International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1052

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Information security management processes for telecommunication organizations

Recommendation ITU-T X.1052

ITU-T

International
Telecommunication
Union

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1052

Information security management processes for telecommunication organizations

Summary

Recommendation ITU-T X.1052 provides best practices for information security management for telecommunication organizations to support Recommendation ITU-T X.1051. This Recommendation is based on a process approach to describe a set of security management areas, which give guidelines for telecommunication organizations to fulfil the control objectives defined in Recommendation ITU-T X.1051. The management areas described in this Recommendation including asset management, incident management and risk management policy management, map the controls defined by Recommendation ITU-T X.1051 to achieve methodologies.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1052	2011-05-29	17	11.1002/1000/11337
2.0	ITU-T X.1052	2020-10-29	17	11.1002/1000/14044

Keywords

Information security management, management guideline, management process.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

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/.

Table of Contents

Recommendation ITU-T X.1052

Information security management processes for telecommunication organizations

1 Scope

This Recommendation provides information security management processes for telecommunication organizations to support the implementation of [ITU-T X.1051].

This Recommendation is based on a process approach to describe a set of security management areas which give guidelines to telecommunication organizations to fulfil the control objectives defined in [ITU-T X.1051].

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 (2016) | ISO/IEC 27011:2016, *Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[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 telecommunications organizations*.

[ITU-T X.1057] Recommendation ITU-T X.1057 (2011), *Asset management guidelines in telecommunication organizations*.

3 Definitions

3.1 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 is complied with or not.

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

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

PDCA	Plan-Do-Check-Act

5 Conventions

None.

6 Overview

6.1 Objective

[ITU-T X.1051] defines categories of security controls for telecommunication organization security management, including security policy, organization of information security, and human and resources security. This guideline defines processes in information security management in the organization and a series of main activities to conduct and support the implementation of security controls.

6.2 Processes

According to the best practice and experience of telecommunication organizations' security management work, combined with the plan-do-check-act (PDCA) management cycle, the information security management of telecommunication organizations should include seven main processes as listed below and shown in Figure 1.

1) Conduct risk assessment for information security,
2) Establish security management policy,
3) Define information security controls,
4) Implement information security controls,
5) Operation and maintenance for the information security controls,
6) Monitoring and auditing on the information security controls, and
7) Improve information security processes and controls.

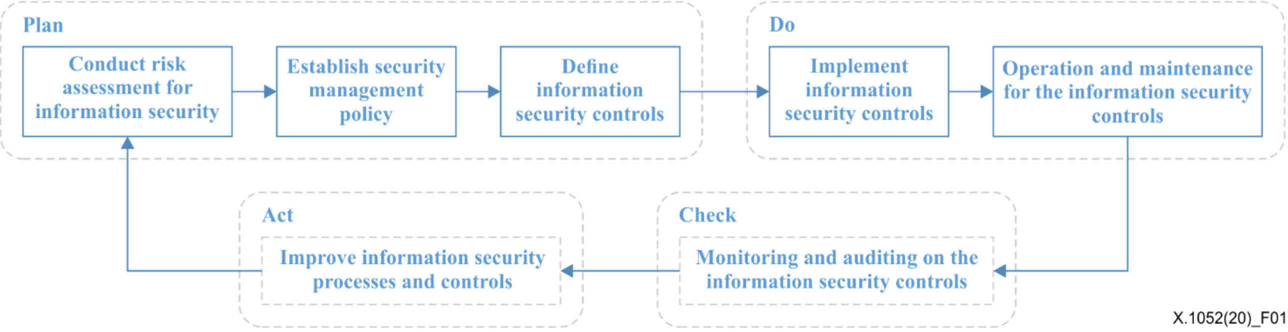
Plan
Conduct risk assessment for information security
Establish security management policy
Define information security controls
Do
Implement information security controls
Operation and maintenance for the information security controls
Act
Improve information security processes and controls
Check
Monitoring and auditing on the information security controls
X.1052(20)_F01

Figure 1 – Organizations' information security management processes

The seven processes in the information security management of telecommunication organizations forms a spirally ascending cycle, which makes the organization's information security management level constantly optimize and improve in the process of its own and environmental changes.

The information security management activities of telecommunication organizations involve many factors which mainly focus on the organization, internal personnel, supply chain, users, resources and business, etc. In the processes of information security management activities, all the factors above should be fully considered according to the activity characteristics of the processes.

