

International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1052

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Security management

Information security management framework

Recommendation ITU-T X.1052



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
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1052

Information security management framework

Summary

Recommendation ITU-T X.1052 describes and recommends the framework of information security management for telecommunications to support Recommendation ITU-T X.1051 and other Recommendations in the ITU-T X.105x-series. The information security management framework (ISMF) is based on a process approach to describe a set of security management areas which gives guidelines to telecommunications to fulfil the control object defined in Recommendation ITU-T X.1051 and other Recommendations in the ITU-T X.105x-series. The management areas, which include asset management, incident management, risk management and policy management, map the controls defined by Recommendation ITU-T X.1051 to the implementation methodologies. This way ISMF relates Recommendation ITU-T X.1051, which provides management guidelines for telecommunication organizations, to other Recommendations, such as Recommendations ITU-T X.1055 and ITU-T X.1056, which provide practical methodologies focusing on a specific area of information security management.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1052	2011-05-29	17

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation 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 Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation 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 Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. 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/>.

© ITU 2012

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere.....	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations.....	1
5 Conventions	2
6 Information security management framework in telecommunication organizations ...	2
6.1 Objective.....	2
6.2 Overview of the information security management framework.....	2
7 Policy management.....	4
7.1 Overview	4
7.2 Main activities	5
8 Risk management	5
8.1 Overview	5
8.2 Main activities	6
9 Organization and personnel	7
9.1 Overview	7
9.2 Main activities	8
10 Asset management.....	9
10.1 Overview	9
10.2 Main activities	9
11 System acquisition and development.....	10
11.1 Overview	10
11.2 Main activities	10
12 Operations and maintenance management	12
12.1 Overview	12
12.2 Main activities	12
13 Incident management.....	17
13.1 Overview	17
13.2 Main activities	18
Bibliography.....	19

Recommendation ITU-T X.1052

Information security management framework

1 Scope

This Recommendation provides the information security management framework (ISMF). ISMF maps the controls defined by [ITU-T X.1051] to the practical implementation methodologies by defining a set of management areas, such as asset management, incident management, risk management, policy management and others. This Recommendation gives an overview of the framework and analyses the relationships between these areas. The specific guidelines of each area defined in this Recommendation are provided in a series of other ITU-T Recommendations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[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*.

[ITU-T X.1055] Recommendation ITU-T X.1055 (2008), *Risk management and risk profile guidelines for telecommunication organizations*.

[ITU-T X.1056] Recommendation ITU-T X.1056 (2009), *Security incident management guidelines for telecommunication organizations*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

None.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 configuration item: A security configuration item is a specific security configuration requirement of a specific class of assets, which includes the description of the requirement, the reference method for the implementation of the requirement, and the conditions to check whether the requirement be complied or not.

3.2.2 configuration profile: A group of configuration items suitable for a special class of asset.

4 Abbreviations

This Recommendation uses the following abbreviations and acronyms:

ISIRT Information Security Incident Response Team

ISMF Information Security Management Framework
 ISMS Information Security Management System
 IT Information Technology

5 Conventions

None.

6 Information security management framework in telecommunication organizations

6.1 Objective

[ITU-T X.1051] defines categories of security controls for telecommunication organization security management, such as security policy, organization of information security, and human resources security, among others. ISMF defines a series of main activities to conduct and support the implementation of security controls. ISMF combines the controls in [ITU-T X.1051] and the Recommendations which define implementation methodologies for a number of management areas, such as [ITU-T X.1055] and [ITU-T X.1056].

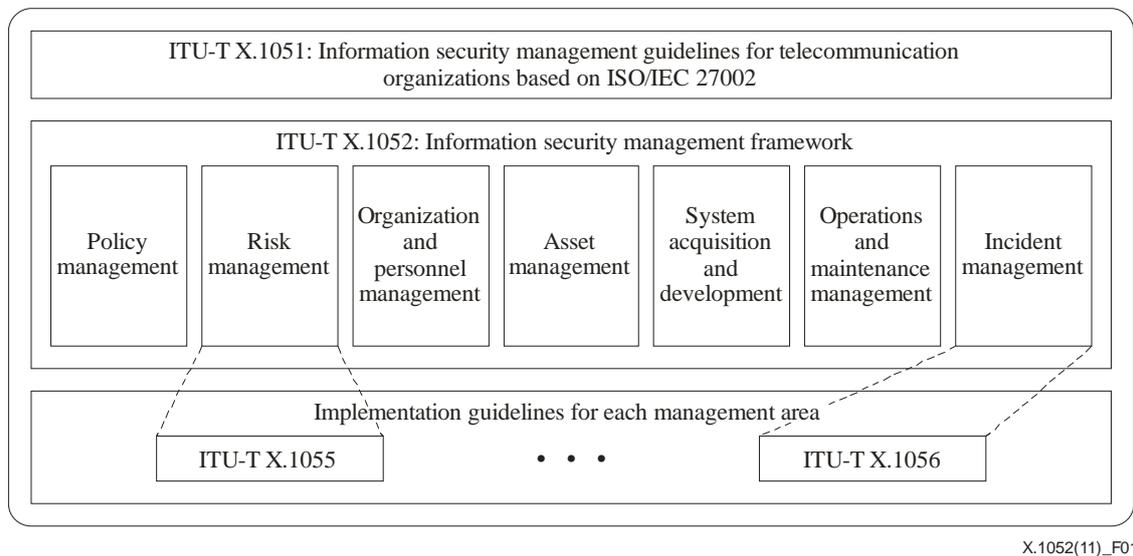


Figure 1 – Relationship between Recommendation ITU-T X.1052 and other ITU-T X.105x-series Recommendations

