by the following: Anything that has value to the organization.

3.3 threat [b-ISO/IEC 13335-1]: A potential cause of an unwanted incident that may result in harm to a system or organization.

3.4 vulnerability [b-ISO/IEC 13335-1]: A vulnerability is any weakness that could be exploited to violate a system or the information it contains.

4 Abbreviations and acronyms

This supplement uses the following abbreviations and acronyms:

DMZ Demilitarized Zone

EDI Electronic Data Exchange

IDS Intrusion Detection System

OAM&P Operations, Administration, Maintenance and Provisioning

TSSR Technology Specific Security Requirements

5 Conventions

None.

6 Guidelines phases

This clause describes the guidelines and how they can be built and leveraged from one phase to another phase of the security life-cycle.

6.1 Security integration into product and systems life-cycle

A complete and cost-effective security solution can be achieved by a comprehensive approach to security, where security is implemented in every step of the product life-cycle: from concept to development to ongoing maintenance. Figure 1 shows the key steps in the security life-cycle and the activities.

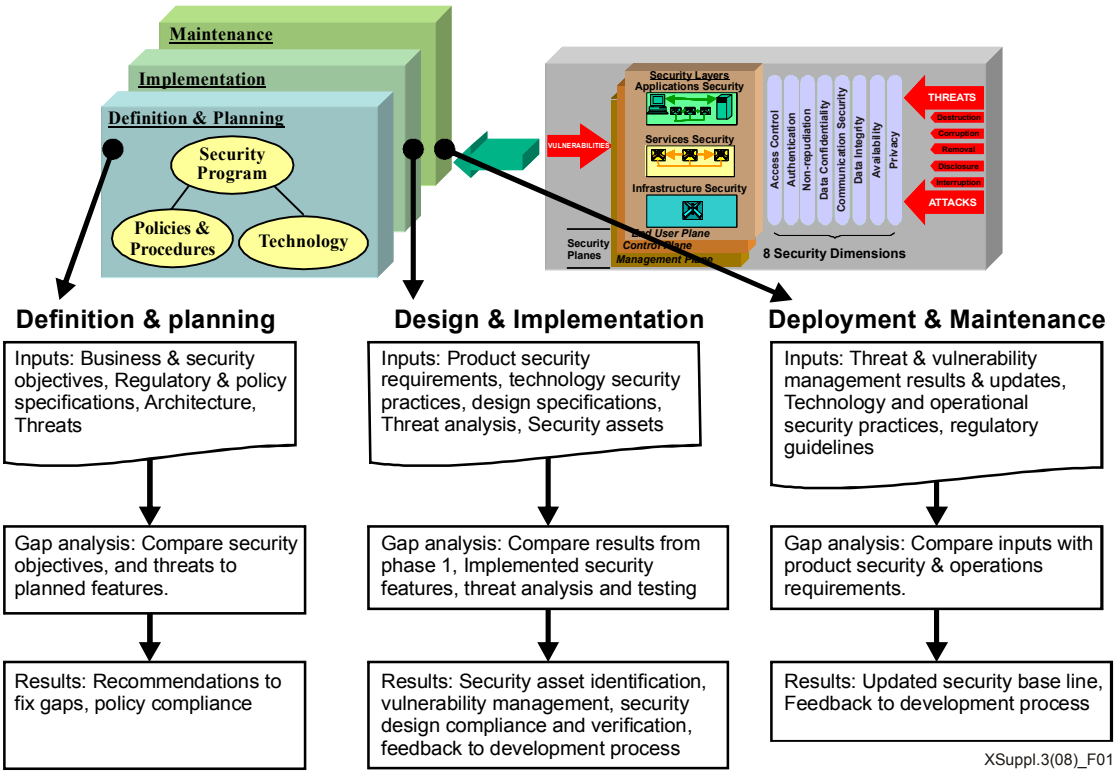


Figure 1 – Network security life-cycle

This supplement presents a technology-agnostic approach to integrating security into the program life-cycle. This supplement leverages existing ITU-T Recommendations and other applicable security standards. These include other ISO, IETF, standards. An example is the security framework [b-ITU-T X.805] that can be used in conjunction with other standards and industry best practices for integrating security in every phase of the development life-cycle.

6.1.1 Definition and planning phase

The definition and planning phase covers guidelines for network security planning and the definition. Analysis of business and security objectives, regulatory and policy specifications, architecture and definition of threats will be part of this phase. This includes:

- Reviewing initial business goals, security policy.
- Analysing the network/solution's security requirements.
- Translating the regulatory and policy requirements into relevant security features.
- Defining security interoperability requirements for network integration.

6.1.2 Design and implementation phase

The design and implementation phase covers the methodology and guidelines required to enable network security implementation. The analysis and results from the definition and planning phase need to be closely tracked to confirm that they are undertaken in the implementation phase. Test results include those from third party or enterprise internal vulnerability testing, security analysis/interview results of the technology specific security requirements (TSSR). Examples of security requirements can be found in [b-ITU-T M.3016.1]. Other technology-specific requirements can be derived from existing standards, such as IETF, ISO. For example, IPSec or encryption requirements can be found in the IETF.

Results from the planning and definition phase are leveraged to develop the guidelines in this phase. This includes:

- Traceability of planning and definition requirements with that of the design and implementation features. This leads to the identification of gaps in planned vs implemented view.
- Input for threat analysis, vulnerability and mitigation of design and implementation.
- Establish security baseline for the current implementation.

6.1.3 Deployment and maintenance

This clause covers the guidelines that can be used to provide consistent network security during the deployment and maintenance phase. This clause does not provide guidelines for deployment itself. The analysis and results from the design and planning phase need to be closely tracked in this phase. Updated TSSRs, standards, testing, and audit results are leveraged to develop guidelines in this phase. This includes:

- Testing and tracking security levels.
- Identifying threats and vulnerability management.
- Input to other phases of the security life-cycle.

6.2 Guidance to organizations on technical security policies

The security policy translates the security goals into organizational, process, high-level and detailed technical security requirements. The technical security policy drives the security life-cycle and the implementation of security across the system/solution life-cycle as shown in Figure 2.