Conducting risk assessment for information security is the first step for information security management of telecommunication organizations. Risk assessment is a series of coordinated activities to assess and control the risks an organization faces. These activities include identifying and assessing the value of the information assets, identifying and analysing the threats and vulnerabilities associated with these information assets, assessing security risks, etc.

In the process of establishing security management policy, information security management objectives, guidelines, and overall management requirements should be proposed, which are the basic principles for organizations to conduct information security management.

When defining information security controls, the organization needs to further define the control measures of information security according to the established security management policy and the characteristics of different systems or services. In this process, the organization needs to define the information security management authority of the involved internal personnel and third-party personnel, clarify the methods of user data collection, processing and storage, define the information security control measures in the system or business process, and formulate specific detailed information security management specifications and other documents.

When implementing information security controls, the telecommunication organization should implement controls based on the information security management policy and the specific defined information security control measures. The security management activities of this process include the qualification review of personnel, the strict authorization of personnel, and the development and implementation of the system or business security requirements in accordance with the information security management specifications. In order to reduce risks, it is necessary to assess the realization of security controls before they can be put into actual operations.

In the daily operation and maintenance process, organizations should deal with information security-related activities such as security awareness, education, training, etc., and realize the security operation and management in the actual production operation and maintenance process, and implement protective measures in various aspects such as assets management and data management.

When monitoring and auditing on the information security controls, telecommunication organizations need to confirm the implementation and effectiveness of existing security measures and find information security threats in various aspects such as organization, personnel operations, and resources.

When improving information security processes and controls, telecommunication organizations need to formulate relevant control measures against the information security threats found in the assessment, take protective measures against the information security events that have occurred, draw lessons from the incidents to formulate preventive measures, and improve information security management capabilities continuously over time.

7 Conduct risk assessment for information security

7.1 Purpose

The purpose of this process is to assess and control the risks an organization faces. This includes a series of coordinated activities such as identifying the objects that the organization needs to protect, analysing the threats and vulnerabilities in its technical and management aspects, identifying security risks and suggesting control measures for risks.

7.2 Outcomes

Risk assessment includes the identification and classification of organizational assets, threat and vulnerability identification, and the assessment of their risks. The outputs of this process include the following:

a) List of organizational assets, including general and telecommunication specific assets which are defined in [ITU-T X.1057].

b) Threat and vulnerability identification results for each type of asset.

c) Information security risk assessment results for systems consisting of assets.

7.3 Guideline

Risk assessment activities for telecommunication organizations include the identification of organizational assets, asset classification, vulnerability and threat analysis of each type of asset, risk analysis and evaluation for systems consisting of assets, and risk control recommendations. Asset identification mainly identifies the information security assets of the organization. The asset classification determines its different grades according to the attributes of different assets. Threat analysis is to identify potential events that may lead to negative outcomes. Vulnerability identification is the analysis of the weak points of the various assets which could be damaged by threats. The risk evaluation needs to identify, analyse and evaluate the risks faced by each system which consists of the identified asset. Proposing risk control recommendations is to propose available security measures based on the results of the assessment. The main activities of risk management comprise the management of the following procedures:

a) Asset list identification: refers to the process by which the relevant personnel of the organization identify a comprehensive list of information security assets. In the process of asset list identification, it is necessary to determine the attributes and characteristics of the recorded assets. Generally speaking, the more specific and detailed the list, the greater the effect. Identified assets include not only hardware assets such as computer equipment, communication equipment, storage media, and infrastructure, but also software assets such as operating systems and software, and related data content.

b) Asset classification: Classify assets based on their importance and level to the organization. The results of the classification reflect the importance of assets to the organization and are the basis for the organization to use appropriate resources to protect assets. The importance of an asset is determined by the importance of the asset to the business process or customer service, and the level of protection is determined by the asset's need for security attributes such as confidentiality, integrity, confidentiality, and so on.

c) Threat analysis: Refers to the analysis of potential events that could lead to negative outcomes for various types of assets. Sources of threats include natural threats, man-made threats, and environmental threats. The analysis of threats requires a full consideration of threats to confidentiality, threats to integrity and threats to availability as defined in [ITU-T X.1055]. For telecommunication organizations, in addition to the general types of threats, consideration should also be given to threats introduced due to the particularity of telecommunication networks, such as defects of SS7, pseudo base stations, telecommunication fraud, etc.