6.2 Overview of the information security management framework

It is necessary for telecommunication organizations to confirm the scope of their information security management system (ISMS), which includes information assets. The guidelines for implementing the information security management and this confirmation should be carried out before assessing the risks to their information assets and determining the subsequent controls of the risks. In addition, it is necessary to establish the structure and form of the information security organization as the base for the implementation of information security for controlling the risks. The risk-controlling activities of the telecommunication organizations should not be isolated from the operations of the organizations. The operations of the organization are generally described in a series of procedures. The risk-controlling activities of information security should be regarded as an integral part of the relevant procedures.

The ISMF describes the main activities related to telecommunication organizations and information security management from the three aspects:

- a) supporting the implementation of information security management within telecommunication organizations, including management areas such as organization and personnel management and asset management;
- b) establishing and continually improving the ISMS, including management areas such as risk management and policy management;
- c) specific operational activities of the telecommunication organization, including management areas such as system acquisition and development management, operation and maintenance management, and incident management.

The seven management areas shown in Figure 1 are, on one hand, a summary of the management activities of a telecommunication organization which are strongly related with the operation of the organization. These, on the other hand, correspond closely to the controls specified in [ITU-T X.1051]. Activities that relate to the organization and personnel management serve and comply with the control objectives defined in the clauses "Organization of information security" and "Human resources security" of [ITU-T X.1051]. In the same way, asset management mainly serves the control objectives described in the "Asset management" and "Physical and environmental security" of [ITU-T X.1051]. Risk management primarily serves to support the control objectives described in the "Communications and operations management", "Access control" and "Information systems acquisition, development and maintenance" of [ITU-T X.1051]. Finally, incident management primarily supports the control objectives given in the "Information security incident management" and "Business continuity management" of [ITU-T X.1051].

The security policy of an organization defines the aims of information security management of the organization, clarifies the management requirements of information security, and provides the necessary suggestions or guidelines. The aim and scope of information security, the purpose of the management, control objects selected and the framework of controlling measures can also be found in the policy.

Risk management should involve the following activities: analyse the threats the organization faces, examine the vulnerabilities of the organization's assets, implement the controls to mitigate the organization's risks and continually improve the effectiveness of the organization information security.

Asset management is an essential aspect of the scope of the ISMS of the telecommunication organization. Asset management involves identifying the assets of the organization, defining the rules for classifying and valuing assets, managing asset inventories, confirming the ownership of assets and reviewing and monitoring asset changes.

By establishing a security organization and confirming the duties of the personnel, organization and personnel management is likely to guarantee the execution of other management activities in the ISMF, such as security policy management and risk management. The main activities of organization and personnel management include clarifying the commitment of the management, founding the relevant responsibility framework and controlling measures, screening the candidates prior to employment, providing the security-relevant education and training during employment, defining and assigning responsibilities for performing employment termination.

Information security management should be a critical component of the telecommunication organization operations. Telecommunication organizations need to confirm the control objectives and controls suitable for them, based on the risk assessment, and to achieve these objectives by changing and optimizing the operating procedures of the organization. The operating procedures of telecommunication organizations should reflect a number of procedures that are strongly related to information security management, such as information systems acquisition, access control of applications and data, configuration management and change control, monitoring review and audit activities, and incident management. ISMF categorizes the control objectives and controls defined by [ITU-T X.1051] and reflects these into the security management areas closely aligned to the organizational operations procedures.

The main content of system acquisition and development management should clearly define the system security demands in the planning phase, examine the realization of security demands in the development phase, and realize and examine the construction requirements of systems in the implementation phase.

Operations and maintenance management is responsible for maintaining the working order of systems, and for doing routine security operations. When changes occur to the information systems or the working environments, operation and maintenance management should evaluate the systems' security, review the existing risk-control measures and update and improve these risk-controlling measures, when necessary, and finally regularly review and manage the changes, including carrying out periodic audits of the information systems.

Incident management is the process which involves detecting, reporting, analysing and evaluating, responding and resolving incidents. An important aspect of incident management is to make recommendations to implement precautionary and remedial measures, and responses to the incidents that have occurred. Post-incident activities should include learning from incident experiences and should enable the organization to enrich the precautionary measures and continually improve the whole incident management methods of information security.