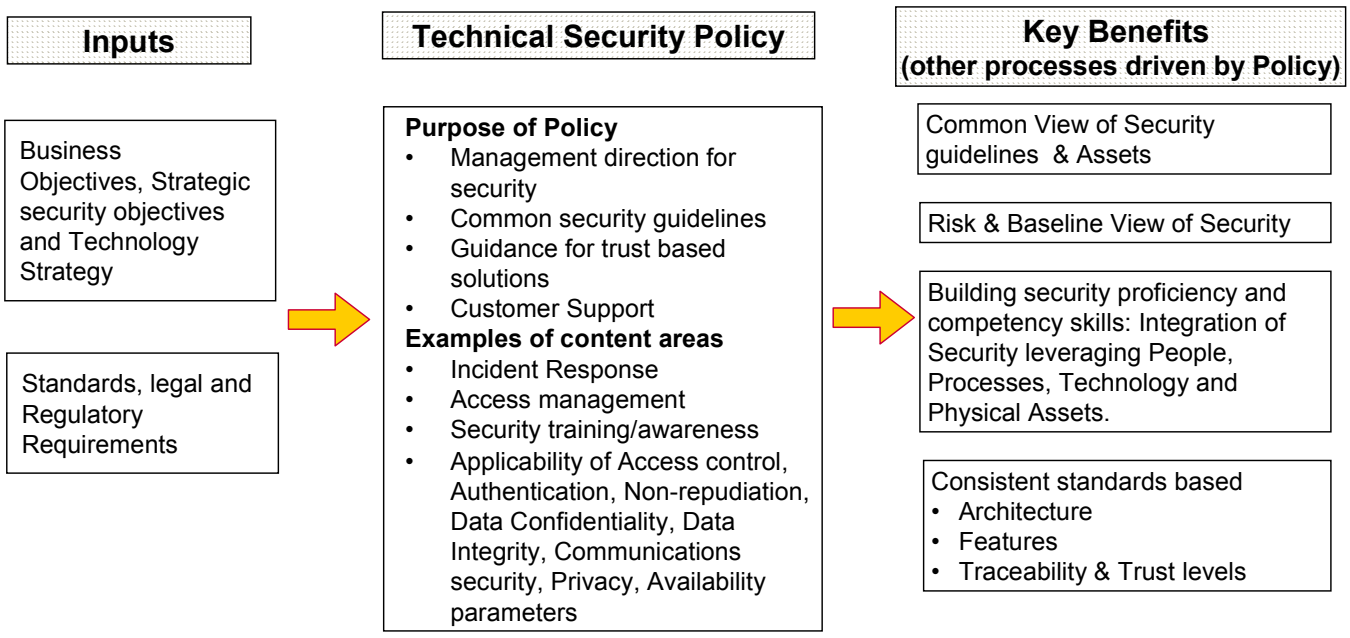


Figure 2 – Policy and impact on network security

[b-ITU-T X.1051] provides details of ISMS security policy. This supplement leverages existing standards on security policy to build and manage the technical policy. The guidelines in this supplement show key components required to build and continuously manage the technical policy. The technical policy helps establish requirements to manage networks that potentially span across multiple operators and contain products and systems from multiple vendors. It also provides

guidelines on regulatory issues. In particular, technical policies are needed to address security and management in network deployments where decisions require rapid access to relevant, accurate and timely network or system status information and other data.

For simplicity, the terms "policy" and "technical policies" are used here generically to refer to both the high-level statements of management intent, as well as the more detailed guidance/requirements that the organization has adopted in order to implement those statements. These more granular layers of policy are often referred to as "standards" or "control standards", "technical baselines" or "minimum baseline standards" and "procedures".

It is important to address security capabilities systematically for:

- Management activities (e.g., management traffic) for infrastructure, services, applications assets.
- Control activities (e.g., session traffic) for infrastructure, services, applications.
- User activities (e.g., bearer traffic) for infrastructure, services, applications.

The security implementation mechanisms define the technical policy requirements that need to be evaluated in the area of access control, authentication, non-repudiation, data confidentiality, communication security, integrity, availability, and privacy. The technical security policy will provide input to the different phases of the security life-cycle, including the definition of technical security requirements, asset and threat analysis and mitigation. Key areas of a technical security policy are listed below.

6.2.1 Managing the security technical policy

Executive management endorsement of the charter, authority, and structure of network and system security need to be covered in this clause. Network and system security policy has the charter to develop, implement, maintain and communicate details of a comprehensive security program to protect the access control, authentication, data confidentiality, data integrity, communication security, non-repudiation, privacy, and availability of the network/system/ organization's network and system resources. This clause of the policy supports the development of security features.

6.2.2 Risk management policy

Appropriate technical security controls need to be built into the company's network and system resources. This protection should be commensurate with a resource's value to the corporation, as determined by the results of a formal risk assessment. This clause of the policy definition includes: network and system ownership which include information owners, resource administrators, information users, addressing:

- Network and system assets, identification, and classification which includes asset identification, asset classifications labels.
- Risk assessments which includes, risk assessment process, inventory of network and system resources, initial risk assessment, re-evaluation process, security baselines.
- Security of media which includes, media: handling and labelling, copying, distribution, storage, transport, disposal and printing.

6.2.3 Security policy for 3rd party suppliers

Network and system security controls need to be implemented for the software and hardware developed by a third party. Contracted third-party company representatives need to be appropriately interviewed and selected, made aware of their network and system security responsibilities, properly disciplined for security violations, and have access privileges adjusted/removed upon changes in job status to ensure data integrity and access control. The policy definition should include: environment controls, worker screening, user acknowledgement of security awareness, separation of duties, critical functions to be separated, network and system

security responsibilities, confidentiality agreements, information security training, third-party compliance and security policies, secure coding and testing. The technical policy of this clause provides input to the planning and definition phase to develop the technical security requirements.

6.2.4 Physical security policy

Company facilities and network and system resources need to have appropriate physical access controls in place to protect them from unauthorized physical access. These access controls include, designated authentication, and non-repudiation built into them. Network and system processing facilities need to be safeguarded against reasonable environmental hazards.

The definitions of the policy include: security of computing and other facilities, entry to facilities, property removal and tracking, power supply, off premises equipment security. The technical policy of this clause provides input to the planning and definition phase to develop the technical security requirements.