d) Vulnerability identification: An analysis of the weak points of the various assets which could be damaged by threats. Vulnerability can be damaging to assets once it is successfully exploited by threats. Vulnerabilities exist in physical environments, organizations, processes, people, management, configuration, hardware, software, and information.

e) Risk evaluation: It is mainly the process of identifying and analysing the risks faced by the systems consisting of various assets and related protective measures. The risks evaluated include information system risk, human resource risk, operational risk, network service risk, physical risk and compliance risk. From the risks faced by the object being evaluated and their associated risk levels.

f) Risk control recommendations: Based on the results of the risk evaluation. Propose alternative security measures for use in developing the security 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 conducting risk assessment

Clause number	Clause title
5	Information security policies
8	Asset management
11.1.4	Protecting against external and environmental threats
12.6	Technical vulnerability management
17	Information security aspects of business continuity management
18	Compliance

8 Establish security management policy

8.1 Purpose

The purpose of this process is to establish the security management policy with the required authority and resources for the development. The security management policy serves as the foundation and core of the organization's information security management and guides the organization's various security management activities.

8.2 Outcomes

The security policy is a collection of security objectives, security management and controls, security management processes, security technology control measures, etc. which are used by telecommunication organizations. It usually appears as a series of different levels of security documents. The result of this process can be divided into multiple levels from abstract to specific, and mainly includes the following aspects:

a) The overall security policy that shows the manager's leadership and commitment to the information security management system.

b) A general security specification that is defined according to the overall security policy. It is usually a higher-level generic specification that can be applied to various systems or services.

c) The relevant procedures, rules, and guidelines for ensuring the implementation of the security regulations which contain the assignment and communication of responsibilities and authorities for information security related roles.

8.3 Guideline

Establishing security management policy should specify the management activities and procedures which include the acquisition, analysis, establishment and approval of security policy requirements and the associated security documentation deriving from this policy.

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

a) Collect and analyse 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 based on the organization's use and execution of the existing policies or based on identifying new security risk and requirements. The main sources of security policies include consideration and definition of the business strategy and objectives of the telecommunication organization, identification and evaluation of the risks which the telecommunication organization faces, the security measures and controls needed to reduce these risks, compliance requirements of the relevant laws, rules and regulations, contractual requirements and obligations, the cultural and societal requirements, and the goals, principles and specific requirements of telecommunication services provided by the organization. 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) Establish the security policy: Establish the relevant security policy based on a detailed analysis of the accepted revisions or new security management and controls, and comprehensive consideration of internal and external organizations, internal personnel, partner personnel, users, systems, services and other factors. If necessary and appropriate, the amendment or establishment of the security policy may need to involve co-operation with suppliers or partners.

c) 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 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.

In all stages involved, the activities should have confirmed the control objectives and the contents of [ITU-T X.1051], as indicated in Table 2.

Table 2 – Clauses of [ITU-T X.1051] related to establishing a security management policy

Clause number	Clause title
5	Information security policies
16.1.1	Responsibilities and procedures
18	Compliance
6.1.1	Information security roles and responsibilities
6.1.2	Segregation of duties
6.1.3	Contact with authorities
6.1.4	Contact with special interest groups
7.1.2	Terms and conditions of employment
11.1.3	Securing offices, rooms, and facilities
11.1.5	Working in secure areas
11.1.6	Delivery and loading areas
15.1.1	Information security policy for supplier relationships
15.1.2	Addressing security within supplier agreements
9.1.1	Access control policy
12.1.1	Documented operating procedures
13.2.1	Information transfer policies and procedures

9 Define information security controls

9.1 Purpose

The purpose of this process is to define the detailed information security controls for different systems, and formulate specific detailed information security management specifications and other documents to be implemented in consideration of the characteristics of different levels of assets in each system for actual construction and development process.

9.2 Outcomes

The information security controls planned for this process should be described as specific security objectives that each system needs to implement, as well as detailed controls on specific security management and technologies that need to be followed. The specific outputs should be reflected in documented detailed security management specifications based on published security management policies, the different features of various systems, and the security risks they face, including:

a) Security plan for the system which defines the security objectives, overall security function requirements that the system needs to achieve, selected security controls which match the system.

b) Security specifications for systems, specifying the specific security techniques and security management measures that the system should adopt in order to achieve security objectives.

9.3 Guideline

Information systems are the basis for telecommunication organizations to carry out services. To ensure the security of their production and operations in the later stages, it is necessary to clarify the needs of security and determine appropriate security control measures during the early planning. The process of defining information security controls should focus on clarifying the security management requirements that the information system needs to meet, analysing the possibility of achieving security requirements, and determining the specific security measures to be taken.