7 Policy management

7.1 Overview

Security policy is the basis of information security management. Policy management is responsible for the management of establishment, approval, reviews, changes and updates of the security policy of a telecommunication organization. Other security documentation, specifications, and guidelines should be derived from this security policy.

Telecommunication organizations need to consider their own requirements and business objectives to be able to establish their security policy. The main sources of input for the development of the security policy, which need to be considered and included in the security policy, are as follows:

- a) consideration and definition of the business strategy and objectives of the telecommunication organization;
- b) identification and evaluation of the risks the telecommunication organization faces and the security measures and controls needed to combat these risks;
- c) compliance requirements of the relevant laws, rules and regulations, contractual requirements and obligations and the cultural and societal requirements, which the organization, its partners, contractors and the service providers have to meet. The security policy should summarize these requirements;
- d) the goals, principles and specific requirements of telecommunication services provided by the organization.

7.2 Main activities

Policy management should specify the management activities and procedures that should be undertaken regarding the acquisition, analysis, organization and approval of security policy requirements and the associated security documentation deriving from this policy.

In all stages involved, the activities should have confirmed the control objectives and the contents of [ITU-T X.1051], as indicated in Table 1.

Table 1 – Clauses of [ITU-T X.1051] related to policy management

Clause number	Clause title
5	Security policy
11.1	Business requirement for access control

The main activities of policy management comprise the management of the following procedures:

- a) Collect the security policy requirements. This collection of requirements applies both to changes to the existing security policy and to the creation of a new security policy. The requirements can be acquired from the organization's use and execution of the existing policies or as a result of identifying new security requirements. After this acquisition and collection of requirements, it is necessary to analyse if they are acceptable to management for the amendment of the existing security policy or if they are acceptable for the establishment of new security policy.
- b) Analyse the requirements and confirm the development of the policy. After the acceptance of the requirements either for the amendment of the existing security policy or the application of a new security policy, an analysis of the application of these requirements needs to be carried out. Finally, a report analysing these requirements should be produced. According to this analysis report, management needs to make a decision as to whether to accept the findings of the report with respect to the application of these requirements. If the findings of the report are approved, then resources should be allocated to the development of the policy. If the findings are rejected, then the reasons and justification for this rejection should be documented.
- c) Establish the security policy. Establish the relevant security policy based on the analysis of the application requirements. If necessary and appropriate, the amendment or establishment of the security policy may need to involve co-operation with suppliers or partners.
- d) Approve and publish the security policy. Management should examine and then approve the amended or newly-established security policy. After the policy has been approved, it needs to be published and distributed to all departments or staff and employees and other interested parties. If the security policy is not approved, it needs to be returned to the developers to be revised to take into account the comments from management.
- e) Monitor and review the policy execution. Monitor the execution of the released security policy to assess and review if it satisfies the security requirements. Improve the security policy by making the relevant changes and amendments to ensure that the content of the security policy continues to meet the organization's requirements.

8 Risk management

8.1 Overview

Risk management is a series of coordinated activities to assess and control the risks an organization faces. This includes identifying the implementation and validity of the security protection measures which protect the information assets of telecommunication organizations. These activities include

identifying and assessing the value of the information assets, identifying and analysing the threats and vulnerabilities associated with these information assets and other assets (e.g., technology and management), assessing security risks, and proposing improvements.

Risk management includes the following steps: assessment, risk reduction, monitoring, and improvement. Assessment means identifying, analysing and evaluating the risks associated with the assets of the telecommunication organization. Risk reduction means identifying the available options to manage and control the risks. Control of risks involves selecting the proper security measures and implementing them. Monitoring means to regularly measure and check whether the results of the controls meet the security requirements of information systems by applying methods for examining, testing and evaluating. Improvement means updating or improving the controls based on the result of monitoring the controls. The management layer of the organizations should be involved in the risk management process by reviewing and examining the results of the risk assessment, and by authorizing the implementation of the risk control measures, and making the decision on whether or not to accept the resulting residual risks.

The steps of risk management mentioned above need to be executed periodically or when the objectives and characteristics of the telecommunication service change or new threats appear. Hence, assessment, control, monitoring and improvement constitute a continual improvement cycle to enable the assets to be effectively protected to ensure that all new security requirements are satisfied and to mitigate new or changing risks.

8.2 Main activities

Risk management mainly includes risk assessment, risk control, monitoring, and improvement. In all stages involved, the activities should comply with the control objective and the contents of the following clauses of [ITU-T X.1051], as indicated in Table 2.