6.2.5 Operations management policy

Personnel responsible for management of infrastructure assets, network services and applications need to follow formal operational and change control procedures to protect data integrity and access control. Company workers should be granted the minimum level of access privileges required to perform their job functions. Additionally, job duties should be separated in accordance with an individual's role and responsibilities. This clause of the policy definition should include: operational and management controls, network system resource configuration, documentation, logs, virus prevention, testing, backup and restore, software updates, patch management, etc. The technical policy of this clause provides input to the planning and definition phase to develop the technical security requirements.

6.2.6 Security monitoring and response policy

Network and system resources need to be monitored to detect system, security, and operational events to protect access control, data integrity, and availability. Formalized incident response and investigation procedures should ensure a timely response to network and system security incident. The policy definitions of this clause should include: network/system monitoring, logs, IDS, communications, review/audit of monitoring, incident reporting and management. The technical policy of this clause provides input to the planning and maintenance phase to develop the technical security requirements.

6.2.7 Communications management policy

Exchange of data between the company and other organizations needs to be protected by adequate controls to ensure confidentiality and communications security. Communication resources should be used for business purposes only. The policy definitions of this clause include: use of encryption, digital signatures, key management, electronic data interchange (EDI), such as e-mail, Internet, acceptable usage criteria for resources and data, voice communications, etc. The technical policy of this clause provides input to the planning and design phase to develop the technical security requirements and security features.

6.2.8 Access management policy

To ensure stringent access control and authentication, individuals and processes need to be positively identified, authenticated, and authorized prior to being granted access to the network and system resources. Non-repudiation mechanisms are needed to determine any unauthorized access. Access should be based on an individual's role and limited to the minimum necessary to perform their job function. Access to network and system resources should be controlled through a managed process that addresses access controls, authentications, modifying and revoking privileges, and periodic review of network and system usage and access privileges. The policy definitions of this clause include user enrolment, authorization, access privileges, user identification, passwords,

authentication and access control features, remote access, password change controls, logs, firewalls, etc.

6.2.9 Third-party services policy

Third parties need to follow the company's network and system security policy and supporting processes when contracted by the company, and acknowledge their responsibility through a formal written statement. Company workers involved in using third-party suppliers need to adhere to the company's network and system security policy for such arrangements. The policy definitions of this clause include: security requirements for 3rd party and contractor, monitoring contract and access controls for 3rd party for network, system and facilities. The technical policy of this clause provides input to the planning and maintenance phase to develop the technical security requirements and security features.

6.2.10 Application/services and infrastructure development policy

Application/services and infrastructure development activities need to follow a development methodology that incorporates network and system security controls into each stage to protect integrity. The policy definitions of this clause include:

- Application/services development process, methodology, development environment access to program source library, risk assessment, restrictions on changes to software packages.
- System business requirements, design, design exceptions, input data validation, message authentication, application auditing/logging, common security requirements, common vendor requirements.
- Application/services testing, application/services review, acceptance testing criteria, protection of system test data.
- Secure coding practices, adherence to secure coding practices avoiding buffer overflows, network security validation, network security scanning.

6.2.11 Disaster recovery and business continuity policy

The critical network and system resources need to have formally developed recovery plans that provide for the prompt and effective continuation of critical network and system services in the event of a disaster to ensure availability and data integrity. The policy definitions of this clause include:

- Business continuity management process, roles and responsibilities, business continuity planning framework, business continuity impact analysis, business continuity plan development, annual inventory.
- Recovery/business continuity plan testing, documentation of plan testing, testing requirements for highly critical systems, testing requirements for moderately critical systems, third-party testing.
- Recovery sites, hot recovery sites.

6.2.12 Legal, compliance and regulatory policy

All technical personnel should comply with the relevant national and local legal, regulatory and contractual requirements to ensure data confidentiality and integrity through compliance testing. The policy definitions of this clause include:

- Legal/regulatory requirements, intellectual property rights, safeguarding of organizational records, privacy of personal information, customer privacy.
- Security compliance testing, testing concepts and process, testing results, compliance tools.
- Country and industry specific compliance requirements.

6.3 Guidance on hierarchical-asset identification

This clause describes a method to identify assets in a systematic way so that all the security assets are identified. The guidelines in this clause can be used to identify critical security assets regardless of the technology or industry vertical.

Identification of assets is a critical step in securing a system and/or network as it provides business and technical insights, such as: 1) how valuable the asset is to the organization relative to the protection needed, 2) what are the critical assets, 3) what should be protected, 4) what business continuity plans need to be put in place for the assets. Assets required to securely support management, control and user traffic and the features required for the functioning of the network infrastructure, services and applications are the focus of this clause.

The assets include hardware, software, interfaces (internal and external), information stored/processed, and protocols used.

The process of asset identification needs to determine the components in a hierarchical structure starting with applications/services, infrastructure that supports management, control and user activities/data as described below:

6.3.1 List of the applications and services being analysed

The list of assets includes applications and services that are supported for local feature functionality, as well as those required to support applications which are part of system/networks element. Examples of telecommunication applications and services include, e-mail, broadcast/multicast of media, VPN, and VoIP, etc.

6.3.2 List of the infrastructure being analysed

The list of assets includes all the infrastructure elements that are a part of the network/system being inventoried. Examples of telecommunication assets include, DSLAM, routers, switches, management platforms, firewalls, etc.

6.3.3 Sub-assets for services and applications

The services and applications in clause 6.3.1 indicate higher level assets. These assets contain more granular objects or sub-assets as defined in this clause.

For each of the services and applications in clause 6.3.1, identify the relevant:

- Management, control or end-user data generated or used by the service/application.
- Management, control or end-user information flows and protocols used by the service/application.
- Management, control or end-user logical ports used by the service/application.
- Software/hardware that enables the service/application (ensure it is included in the infrastructure assets).

Table 1 – Security assets of applications and services

Assets for applications/ services	Addresses management activity	Addresses control activity	Addresses end-user activity
Data used by application	Asset 1	Asset 4	Asset 7
Information flows and protocols	Asset 2	Asset 5	Asset 8
Software/Hardware	Asset 3	Asset 6	Asset 9

The security features that are in place to implement the relevant access control, authentication, non-repudiation, data confidentiality, data integrity, communications security, privacy, and availability mechanisms need to be represented by the assets identified in Table 1. One or more of these assets are associated with the security mechanisms. The numbers of assets in Table 1 is not fixed. They vary as a function of the network and system under consideration.