The main activities of this stage comprise the management of the following procedures:

a) Determine the security objectives: Establish the security objectives to be achieved by the information system according to the information security management policy issued by the organization, the relevant risk assessment results, the characteristics of the information system itself.

b) Analyse security function requirements: According to the established security objectives, analyse the security function requirements that the information system should have, including the division strategy of the network security domain, the security equipment and protection measures required at all levels of the network boundary.

c) Implement security plans: Analyse the security control measures that can be taken for each security function requirement, evaluate the realization cost and feasibility of various control measures, and select measures that match the information system to complete the security plans.

d) Review and confirm the security plan: The organization should review the security plan. After approval, the security plan will enter the security specifications preparation section. Otherwise, the proposals that have not passed the review need to be revised.

e) Implement security specifications: Compile specific security specifications based on the identified security function requirements and security plan.

f) Review and publish security specifications: The organization should review and publish the security specifications to the relevant personnel and experts after approval as a basis for later implementation. If the specifications are not approved, the specifications need to be revised.

When defining information security controls, it is necessary to fully consider the relevant security control measures of [ITU-T X.1051] in terms of users, technical means, personnel, partners, etc., as indicated in Table 3.

Table 3 – Clauses of [ITU-T X.1051] related to defining information security controls

Clause number	Clause title
6.1.5	Information security in project management
6.2	Mobile devices and teleworking
9.1.2	Access to networks and network services
9.3	User access management
9.4	System and application access control
10	Cryptography
11.1	Secure areas
12.4.2	Protection of log information
12.6	Technical vulnerability management
13.1	Network security management
13.2.3	Electronic messaging
14.1	Security requirements of information systems
17.1.1	Planning information security continuity
17.2	Redundancies

10 Implement information security controls

10.1 Purpose

The purpose of this process is to implement the information security controls required for the normal operation of the system based on previous planning. Organizations need to complete the management activities of resource allocation, system development, engineering construction and other aspects, and after passing the security acceptance, the information systems, business platforms and related resources will be handed over to the actual production and operation.

10.2 Outcomes

The process of implementing security management and controls needs to complete activities such as resource allocation, system development, system construction, and other related activities. The final outputs include the following aspects:

a) Resources required by the system or platform: physical environment, equipment, personnel, etc.

b) System development documentation, source code: A series of documents and source code completed during the system development process, such as development requirements documents, design documents, test reports, source code, etc.

c) The security function of the system or the security function module of the original system: Various security functions that are actually available.

d) Security acceptance report: The security acceptance report passed by the security function verification of the system in which the details of the methods, results and personnel signature of the security function acceptance are recorded.

10.3 Guideline

In this process, telecommunication organizations need to implement various security controls required to realize the normal operation of the system, including configuring resources according to previously defined objectives, security function requirements, security solutions, security specifications, implementing system security development, and implementing system security construction. Management activities in the following are required:

a) Resources allocation: The organizations need to allocate the required physical environment, personnel and other resources according to the requirements of the system, and ensure that the configured resources meet the needs of information security management.

b) Compile a security development plan: The 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.

c) System security development: The organizations need to implement the system development work according to the development plan, implement the various controls required by the security specification, and also take measures to ensure the security of the development process, documents, and source code to prevent security vulnerabilities and back doors in the code. 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.

d） Security review: After completing the development, the organizations should designate auditors, independent of developers, to carry out a security review 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.

e) Deploying information system: When the system development is completed and put into construction, the organizations should deploy the information system according to security specifications, and control the impact on other existing system. The interface between systems should be strictly controlled.

f) Acceptance of the 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.

In all stages involved, the activities should have confirmed the control objectives and the contents of [ITU-T X.1051], as indicated in Table 4.

Table 4 – Clauses of [ITU-T X.1051] related to implementing information security controls

Clause number	Clause title
11	Physical and environmental security
7.1	Prior to employment
12.1	Operational procedures and responsibilities
14.1	Security requirements of information systems
14.2	Security in development and support processes
14.3	Test data
15.1.2	Addressing security within supplier agreements

11 Operation and maintenance for the information security controls

11.1 Purpose

The purpose of operation and maintenance for the information security controls is to keep the security of information systems effective and efficient. This is important when the system is in daily operation or changes occur.