Table 2 – Clauses of [ITU-T X.1051] related to risk management

Clause number	Clause title
5	Security policy
10	Communications and operations management
11	Access control
15	Compliance

Each stage of risk management is described below:

- a) **Assessment:** Risk assessment identifies and analyses the threats, vulnerabilities and relevant protection measures of evaluated assets. The evaluated risks include information system risks, human resource risks, operation risks, network service risks, IT service risks, physical risks, compliance risks, etc. After the risks are evaluated, the risks confronted by the evaluated assets and the relevant risk levels are generated as the input of risk control.
- b) **Risk reduction:** Risk reduction focuses on selecting and implementing the proper security measures based on the results of risk assessment, and controlling the risks confronted by the organizations to an acceptable level. Risk reduction consists of three steps: judging current risks, selecting control objectives and controls, and implementing risk controls.
 - i) Risk-decision making includes estimating whether current risks are acceptable and selecting an appropriate set of security controls and measures for the treatment of risks. In addition to the option of reducing the risk, there are two other options: transferring the risks to outside parties, e.g., suppliers, and avoiding the risks by not using the assets confronting the risks.

- ii) Selecting control objectives and controls includes analysing the risk control requirements and defining the risk reduction objectives and controls. The risk reduction objectives and controls could be selected from [ITU-T X.1051].
 - iii) Implementing risk controls includes specifying the risk reduction implementation plans and carrying them out.
- c) **Monitoring:** Monitoring includes continuously reviewing the changes to residual risks, changes to assets, new threats and vulnerabilities, and other changes in the business that might introduce new risks. The monitoring process also includes checking the effectiveness of the security controls and measures selected at the risk-reduction step. This can be done through a security audit, post-incident analysis, complaints from clients about telecom services, and measurements to check the performance and effectiveness of the security controls in an operational environment.
- d) **Improvement:** This step focuses on improving the effectiveness of the selected security controls and measures by optimizing procedures or technically improving the implementation of security controls and ensuring that the improvements achieve their intended objectives.

9 Organization and personnel

9.1 Overview

Organization and personnel management in a telecommunication organization mainly refers to setting up the security framework for the organization, initiating and controlling the implementation of security procedures, specifying the security roles related to the security procedure, and allocating the security roles to the relevant personnel.

The personnel of the organization include both the internal and the external personnel (e.g., the personnel of third parties, e.g., suppliers). Internal personnel management includes, among other things, setting up the security organizational structure, drawing up, checking and approving the security-related responsibilities of the posts, and conducting follow-up inspections. Setting up a security organizational structure refers to designing and maintaining a rational security organizational infrastructure that will be used for information security management. Drawing up security-related responsibilities of the post refers to specifying the security-related responsibilities of the post according to the assets and procedures related to the post. Checking and approving the security-related responsibilities of the post refers to checking whether the responsibility meets actual requirements and authorizing its fulfilment. Conducting follow-up inspections refers to continually monitoring whether the responsibilities of the post meets the post's security requirements, especially when the post description changes.

Telecommunication organizations rely on third-party suppliers for various types of service. The telecommunication organization should ensure that the introduction of third-party services will not affect the security of the organization's information processing facilities and information assets. Third-party management includes confirmation of the scope of work and third-party capability for delivering services in a secure way. Confirmation of the scope of work refers to confirming whether the third-party personnel are allowed to participate in activities, taking into consideration the importance of the system and the sensitivity of the relevant information. Confirmation of the third-party capability refers to the process of drawing up criteria and conditions for allowing third-party employees to enter the telecommunication organization's facilities and to handle and process information assets of the organization. Telecommunication organizations should assure themselves of the third-party capability by some form of inspection, e.g., through an auditing, checking, and managing process for the qualification of third-party personnel and their activities in the telecommunication organization.

9.2 Main activities

Internal personnel management includes, among other things, setting up the security organization, drawing up, checking and approving the security-related responsibilities of the posts, and conducting follow-up inspections. In all stages involved, the activities should comply with the contents and control objectives of [ITU-T X.1051], as indicated in Table 3.

Table 3 – Clauses of [ITU-T X.1051] related to organization and personnel

Clause number	Clause title
6.1	Internal organization
6.2	External parties
8.1	Prior to employment
8.2	During employment
8.3	Termination or change of employment
10.1	Operational procedures and responsibilities
10.2	Third party service delivery management
11.2	User access management
11.3	User responsibilities
12.5	Security in development and support processes

The specific activities of organizational personnel management are described below:

- a) Setting up the security organization. It refers to providing an organizational guarantee for the organization to achieve the information security goals by designating and conveying information security responsibilities and setting up an internal coordination and cooperation framework. The activity should include establishing the relevant processes at the management level needed to approve the information security policy, designate security roles, and coordinate the implementation of security controls in the organization. This process is the basis for the security of the organization.
- b) Drawing up security-related responsibilities of the posts. It refers to developing information security requirements (e.g., confidential requirements) for the posts, depending on the assets and procedures related to each post in the organization. The detailed rules and criteria of the posts need to be established in order to guide the personnel assigned to each post.
- c) Checking and approving the posts' responsibilities. It refers to checking, approving and releasing the newly-created or revised post responsibilities. If not approved, the responsibility statements should be returned for revision to the related compiling sector. Once the post responsibilities have been released, the changes will be notified to the pertinent sectors or leaders.
- d) Follow up inspection. It refers to continually tracking the released security post responsibilities and confirming whether they meet the security demands. If the demands are not met, the post responsibilities should be revised.