6.3.4 Sub-assets for infrastructure

The infrastructure elements in clause 6.3.2 indicate higher level assets. These assets contain more granular objects or sub-assets as defined in this clause. For each of the infrastructure assets in clause 6.3.2, identify the relevant:

- Management, control or end-user interfaces (physical and logical) used by the network element. This includes the network interfaces, ports, cards, memory, etc.
- Management, control services and protocols dedicated to the operation of the network elements, systems. This includes support applications, element identification/addressing information and configurations required for control and management of the network element or system.
- Software/hardware that enables the network element or system. This includes resident data bases, OS, middleware and other software required to operate the infrastructure element.

Table 2 – Infrastructure assets

Assets for infrastructure element/system	Addresses management activity	Addresses control activity	Addresses end-user activity
Physical & logical interfaces used by NE	Asset 11	Asset 14	Asset 17
Data and information flows and protocols for NE	Asset 12	Asset 15	Asset 18
Software and/or applications required for NE	Asset 13	Asset 16	Asset 19

The security features that are in place to implement the relevant access control, authentication, non-repudiation, data confidentiality, data integrity, communications security, privacy and availability mechanisms can be represented by the assets identified in Table 2. One or more assets are associated with the security mechanisms. The number of assets shown in Table 2 is not fixed. They vary as a function of the network and system under consideration.

Once the assets are identified, it will be easier to analyse the threats, vulnerabilities and mitigations to secure these assets.

6.4 Guidance for understanding threats, vulnerabilities and mitigations

This clause describes the relationship between threats, vulnerabilities and mitigations as they pertain to products, systems, networks, services, applications, solutions, etc., which are known as targets of evaluation. The guidance also describes the following five activities that are performed in order to understand and improve the security posture of the target of evaluation. The five activities are:

1) *Threat definition*: identifies industry known, field insights, circumstances, or events that have the potential to adversely impact a business, institution or individual. The result of this step produces a list of industry known threats, incidents, regulatory constraints that are applicable to the target of evaluation.

2) *Hierarchical-asset identification*: identifies information assets that need to be protected against threats. The result of this activity is a list of all assets and their role in the target of evaluation. The critical assets will also be identified (e.g., potential to have severe impact if this asset is compromised).

3) *Threat analysis*: determines the extent to which information assets are exposed to threats. The result of this activity is a list of the assets and the extent to which they are exposed to threats.

4) *Vulnerability management*: determines which actual vulnerabilities are potentially subject to threats and identifies mitigations to mitigate these vulnerabilities. The result of this activity produces a list of actual vulnerabilities that need to be mitigated.

5) *Mitigation quantification and prioritization*: assigns values to mitigations and the priority of their implementation.

Figure 3 depicts the relationship of these definitions. The rectangular objects in Figure 3 indicate entities that are outside the control of the business, institution, organization, etc. The oval objects indicate entities that the business, institution, etc., can control. As can be seen from Figure 3, the objective of the five activities described previously is to develop mitigations for vulnerabilities in order to prevent attacks against the target of evaluation.

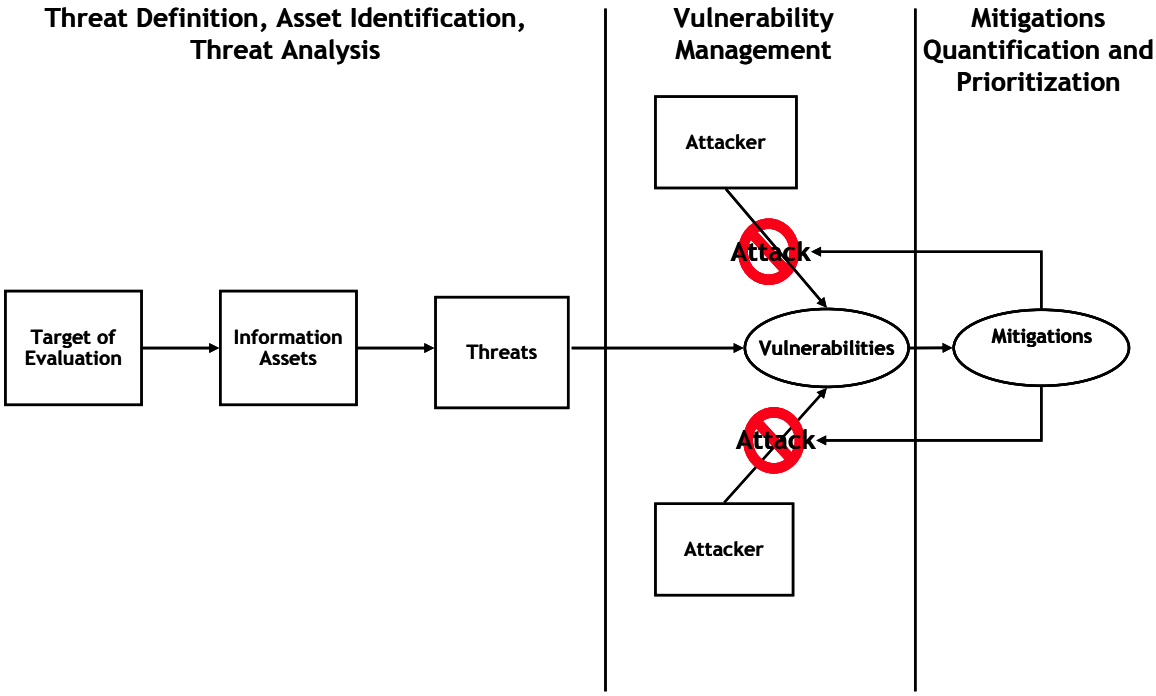


Figure 3 – Relationship of information security terms and activities

6.4.1 Threat definition

Threat definition or identification of threats consists of examining the scope of the underlying technologies and identifying the industry- and technology-specific dangers to the product, system, network, service, solution, etc., being analysed. For example, if the target of evaluation delivers content to subscribers, theft of content would be an appropriate threat to be included in the analysis (industry-specific threat). Likewise, if the target of evaluation includes a wireless or cellular component, RF jamming would be an appropriate threat to be included in the analysis (technology-specific threat). Industry and technology fora, as well as standards bodies, are

consulted as part of the threat definition process. The concepts of threats are well known and they are not described in this supplement in detail.