11.2 Outcomes

Operation and maintenance for the information security controls involves various activities in the daily operation of the system, including security configuration, security changes and others. The specific outputs should be reflected in a series of documents and configuration results generated during the daily operation and maintenance process, including:

a) Security configuration baseline: Defines the various security configuration requirements that need to be observed during system operation;

b) Authority allocation and approver configuration: The account number, authority assignment rules and distribution results of the operators involved in the system are clarified. For the account with high authority such as sensitive information, the configuration of the approver is also included.

c) Network interconnection scheme: Clarify the network interconnection implementation requirements of the system and other networks and applications;

d) Remote access review result: The review result for the remote access requirement is clarified, and the remote access can be allowed only when the review result is allowed.

e) Malware report: Periodically generated malware analysis and processing results for system terminals and servers.

f) Security change plan: The network security change technical plan formulated for the change requirements generated in the security operation, including technical solutions, reversal measures, and scope of influence.

11.3 Guideline

Operations and maintenance for the information security controls include several activities, such as security configuration management, security change management, network interconnection management, remote access management, malware detection and processing, etc. These activities are described as follows:

a) Set up a system security configuration benchmark: Refer to relevant specifications and best practices to form a combination of security configuration items that the information systems and devices in the organization need to comply with. The organizations can establish different levels of security configuration benchmarks based on different levels of systems, equipment, and manufacturers according to the importance;

b) Implement security configuration: According to the security configuration benchmark, perform specific security configuration on each system and device to ensure that each configuration meets the requirements of the security configuration reference.

c) Security authorization management: Formulate the authority allocation rules for the personnel, programs, and interfaces involved in the system, and assign accounts according to the rules. For an account involving sensitive operations, the corresponding operation approver is assigned at the same time, and the behaviour when performing sensitive operations should be reviewed.

d) Network interconnection management. The organizations need to determine the network interconnection rule according to the security policy, analyse the requirements of the business department or the third-party network owner to implement or revoke the network interconnection, formulate the network connection implementation plan and review the plan, and implement it after the review is approved.

e) Remote access management: Collect the requirements and requests for remote access of third parties, mobile working, telecommuting, etc., and authorize the remote access requests according to the organization's remote access rules. Then 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 confidentiality agreement should be signed.

f) Security operation management: Manage various operations during the system operation, especially strengthen the management of assets and take measures to prevent data leakage. When sensitive information is inquired after or operated, the approver should review it. After the approval, the operator can execute it.

g) Malware detection and processing: The organization should regularly check and obtain the latest malware definitions, and perform malware detection and processing on the client and server periodically, and submit malware detection and processing reports to the management level periodically according to the processing results.

h) Security change management: Organizations need to establish security technology solutions required for network changes, according to the change requirements generated during the operation process, the existing network conditions and relevant technical specifications, and implement changes after the test is completed, including system upgrades, version updates, patch updates, etc.

In all stages involved, the activities should have confirmed the control objectives and the contents of [ITU-T X.1051], as indicated in Table 5.

Table 5 – Clauses of [ITU-T X.1051] related to managing operation and maintenance for the information security controls

Clause number	Clause title
7	Human resource security
8	Asset management
9	Access Control
11	Physical and environmental security
12	Operations security
13	Communications security
15.1.2	Addressing security within supplier agreements

12 Monitoring and auditing on the information security controls

12.1 Purpose

The purpose of monitoring and auditing on the information security controls is to confirm the implementation and effectiveness of existing security measures and find information security threats in various aspects.

12.2 Outcomes

The organizations' monitoring and auditing process includes multiple activities to identify items that do not meet the information security control objectives and control requirements, as well as new risks that change over time. The outputs should be reflected as a series of files, including:

a) Security emergency response plan: Security incident emergency plan formulated according to the recovery time objectives and recovery point objectives of different systems, combined with risk control strategies, considering different aspects of the business-related platform system infrastructure, network, system, and business itself.

b) Daily monitoring records: Record information for daily information security monitoring, including abnormal access, abnormal traffic, and various types of network attack behaviours.

c) Security audit results: Regular or irregular information security risk assessment and audit results of operation logs, including compliance usage, high-risk, abnormal or illegal usage, etc.

d) Security event report: Security event summary report after a security event occurs, which records and summarizes the causes, phenomena, treatment methods, and improvement suggestions.