Third-party management comprises confirmation of the scope of activities performed by third parties, determination of third-party required qualifications, audit, and inspection. The specific activities are described below:

- a) Confirmation of the scope of activities. This refers to determining whether third-party personnel are allowed to participate in activities, taking into consideration the importance of the system and sensitivity of the information involved. An output of this activity is the specification of the sub activities third-party personnel are allowed to participate in and the

ones that need to be completed only by internal personnel of the telecommunication organization.

- b) Determination of required qualifications. This refers to the process that determines the qualifications that a third-party and its personnel should have, taking into account the sensitivity of the assets involved in the third-party activities and the protective measures deployed by the organization. This is done based on a clear definition of the scope of the third-party participation. The description of the required qualifications should clarify requirements such as third-party qualification, confidentiality, security awareness of staff, security obligation, and responsibility. It should also confirm the protective measures to be implemented for the third party, such as the access border of the network and limitation of participation in activities, and specify strict access control measures at the border in order to avoid unnecessary disclosure of information.
- c) Audit. This refers to implementing a security audit carried out on third parties prior to the signature of contracts and service level agreements (SLAs). This involves ensuring that the qualifications of the third party meet the organization's requirements, and that all third-party personnel sign a confidentiality agreement with the organization. It also involves monitoring, recording and auditing the processes used by the third party to provide their services.

10 Asset management

10.1 Overview

Asset management mainly refers to classification and control of organizational assets, whose goal is to define and manage the assets within the security boundary of the organization and maintain appropriate protection on organizational assets. Asset management includes establishing the policy for asset management, surveying and identifying the assets, classifying and registering the assets, evaluating the importance level for assessing the value of the assets, and performing change management.

10.2 Main activities

The asset management activities mentioned in clause 10.1 comply with the controls and control objectives of [ITU-T X.1051], as indicated in Table 4.

Table 4 – Clauses of [ITU-T X.1051] related to asset management

Clause number	Clause title
7.1	Responsibility for assets
7.2	Information classification
9.1	Secure areas
9.2	Equipment security

The specific activities of asset management are described below:

- a) Establishment of the policy for asset management. For the purpose of systematically and efficiently managing the assets, protection objectives should be defined and a management policy should be established for handling assets and selecting control measures. These activities may be helpful as a baseline to determine practicality and cost efficiency of protective controls.

- b) Survey and identification. There are many various assets such as IT systems in telecom business organizations. In order to effectively protect the assets, it is first necessary to survey and identify overall assets within the security boundary for risk analysis including asset evaluation. Fundamentally, it is one of the substantial activities for the valuation of each asset.
- c) Classification and registration. Identified assets through the established asset boundary are classified by their types in the asset classification criteria. There are classifications by asset items and business process. Classification and registration activities for assets mean that those assets should be protected and managed in the asset register. One of the important considerations is to determine the number of classification categories and the benefits to be gained from their use.
- d) Evaluation of asset value. To determine the measures required to adequately secure an asset, the asset should be evaluated and classified according to its evaluation results. For determining each asset's value, it can be evaluated based on three primary security requirements, that is, confidentiality, integrity, and availability. Assessing the value of the assets is the first task in all risk analyses.
- e) Performance of change management. Many attributes of an asset change as time passes. Therefore, an asset manager should periodically check its current status and update the asset register. A key purpose of follow-up and update is to check whether or not each asset is well managed according to its security level.

11 System acquisition and development

11.1 Overview

Information systems are the basis of telecommunication systems and services. Including security in the design and implementation of information systems is crucial to protect the organization's information assets against the risks the organization faces. The acquisition process of information systems can be broken down into three steps: system planning, design and development and implementation. The security requirements of information systems should be taken into account in these three steps.

In the system planning phase, the key point is that the security requirements of the information system needs to be clarified, and an analysis for realizing the security requirements in terms of security controls and measures needs to be considered. In the development phase, besides implementing the security requirements determined in the planning phase, it is necessary to guarantee security in the development process, for the documentation and software source codes, and to adopt security controls to prevent the security defects in the software programs. In the implementation phase, it is imperative to ensure that there is no impact or conflict between the system being implemented and other systems, especially the existing legacy systems, which provide the telecommunication services. It is also important that all the planned security requirements are satisfied before the acceptance of the system being implemented.

11.2 Main activities

System acquisition and development mainly comprises system planning, development and implementation. In all stages involved, the activities should comply with the contents and control objectives of [ITU-T X.1051], as indicated in Table 5.