The result of this activity produces a list of industry known threats, incidents, regulatory constraints that are applicable to the product, solution, etc. Thus, this step will provide the answers to the following questions:

1) What are the security requirements needed to meet the business objectives?

2) What are the known threats to the industry vertical the target or evaluation is being used in?

3) What are the regulatory compliance guidelines that need to be met for the industry vertical?

4) What are the technology limitations of the target of network?

6.4.2 Hierarchical-asset identification

Information asset identification consists of identifying the target of evaluation's hierarchical-assets that need protection. The information assets can consist of a software, a system, a network, a network element, a component of a system or network element (e.g., RAM, physical/logical ports, etc.), a protocol, or sensitive data (e.g., subscriber SSNs). Information assets are extracted from technical documentation such as functional requirements specifications, product specifications, system design documents, network architecture or design documents, protocol specifications, etc.

The result of this step is the list of all information assets and their role in the product, solution, etc. The critical information assets will also be defined. Critical information assets are those assets that have potential for severe impact if compromised. Thus, this step will provide the answers to the following questions:

1) What are the distinct types of network equipment and facility groupings that need to be protected?

2) What are the distinct types of network activities that need to be protected?

The combination of the previous activities provides a list of threats based on industry vertical and the inventory of information assets. Clause 6.3 describes the methodology to identify information assets.

6.4.3 Threat analysis

A threat analysis determines the extent to which an information asset is exposed to each threat identified in the first activity. It consists of applying a standardized or industry-recognized threat types (e.g., X.800 threat types) to the information assets in order to determine the susceptibility of each asset to the identified threats. The information assets are analysed in the context of the applicable threats. As an example, if a CD-ROM containing employee SSNs (information asset) is stolen (X.800 theft threat type), identity theft (identified passive threat) could result.

The actual determination of whether the threat could be exploited in the form of an attack is made in the vulnerability management activity described below. Continuing the CD-ROM example, the vulnerability analysis would examine the CD-ROM custodial procedures and make a determination if the CD-ROM is vulnerable to being stolen.

The result of this activity is a summarized list of threats that will impact the information assets. Thus, by performing this clause, the following questions will be answered:

1) What are the threats that can impact each information asset?

2) How is the information asset exposed to the threats?

A threat analysis can be performed by filling out the applicable portions of the following template for each information asset.

Table 3 – Template for determining threats to identified assets

Asset ID	Asset name	Description	Threat(s)
1.0	Asset #1		Threats for Asset #1
Threat model (e.g., X.800)	Corruption	Describe how Asset #1 can be corrupted.	Threat(s) realized if Asset #1 is corrupted.
	Destruction	Describe how Asset #1 can be destroyed.	Threat(s) realized if Asset #1 is destroyed.
	Theft/Removal	Describe how Asset #1 can be stolen/removed.	Threat(s) realized if Asset #1 is stolen/removed.
	Disclosure	Describe how Asset #1 can be disclosed.	Threat(s) realized if Asset #1 is disclosed.
	Interruption	Describe how Asset #1 can be interrupted.	Threat(s) realized if Asset #1 is interrupted.

6.4.4 Vulnerability management

Vulnerability management identifies mitigations for information assets that are exposed to threats. The analysis of the underlying implementation, as well as cross-layer co-implementation of mitigations, is used to reduce the number of mitigations necessary to provide adequate security. For example, if a portion of the threat, vulnerability results is for UMTS which provides encryption across the air link using the KASUMI algorithm, no additional mitigations are necessary in order to protect against eavesdropping on the air link in the infrastructure layer. Another example is if the IPSec ESP protocol is specified to provide end-to-end security of an information flow across the services layer, then no additional encryption mitigations may be required for that information flow at the infrastructure layer.

The result of this activity produces a list of actual vulnerabilities that need to be mitigated. Thus, by performing this clause, it will answer the questions:

1) What are the actual vulnerabilities in the information assets that could be exploited by an attacker?

2) What mitigations are missing and need to be deployed?

Vulnerability management can be performed by filling out the following template for each information asset. Factors, such as avenue of attack, method of attack, and impact of attack, need to be taken into account when filling in the vulnerabilities column for each information asset in the applicable portions of the template below. Avenue of attack means the conduit an attacker would take in order to reach the information asset in order to form the attack. Method of attack means the types of tools, techniques, etc., that an attacker would use in performing the attack. The impact of the attack means the results a successful attack would have on the asset.

When filling out the mitigations column, factors, such as the security capabilities inherent in the information asset's underlying technology, physical location in the solution (e.g., DMZ), compensating security capabilities already identified for higher layers (e.g., IPSec), need to be taken into account.

Table 4 – Template for determining vulnerabilities to identified assets

Asset ID	Asset name	Vulnerability description	Mitigations
1.0	Asset #1		Roll-up Mitigations from below
	Vulnerability #1	Describe Vulnerability #1	Mitigations to prevent the exploitation of Vulnerability #1.
	Vulnerability #2	Describe Vulnerability #2	Mitigations to prevent the exploitation of Vulnerability #2.
	Vulnerability #3	Describe Vulnerability #3	Mitigations to prevent the exploitation of Vulnerability #3.
	Vulnerability #4	Describe Vulnerability #4	Mitigations to prevent the exploitation of Vulnerability #4.
	Vulnerability #5	Describe Vulnerability #5	Mitigations to prevent the exploitation of Vulnerability #5.

6.4.5 Mitigation quantification and prioritization

The objective of mitigation quantification and prioritization is to determine the order in which the mitigations are to be implemented. A mitigation value is calculated using a technique that is typically a function of the asset's attractiveness to attackers, the ease of attacking the asset's vulnerabilities, the technical impact a successful attack would have, the business impact a successful attack would have, the business priority of the associated threat, cost of implementing the mitigation, etc.

Computation of mitigation value can be done by available risk assessment techniques that are applicable to the network conditions. Examples of risk analysis are described in standards such as [b-NIST SP 800-30]. These methods assign numeric values of 1, 0.5 and 0.1 to High, Medium and Low estimates of likelihood, and impact. This supplement does not recommend assigning such fixed values. They should be determined by the telecommunication network operator to suit their business objectives.

The result of this activity produces a prioritized list of mitigations that need to be implemented. Thus, by performing this clause, the following questions will be answered:

- What kind of protection is needed and against what threats?
- What mitigations are critical and need to be implemented now?