12.3 Guideline

Monitoring and auditing on the information security controls include a series of activities, such as security early warning management, security risk monitoring, log audit, incident emergency response, etc.

a) Security early warning management: Collect early-warning information from the internal security incident processing results, security announcements of software/hardware vendors, or other security organizations. Analyse the impact analysis in conjunction with network security technologies to determine whether it is necessary to adopt additional controls, and release security early-warning reports if adopting additional controls is not imperative. For the security early-warnings that need to adjust the security controls, make recommendations for improvements and perform security configuration management or install patches after review of the suitability, adequacy and rationality.

b) Monitor changes of security configurations. Monitor the status of the implementation of the security configuration profiles on assets and identifying those items that fail to meet the benchmark. If a violation of the security configuration is found, the configuration should be adjusted based on the security benchmark.

c) Monitor remote access status: Check the remote access records regularly to determine whether there is abnormal access, and take necessary measures to correct the problems found in the inspection.

d) Monitor network traffic: Monitor network boundaries, alert in time when receiving access requests that violate boundary policies, and detect suspected attacks. At the same time monitor intranet data traffic, provide early warning when monitoring the transmission of sensitive data in batches, and identify potential existing loopholes.

e) Security audit: Review the implementation of information security management of the system and find any non-compliance or potential risks and form a security audit report periodically or when important events occur, including compliance audits, vulnerability scans, log audits, etc.

f) Incident emergency response: Formulate emergency response plans for information security incidents, organize emergency drills regularly according to emergency plans, and make real-time or near-real-time responses according to the methods and processes defined in [ITU-T X.1056] when related events occur.

In all stages involved, the activities should have confirmed the control objectives and the contents of [ITU-T X.1051], as indicated in Table 6.

Table 6 – Clauses of [ITU-T X.1051] related to monitoring and auditing on the information security controls

Clause number	Clause title
12.4	Logging and monitoring
12.7	Information systems audit considerations
16.1.2	Reporting information security events
16.1.3	Reporting security weaknesses
16.1.4	Assessment of and decision on information security events
16.1.5	Response to information security incidents
17.1.3	Verify, review and evaluate information security continuity

13 Improve information security processes and controls

13.1 Purpose

The purpose of improving information security processes and controls is to keep the information security controls aligned with the organizations' information security management system as the organizations' environment changes over time.

13.2 Outcomes

The process of improving information security processes and controls mainly improves information security elements based on information security incident data, results of security audits, new risks, new threats, and development trends over time. Including system recovery, incident handling, revision of existing information security management solutions and related documents. As a result of the successful performance of this process, the outputs include:

a) Information security controls and capabilities are improved.

b) Information security improvement solution: It defines new controls that should be taken in response to the lack of existing controls, new risks, new threats, etc., including the improvement requirements for various elements of information security management to continuously improve the information security protection capabilities.

c) Records of improving solution deployment: Detailed records of deployment of controls and deployment results.

13.3 Guideline

In the improving information security processes and controls process, telecommunication organizations need to formulate relevant control measures against the information security threats found in the assessment, take protective measures against the information security events that have occurred, draw lessons from the incidents to formulate preventive measures, improve the usability, suitability, adequacy and effectiveness of the information security controls, add missing elements required by changes in the organization's environment, and keep information security management capabilities continuously over time. Some necessary activities need to be carried out, including: summarizing lessons learned, formulating improvement solutions and plans, implementing specific improvement controls, etc. as follows:

a) Summarise experience and lessons: Summarize various types of security early warning information, security audit results, and security incidents, evaluate the shortcomings of existing control measures, analyse whether improvements are needed, and determine whether it is necessary to adjust existing security policies and security programs.

b) Formulate improvement solutions and plans: If improvements are needed, formulate specific information security improvement solutions and plans, and review the adjusted content.

c) Deploy improvement controls: Perform system recovery to restore any capabilities or services that were impaired due to security incidents and modify controls according to the evaluated improvement solutions and plans. For the improved content, it should be documented in a timely manner, and the non-conforming content in various existing documents should be updated.

In all stages involved, the activities should confirm the control of objectives and the contents of [ITU-T X.1051], as indicated in Table 7.

Table 7 – Clauses of [ITU-T X.1051] related to improving information security processes and controls

Clause number	Clause title
16.1.6	Learning from information security incidents
16.1.7	Collection of evidence
17.1	Information security continuity

Bibliography

[b-ISO/IEC 27001] ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*

[b-ISO/IEC 27002] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security management.*

[b-ISO/IEC 27034] ISO/IEC 27034-2:2015, *Information technology – Security techniques – Application security – Part 2: Organization normative framework.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020