Table 5 – Clauses of [ITU-T X.1051] related to system acquisition and development

Clause number	Clause title
10.3	System planning and acceptance
12.1	Security requirements of information systems
12.2	Correct processing in applications
12.3	Cryptographic control
12.4	Security of system files
12.5	Security in development and support processes

The specific activities of system acquisition and development are described below:

11.2.1 System planning

- a) Define system security objectives. A set of the system security objectives need to be defined and identified according to the security policy established by the telecommunication organization, the result of the risk assessment, and the business features that the system supports.
- b) Determine system security requirements. Based on the system security objectives, the organization needs to analyse and identify a specific set of system security control requirements and to evaluate the feasibility of these system security requirements.
- c) Compile system security specifications based on system security requirements.
- d) Review and approve system security specifications. The result of the approval process should be fed back to the relevant personnel and experts. If the specifications are approved, then the development team can go ahead with the system development process and security implementation process. Otherwise, if the specification is not approved, the specification needs to be revised.

11.2.2 System development

- a) Compile a security development plan. Telecommunication organizations should establish a security plan to guide the development of information systems. The development of a telecommunication organizations' information system will typically involve a variety of development processes such as internal development, outsourcing development and outright purchasing and acquisition processes. The plans and specifications should specify the requirements for various development processes to ensure that the security controls of system development have been implemented properly and no intentional or unintentional weaknesses are left during development. Security development plans and specifications need to be approved by the management of telecommunication organizations.
- b) Implement security development plans and specifications. Depending on the development process being used, the specific requirements of the security development plans and specifications should be specified in the system development regulations of the organization or in the development contract signed by the organization and the development service supplier. During the process of development, checks and reviews should be carried out at each step of the development process. This should verify that the security objectives and requirements are met.
- c) Security audit. After completing the development, the telecommunication organization should designate auditors, independent of developers, to carry out a security audit on the developed system so as to ensure that the system achieves the requirements in the system security development plans and specifications and confirm the compliance of development activities during the developing process.

11.2.3 System implementation

- a) Compiling a security scheme for information system deployment. Telecommunication organizations need to establish security plans and specifications for guiding their information system deployment. The scheme for a specific information system deployment needs to depend on the above plans and specifications, related contracts, system sensitivity, system access information and other information during the deployment, and be approved by the management of the telecommunication organization.
- b) Deploying information system. According to the security scheme defined for the information system deployment, the telecommunication organization should deploy the information system, ensuring that the deployment meets the requirements of the security specifications, and controlling the impact on other existing systems.
- c) Acceptance of information system. After the deployment, the security specifications specified in the contract or other required documentation should be tested and verified to check whether the information system meets the security requirements. If not, revisions need to be made until the requirements are met and acceptance is given.

12 Operations and maintenance management

12.1 Overview

Operations and maintenance management is responsible for keeping the security of information systems effective and efficient. This is particularly important when changes occur, or are likely to occur, in the system, resources, or assets in the operating environments.

12.2 Main activities

Operations and maintenance management includes several activities, such as security early-warning management, security configuration management, security patch management, security change management, network interconnection management, remote access management, antivirus management, and data leakage management. These activities are described as follows.

12.2.1 Security early-warning management

Security early-warning management involves the process for collecting, distributing, handling and processing of relevant early-warning information. Security early-warning management needs to comply with the control objectives and controls defined in [ITU-T X.1051], as indicated in Table 6.

Table 6 – Clauses of [ITU-T X.1051] related to security early-warning management

Clause number	Clause title
13.1	Reporting information security events and weaknesses

The specific activities of security early-warning management mainly include the following steps:

- a) Collection: Collect early-warning information from the results of internal security incidents of organizations, security announcements of software/hardware vendors, and other security organizations.
- b) Analysis: Analyse the impact of the information on relevant assets, judge whether it is necessary to adopt additional controls, and release security early-warning reports if adopting additional controls is not imperative.

- c) Recommendations: Make recommendations for improvements to the security early-warning controls.
- d) Review: Review the suitability, adequacy and rationality of the recommendations made. This might involve invoking the security configuration management process if the recommendations need to change the security configurations of the relevant assets; invoking the security patch management process if the recommendations involve installing security patches/updates associated with the relevant assets.
- e) Track the implementation: Track the implementation of the recommendations and inform the status of the implementation to relevant parties.

12.2.2 Security configuration management

Security configuration management refers to the management of the security configurations of information assets. This includes maintaining asset configuration requirements and documenting and recording the status of the implementation of the requirements on assets. Security configuration management needs to comply with the control objectives and controls defined in [ITU-T X.1051], as indicated in Table 7.

Table 7 – Clauses of [ITU-T X.1051] related to security configuration management

Clause number	Clause title
7.2.2	Information labelling and handling
11.5	Operating system access control
11.6	Application and information access control
12.2	Correct processing in applications
12.3	Cryptographic controls

The specific activities of security configuration management include the following steps:

- a) Collect security configuration items. Security configuration items of a specific asset come from several related sources such as related specifications, suggestions of security improvement in early-warning management, etc. The objective of this step is to identify security configuration items that a specific asset needs to comply with.
- b) Build asset configuration profiles. The configuration profile is a group of configuration items suitable for a specific class of asset, such as equipment, information system or information service.
- c) Set up a profile benchmark. Defining a benchmark for the configuration profile provides a means for evaluating the variables of the configuration profile items in accordance to the profile as well as the importance of the related asset and its environment. Telecommunication organizations could check their assets against the benchmark related to them.
- d) Implement security configurations. The implementation of the configuration profile of the asset is part of the security change management process.
- e) Monitor changes of security configurations. Monitoring the status of the implementation of the security configuration profiles on assets, and identifying those items that fail to meet the benchmark.
- f) Review and track security configurations. Continually review and check whether the security configurations fulfil the security requirements of assets, to make adjustments to the configuration where necessary in order to meet the security requirements, and make

changes to the profiles or benchmarks by adding or removing configuration items, as well as to meet the security requirements, change the value of the variables, etc.