Mitigation quantification and prioritization can be performed by filling out a template similar to the one below for each mitigation that was defined. Examples of security mechanisms or mitigations can be found in [b-ITU-T M.3016.3]. Other technology-specific requirements can be derived from existing standards such as IETF, ISO. As can be seen from the template, example factors to be taken into consideration when quantifying a mitigation include attractiveness of the asset to attack, frequency that the asset will be attacked in the absence of the mitigation, impact of a successful attack against the asset exploiting the lack of the mitigation, and the cost of implementing the mitigation. The value of the mitigation is then seen to be a function of these parameters. Determining the values for these parameters varies from organization to organization, and there are no industry standards that can be used to determine these parameters. Typically, qualitative values such as high, medium and low are assigned to fit the business and network security objectives. The factors provided in the sample template can be added to, modified or deleted to suit the needs of the particular business, organization or institution. The function used to calculate the mitigation's value is thus unique to the business, organization or institute and can be automated, semi-automated or manual. The mitigations are prioritized based on the value resulting from this calculation.

Table 5 – Template for mitigation value calculation

Asset ID.	Asset name	Example mitigation value calculation				
		Attractiveness to attack	**Freq. of attack**	**Impact of attack**	**Cost to implement**	**Mitigation value**
1.0	Asset #1					
	Mitigation #1	Value representing Asset #1's Attractiveness to Attack.	Value representing frequency that Asset #1 will be attacked if Mitigation #1 is not deployed.	Value representing impact of attack against Asset #1 that exploits lack of Mitigation #1.	Value representing cost to implement Mitigation #1.	Function of: • Attractiveness to Attack, • Freq. of Attack, • Impact of Attack, • Cost to Implement for Mitigation #1.
	Mitigation #2	Value representing Asset #1's Attractiveness to Attack.	Value representing frequency that Asset #1 will be attacked if Mitigation #2 is not deployed.	Value representing impact of attack against Asset #1 that exploits lack of Mitigation #2.	Value representing cost to implement Mitigation #2.	Function of: • Attractiveness to Attack, • Freq. of Attack, • Impact of Attack, • Cost to Implement for Mitigation #2.
	Mitigation #3	Value representing Asset #1's Attractiveness to Attack.	Value representing frequency that Asset #1 will be attacked if Mitigation #3 is not deployed.	Value representing impact of attack against Asset #1 that exploits lack of Mitigation #3.	Value representing cost to implement Mitigation #3.	Function of: • Attractiveness to Attack, • Freq. of Attack, • Impact of Attack, • Cost to Implement for Mitigation #3.
	Mitigation #4	Value representing Asset #1's Attractiveness to Attack.	Value representing frequency that Asset #1 will be attacked if Mitigation #4 is not deployed.	Value representing impact of attack against Asset #1 that exploits lack of Mitigation #4.	Value representing cost to implement Mitigation #4.	Function of: • Attractiveness to Attack, • Freq. of Attack, • Impact of Attack, • Cost to Implement for Mitigation #4.

6.5 Guidance on security assessments

Guidance on security assessment leverages security policy, asset identification, threat analysis, and vulnerability management which are described in the previous clauses. The assessment guidelines cover the three phases shown in Figure 1. This clause of the guidelines specifies the controls that can be used for assessment, and the inputs required for the three stages of Figure 1. Inputs for the planning and definition stage include security documentation (policy, architecture, network requirements, and threats) and technology specific security requirements (TSSRs) based on the standards and industry implementation. TSSRs vary for different networks and systems based on the underlying technologies and deployment environments. Examples of TSSRs are the use of secure protocols, such as IPSec, SSHv2, TLS, Layer 2 or layer 3 VPNs in different network conditions to secure management, control and end-user traffic. This supplement does not specify the list of TSSRs. A business or organization can derive the TSSR from applicable standards and industry security practices. Examples of security services can be found in [b-ITU-T M.3016.2]. Other technology-specific requirements can be derived from existing standards such as IETF, ISO.

Inputs for phase 2 (design and implementation) include a combination of one or more of the following: results from phase 1, TSSR implementation analysis, network security implementation status as indicated by security interviews, threat analysis results and test results from network security vulnerability audits. The inputs and security controls are further defined in this clause. An example is the security framework [b-ITU-T X.805] that can be used in conjunction with other standards and industry best practices for integrating security in every phase of the development life-cycle

The inputs to the deployment and maintenance phase include the relevant TSSR and test results that are specific to the network maintenance stage.

6.5.1 Controls for security assessment

A set of controls and sub-controls are needed to guide the network security assessment. The controls need to represent the security of various network activities that govern the network elements, network systems and their software/hardware components, services and applications. These network activities need to be generic enough so that they are accepted as technology independent. The network activities should also represent types of information flows essential to maintain and operate the end-to-end solution for its intended purpose. The activities that fit the preceding description are management, control/signalling and user traffic and their interactions with the network infrastructure, services and applications. These activities need to be qualified by parameters to indicate the security impact and solutions. These security parameters are the sub-controls in providing guidance to network security assessment.

The nine security controls shown in Figure 4, M-I, C-I, U-I, M-S, C-S, U-S, M-A, C-A and U-A are further explained in the rest of this clause.

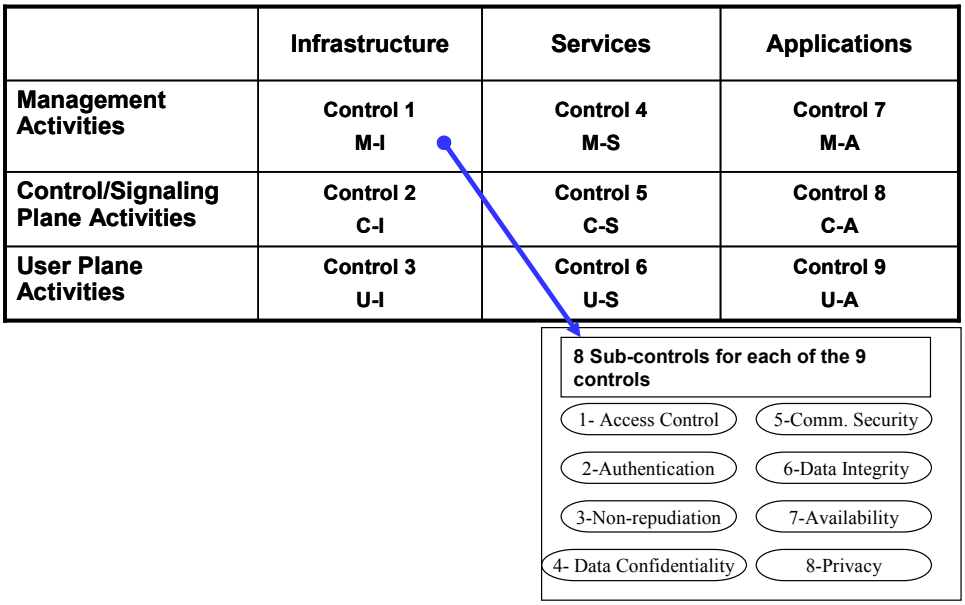


Figure 4 – Security controls for assessment

6.5.2 Control 1: M-I (Management, Infrastructure)

Securing the management activity for the infrastructure layer is concerned with securing the operations, administration, maintenance, and provisioning (OAM&P) of the individual network elements, communication links, and server platforms that comprise the network. The configuration of network devices and communications links is considered to be a management activity as well. An

example of infrastructure management that needs to be secured is the configuration of an individual router or switch by network operations personnel.

6.5.3 Control 2: C-I (Control, Infrastructure)

Securing the control activity of the infrastructure layer consists of securing the control or signalling information that resides in the network elements and systems, as well as securing the information transfer between network elements and systems. For example, the routing tables residing in the network switches need to be protected from tampering or unauthorized disclosure. In another example, routers need to be protected from receiving and propagating bogus routing updates or responding to bogus routing requests originating from spoofed routers.

6.5.4 Control 3: U-I (End-User, Infrastructure)

Securing the end-user activity of the infrastructure layer consists of securing user data as it resides in the network elements/systems, as well as while it is being transported across communications links. Protecting user data resident on server platforms is of concern here, as well as protecting user data against unlawful interception, as it is transported through network elements or across communication links.

6.5.5 Control 4: M-S (Management, Services)

Securing the management activity of the services layer is concerned with securing the OAM&P functions of network services. The configuration of network services is an example of a management activity. Another example of services management that needs to be secured is the provisioning of authorized users of an IP service by the network operations personnel.

6.5.6 Control 5: C-S (Signalling activity, Services)

Securing the control/signalling activities for the services consists of securing the control or signalling information used by the network service. An example of type of issues that would belong to this clause is securing the SIP protocol that is used to initiate and maintain the VoIP service.

6.5.7 Control 6: U-S (End-User activity, Services)

Securing the end-user activity of the services layer consists of securing user data as it uses the network service. For example, the confidentiality of a user's conversation needs to be protected in a VoIP service. Likewise, a DNS service needs to ensure the confidentiality of users of the service.

6.5.8 Control 7: M-A (Management activity, Applications)

Securing the management activity for the applications is concerned with securing the OAM&P functions of the network-based applications. The configuration of network-based applications is considered to be a management activity as well. For an e-mail application, an example of the management activity that would need to be secured is the provisioning and administration of user mailboxes.

6.5.9 Control 8: C-A (Control/Signalling, Applications)

Securing the control/signalling activities of the applications consists of securing the control or signalling information used by the network-based applications. This type of information typically causes the application to perform an action in response to receiving the information. For example, issues of securing the SMTP and POP protocols used to control the delivery of e-mail would be addressed here.

6.5.10 Control 9: U-A (End-User, Applications)

Securing the end-user activity of the applications layer consists of securing user data provided to the network-based application. For example, the confidentiality of a user's credit card number needs to be protected by an e-commerce application.

6.5.11 Sub-controls

For each control area described in clauses 6.5.2-6.5.10, there are eight sub-controls. The applicable TSSR and threat-mitigation techniques belong to one of these sub-controls.

6.5.12 Access sub-control (AC)

The access sub-control protects against unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, role-based access control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorized for.

6.5.13 Authentication sub-control (AU)

The authentication sub-control serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

6.5.14 Non-repudiation sub-control (NR)

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as, proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

6.5.15 Data confidentiality sub-control (DC)

The data confidentiality sub-control protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality.

6.5.16 Communication security sub-control (CS)

The communication security sub-control ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points).

6.5.17 Data integrity sub-control (DI)

The data integrity sub-control ensures the correctness or accuracy of data. The data is protected against unauthorized modification, deletion, creation, and replication and provides an indication of these unauthorized activities.

6.5.18 Availability sub-control (AV)

The availability sub-control ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

6.5.19 Privacy sub-control (PR)

The privacy sub-control provides for the protection of information that might be derived from the observation of network activities. Examples of this information include web-sites that a user has visited, a user's geographic location, and the IP addresses and DNS names of devices in a service provider network.

6.5.20 Target network identification and assets to be secured

The scope of security assessment is determined by the target network identification and the assets that need to be secured. The asset identification is described in clause 6.3. These guidelines apply in the security assessment clause also and they are not repeated here.

6.5.21 Guidelines for planning/definition phase

- Define network security requirements and security architecture:

  Network security requirements are derived from the business security objectives. Additional details for these objectives are defined by the policy and regulatory requirements, architecture and deployment environment. Policy guidelines are provided in clause 6.2.

- Identify the technology specific security requirements (TSSR) applicable to the network:

  TSSR identification will be spread over the two phases of the security life-cycle, planning and definition, and design and implementation. The security requirements for the solution should be compatible with the applicable TSSR. TSSRs need to be derived from applicable standards and industry practices by the organization.

- The threat analysis clause explains how to identify the threats at this stage. Services and applications (without the sub-assets) are identified at this stage.

The planning and definition phase analyses security by:

1) Deriving the high level security features and comparing them against the security coverage to address the applicable threats, TSSR, and policy/regulatory requirements.
2) Identifying the security features that will be further developed to implement access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, privacy and availability.
3) Providing results to include the list of security requirements, TSSR and gaps in the security features as shown in Table 6.