12.2.3 Security patch management

Security patch management needs to comply with the control objective and the controls of [ITU-T X.1051], as indicated in Table 8.

Table 8 – Clauses of [ITU-T X.1051] related to security patch management

Clause number	Clause title
12.6	Technical vulnerability management

The specific activities for patch management mainly include the steps shown below:

- a) Identify security patch requirements. Track and collect information on security patches/updates from the suppliers or vendors of assets and security recommendations from security early-warning management. Based on this information, generate the patch requirements for the asset.
- b) Check and test the effectiveness of the security patches.
- c) Priority of patches. In accordance with the impact analysis of the vulnerabilities, risks and the environment of the related asset, decide upon an implementation priority of the patches.

The activities of patching, such as creating a change plan of the patch installation, authorizing the plan, and implementing the plan, will become part of the security change management process.

12.2.4 Security change management

Security change management refers to management on changes to the information systems of the telecommunication organization. This includes the management for testing and implementing the change plan, and verifying and feeding back the result of the change. Security change management needs to comply with the control objectives and the controls of [ITU-T X.1051], as indicated in Table 9.

Table 9 – Clauses of [ITU-T X.1051] related to security change management

Clause number	Clause title
7.1	Responsibility for assets
12.4	Security of system files
12.5	Security in development and support processes

The specific activities for security change management mainly include the steps shown below:

- a) Change requests and requirements. Collect change requirements from activities such as configuration management, patch management process, etc., and then formulate requests for changes to be implemented.
- b) Establish a security change plan. Establish the security change plan, including the scope of the impact associated with the change, and detailing the process of changes to operations, details of the process for checking the effectiveness of the changes, and details of operational processes of rollback, service continuity plans, etc., to minimize any negative impact and/or conflict of implementing the changes on the related assets.

- c) Test security change plan. After establishing the security change plan, conduct lab tests and on-site tests for the plan. Lab tests refer to testing the feasibility of the plan in a simulated environment. On-site tests refer to conducting the test in a selected on-site environment to check whether the plan, that passed lab-test, is feasible or not. Care needs to be taken when conducting tests on operational systems, to avoid compromising the operations and causing system failures and/or disruptions to operations.
- d) Authorize the plan. According to test results and the impact analysis of the related assets, the change plan should be authorized and approved by management in charge of operations.
- e) Implement the security change plan. According to the security change plan, change the security configuration; install security patches, etc.
- f) Track and monitor security changes. Continually track and monitor the implemented security configuration changes to check whether the change has been effective or not, and whether the change has caused any negative impact on the operations security of systems or network.

12.2.5 Network interconnection management

Network interconnection management needs to comply with the control objectives and controls of [ITU-T X.1051], as indicated in Table 10.

Table 10 – Clauses of [ITU-T X.1051] related to network interconnection management

Clause number	Clause title
10.6	Network security management
11.4	Network access control
12.5	Security in development and support processes

The specific activities of network interconnection management mainly include the steps shown below:

- a) Establish the principles for network interconnections. The principles for network interconnection should be defined according to the security policy. This is important in order to be able to implement the security requirements of network access between different networks of telecommunication organizations.
- b) Establish the plan for the network interconnection. Establish the plan for implementing network connection requirements in accordance with the operational needs of the business department of the organization or a third-party network owner.
- c) Examine the network interconnection plan. Examine if the network interconnection plan complies with the principles of network interconnection. If not approved, the plan should be returned to its author in order to be appropriately revised.
- d) The implementation of the network interconnection plan will be turned into the security change management process.
- e) Examine and track the implementation results. Examine whether the implementation results of network interconnection match the content of the network interconnection plans, and update the information of network interconnections, where necessary, to ensure there is a correct match.

12.2.6 Remote access management

Remote access management should comply with the control objectives and the controls of [ITU-T X.1051], as indicated in Table 11.

Table 11 – Clauses of [ITU-T X.1051] related to remote access management

Clause number	Clause title
11.7	Mobile computing and telecommuting

The specific activities of remote access management mainly include the steps shown below:

- a) Establish the organization's rules and procedures for remote access according to the security policy.
- b) Identify the requests and requirements for remote access. Collect the requirements and requests for remote access of third parties, mobile working, telecommuting, etc.
- c) Authorize the remote access requests according to the organization's remote access rules.
- d) Implement the provision of remote access. Implement the remote access, minimizing the scope and the period of the access according to the requests and the rules for remote access. If the remote access involves a third party, then a confidential agreement should be signed.
- e) Monitor the status of the remote access. Periodically check the operational and audit trail records of the remote access, and examine if there are any abnormal access records.