Table 6 – Security planning and definition

#	Business objectives	Services/ applications	Known threats	Applicable TSSR	Impact sub-controls	Security features planned	Gaps
1	Req 1	Svc 1	Threat 1	TSSR 1	AC, AU, etc.	Feature 1	None
2	Req 2	Svc 1	Threat 2	TSSR n	NR, etc.	----	Support NR

6.5.22 Guidelines for design and implementation

The design and implementation phase of the security life-cycle provides the technical details of architecture, protocols, network technology, software development, OAM&P design. Evaluating and baselining security is a key activity of this phase. Results of this phase leverage the input from the planning and definition phase. Key activities of this phase include:

1) Security assets

   Assets can belong in any one of the controls as discussed in clauses 6.5.2-6.5.10. Asset identification by controls will help in building a comprehensive list covering the management, signalling, and end-user activities. Asset identification is described in clause 6.3.

2) Threat analysis and mitigations

Threat analysis determines threat mitigations and their implementation priority. Threat analysis is described in clause 6.4. Threat, vulnerability management, and implementing mitigations are critical in the design and implementation phase.

3) TSSR

Identify TSSRs that are applicable to the security of services, applications, and network technology that is being planned. TSSRs serve as a key input to security quantification activity together with the threat, vulnerability management.

4) Establish security baseline for the current implementation.

Baseline of design plans can be derived by determining the current security position. This includes interviews with the security engineers, architects and product managers responsible for the network elements, threat analysis and vulnerability testing and verification. The results of security quantification need to present the compliance of various controls and sub-controls described in clauses 6.5.2-6.5.19. This supplement does not specify the format for the representation of the results. It is common practice in the industry to represent implementation levels at a given time, as a measure of security quantification.

Tables 7 and 8 show the assessment results for the implementation phase. The vulnerabilities in the solution can be identified by various industry techniques, such as architecture analysis, security audits/scans, testing. The results of this phase need to provide a list of mitigations that are prioritized to address the impact on the controls and sub-controls. The assets and mitigations in Tables 7 and 8 can be independent or they may overlap. A systematic analysis indicated by these tables ensures that no assets and the associated threats and vulnerabilities are overlooked.

Table 7 – Security implementation – Applications

Service/ Application	Asset	Threat exposure	Vulnerability	Impact sub-controls	Mitigation	Gaps	Prioriti-zation of mitigation
M-A	Asset1	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
C-A	Asset2	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
U-A	Asset3	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact

Table 8 – Security implementation – Infrastructure

Infrastructure	Asset	Threat exposure	Vulnerability	Impact sub-controls	Mitigation	Gaps	Prioritization of mitigation
M-I	Asset4	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
C-I	Asset5	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
U-I	Asset6	How is vulnerability exploited by the exposure	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact

6.5.23 Guidelines for deployment and maintenance phase

The guidelines for this phase show how the results from the previous two phases are leveraged to implement security. This clause provides guidelines for consistent network security during the deployment and maintenance phase. The clause does not provide guidelines for deployment itself. The deployment and maintenance phase focuses on variations in network operating environment and issues, such as software updates, incident management, regulatory compliance, etc. The key activities for this phase include:

1) Additional TSSR or modifications to the current ones may be necessary to account for the network deployment and operating conditions, regulatory requirements (e.g., privacy) and policy.
2) The baseline results of security quantification and threat vulnerability assessment from the design and implementation phase are a starting point in this phase. These results can be verified and updated periodically.
3) Updates to the threat exposures, vulnerability management and mitigations are also required to factor any network deployment exceptions from the original design and implementation requirements.
4) The security assessment results from design and implementation need to be verified and periodically updated as a part of the security life-cycle during this phase.
5) Update security quantification results from the design and implementation phase. Any variations can be used to provide a feedback to the appropriate security life-cycle phase.

Tables 9 and 10 show the results for the deployment and maintenance phase. The vulnerabilities in the solution can be identified by various industry techniques, such as architecture analysis, security audits/scans, testing. The work in this phase is relatively easier, as it can leverage results from the design and implementation phase. The results of this phase should provide a list of mitigations that are prioritized to address the impact on the controls and sub-controls. These results need to account for the network configuration variations in the deployment scenarios. The assets and mitigations in Tables 9 and 10 can be independent or they may overlap. A systematic analysis indicated by these tables ensures that no assets and the associated threats and vulnerabilities are overlooked. Results from these tables can be used to update the security levels determined in the design phase, and this will provide a feedback to the security life-cycle to improve security.

Table 9 – Service and applications – Maintenance and management

Service/ Application	Asset	Vulnerability (based on testing/ analysis)	Impact sub-controls	Mitigations	Gaps	Prioritization of mitigations
M-A **M-S**	Asset1	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
C-A **C-S**	Asset2	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
U-A **U-S**	Asset3	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact

Table 10 – Infrastructure – Maintenance and management

Infrastructure	Asset	Vulnerability (based on testing/analysis)	Impact sub-controls	Mitigations	Gaps	Prioritization of mitigations
M-I	Asset4	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
C-I	Asset5	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact
U-I	Asset6	Identify the vulnerabilities from testing and analysis.	What sub-controls of 6.5.11 are impacted	Describe mitigation	List the gaps in sub-controls	Prioritize based on the business impact

Bibliography

[b-ITU-T H.235.0] Recommendation ITU-T H.235.0 (2005), *H.323 security: Framework for security in H-series (H.323 and other H.245-based) multimedia systems*.

[b-ITU-T M.3016.0] Recommendation ITU-T M.3016.0 (2005), *Security for the management plane: Overview*.

[b-ITU-T M.3016.1] Recommendation ITU-T M.3016.1 (2005), *Security for the management plane: Security requirements*.

[b-ITU-T M.3016.2] Recommendation ITU-T M.3016.2 (2005), *Security for the management plane: Security services*.

[b-ITU-T M.3016.3] Recommendation ITU-T M.3016.3 (2005), *Security for the management plane: Security mechanism*.

[b-ITU-T M.3016.4] Recommendation ITU-T M.3016.4 (2005), *Security for the management plane: Profile proforma*.

[b-ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

[b-ITU-T X.805] Recommendation ITU-T X.805 (2003), *Security architecture for systems providing end-to-end communications*.

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2008) | ISO/IEC 27011:2008, *Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002*.

[b-NIST SP 800-27] NIST SP 800-27 (2004), *Engineering Principles for Information Technology Security*.

[b-NIST SP 800-30] NIST SP 800-30 (2002), *Risk Management Guide for Information Technology Systems*.

[b-NIST SP 800-53] NIST SP 800-53 (2007), *Recommended Security Controls for Federal Information Systems*.

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

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2009