12.2.7 Antivirus management

Antivirus management should comply with the control objectives and the controls of [ITU-T X.1051], as indicated in Table 12.

Table 12 – Clauses of [ITU-T X.1051] related to antivirus management

Clause number	Clause title
10.4	Protection against malicious and mobile code

The specific activities of antivirus management mainly include the steps shown below:

- a) Check and acquire the latest virus definitions periodically.
- b) Forward the virus definitions to the clients and servers of antivirus software.
- c) Execute the antivirus tasks periodically.
- d) Submit the antivirus reports. According to the results of virus scan, submit periodically the antivirus reports to the management level.

12.2.8 Data leakage management

Telecommunication organizations hold sensitive information of the organization, its staff and employees, and of its customers. This includes sensitive customer personal information, contents of customer communications, etc. Data leakage management is necessary to protect information from being exposing to unauthorized third parties. Data leakage management should comply with the control objectives and the controls of [ITU-T X.1051], as indicated in Table 13.

Table 13 – Clauses of [ITU-T X.1051] related to data leakage management

Clause number	Clause title
10.7	Media handling
10.8	Exchange of information
10.9	Electronic commerce services

The specific activities of data leakage management mainly include the steps shown below:

- a) Establish the requirements and specifications for data leakage management according to the security policy.
- b) Establish the process for handling sensitive data: storing, processing, sharing and transmission, and destruction. This includes data distribution, processing in the systems, and data transfer between systems. Data leakage management is based on establishing and implementing a data classification scheme and the detailed recording of where the data is stored and transferred to.
- c) Establish the specifications and process/procedures for media handling, information publishing and exchange of information between organizations or inter-sectors of the organization.
- d) Monitor the interfaces and boundaries of data exchange and report any data leakage incidents.
- e) Update the specifications and process/procedures described above and optimize these processes/procedures to ensure effective data leakage management.

13 Incident management

13.1 Overview

Even after telecommunication organizations have adopted the right security controls, residual risks still exist and security incidents unavoidably happen, which directly or indirectly exert a negative influence on the telecommunication service delivered by the organization. It is important that telecommunication organizations establish a well-structured and planned process to handle information security incidents.

The incident management process includes several stages: preparation and planning, detection and reporting of incidents, assessing and evaluating incidents, responding to incidents, recovery from incidents, and lessons learnt. Preparation involves designing, testing, and maintaining incident handling plans to be able to effectively respond to security incidents. Protection refers to adopting some controls to protect various assets from the threats faced by the organizations. Detection and reporting activities involve making sure those incidents are detected and reported in a timely way to be able to respond and handle the incidents effectively. Detection and reporting activities involve monitoring the systems, services and business process to check whether an incident is occurring. There are various detection and monitoring mechanisms and procedures that can be deployed for this purpose. Incident assessment and evaluation refers to the process for analysing the severity of incidents and the impact they may have. This process also enables the incident handling team to be able to set priorities and define the sphere of influence of the incidents. Responding to incidents involves handling incidents in a timely and effective way to ensure a minimal potential damage of the incident on the telecommunication organization. Recovery from the incident involves getting the telecommunication organization back to normal operation. Finally, there are valuable lessons to be learnt from the incidents that have occurred, and so it is important that the telecommunication organization take the opportunity to make essential improvements to avoid and protect against future potential incidents. This should include implementing improvements to the information

security controls to prevent recurrence of the incident, better user awareness for reporting incidents, and making the incident management process more effective.

An information security incident team, sometimes referred to as information security incident response team (ISIRT), should exist in the telecommunication organization. The role of this team will be to take charge of the incident management process. The main activities of ISIRT include both passive and active response services as well as providing security quality management services. Passive response service mainly includes alarm and incident management activities, and vulnerability management and manual processing. Active response service includes announcement, technical observation, security examination and evaluation, security tools configuration and maintenance, security tools development, intrusion detection service and security-related information spreading. The security quality management service includes risk analysis, service continuity and disaster recovery plans, security consultancy, awareness and education activities, and product evaluation.

13.2 Main activities

Incident management needs to confirm the control objectives and the contents of [ITU-T X.1051], as indicated in Table 14.

Table 14 – Clauses of [ITU-T X.1051] related to incident management

Clause number	Clause title
10.5	Back-up
10.10	Monitoring
13.1	Reporting information security events and weaknesses
13.2	Management of information security incidents and improvements
14	Business continuity management

The main activities related to incident management in a telecommunication organization and its ISIRT are described in [ITU-T X.1056].

Bibliography

[b-ISO/IEC 27002] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management.*

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	Terminals and subjective and objective assessment methods
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