International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 13

(09/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

ITU-T X-series Recommendations – Supplement 13

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

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

Supplement 13 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

Summary

Supplement 13 to ITU-T X-series Recommendations provides interpretable guidance for users of Recommendation ITU-T X.1051 with additional explanations and implementation guidance for each clause and control specified in Recommendation ITU-T X.1051. This Supplement is intended to assist telecommunications organizations in the implementation of information security controls based on Recommendation ITU-T X.1051.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 13	2012-09-07	17	11.1002/1000/11754
2.0	ITU-T X Suppl. 13	2018-09-07	17	11.1002/1000/13730

Keywords

ITU-T X.1051, information security controls, users' guide.

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Supplement 13 to ITU-T X-series Recommendations

ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051

1 Scope

The scope of this Supplement is to provide interpretable guidance for users of [ITU-T X.1051]. This Supplement gives additional explanations and implementation guidance for each clause and control specified in [ITU-T X.1051]. This Supplement is intended to assist telecommunications organizations in the implementation of information security controls based on [ITU-T X.1051].

2 References

[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.*

[ISO/IEC 27000] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this Supplement, the definitions given in [ITU-T X.1051] and [ISO/IEC 27000] apply.

3.2 Abbreviations

This Supplement uses the following abbreviations and acronyms:

ASP Application Service Provider

CSIRT Computer Security Incident Response Team

DDoS Distributed Denial of Service

DoS Denial of Service

DMZ Demilitarized Zone

FTP File Transfer Protocol

HTTP Hypertext Transfer Protocol

IDC Internet Data Centre

IP Internet Protocol

IPS Intrusion Prevention System

ISAC Information Sharing and Analysis Centre

ISP Internet Service Provider

LAN Local Area Network

PII Personally Identifiable Information

SIP Session Initiation Protocol

SMTP Simple Mail Transfer Protocol

SSID Service Set Identifier

VoIP Voice over Internet Protocol

VPN Virtual Private Network

4 Overview

4.1 Background

In implementing information security controls for telecommunications organizations, it is essential to take account of telecommunication-specific requirements. Telecommunications organizations, the facilities of which are used by various users to process information such as personal data, confidential data and business data, should handle this information with due care and attention in order to apply an appropriate level of protection.

[ITU-T X.1051] provides guidance for telecommunications organizations to support the implementation of information security controls based on [ISO/IEC 27002]. [ITU-T X.1051] has a format similar to that of [ISO/IEC 27002], and includes additional guidance and telecommunication-specific controls in addition to those contained in [ISO/IEC 27002]. Specifically, this guidance covers:

– cases where objectives and controls specified in [ISO/IEC 27002] are applicable without the need for any additional information and only a reference is provided to [ISO/IEC 27002];
– cases where controls need additional guidance specific to telecommunications; the ISO/IEC 27002 control and implementation guidance are applicable, with the specific telecommunication guidance related to this control; and
– a telecommunication sector-specific set of control and implementation guidance as described in Annex A.

4.2 Structure

This Supplement will assist telecommunications organizations to understand the telecommunication-specific controls and the implementation guidance in [ITU-T X.1051] by providing additional detailed explanations, as well as examples of implementation and best practices.

The structure of clauses 5 to 18 and Appendix I are the same as in [ITU-T X.1051]. This Supplement specifically focuses on those clauses where additional guidance is needed:

– Organization of information security (clause 6);
– Human resources security (clause 7);
– Asset management (clause 8);
– Access control (clause 9);
– Physical and environmental security (clause 11);
– Operations security (clause 12);
– Communication security (clause 13);
– Systems acquisition, development and maintenance (clause 14);
– Supplier relationships (clause 15);
– Information security incident management (clause 16);
– Information security aspects of business continuity management (clause 17);

– Telecommunications extended control set (Appendix I).

5 Information security policies

There is no telecommunication-specific implementation guidance in clause 5 of [ITU-T X.1051].

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

6.1.1 Information security roles and responsibilities

(Refer to control and telecommunications-specific implementation guidance in clause 6.1.1 of [ITU-T X.1051].)

The roles and responsibilities concerning information security carried out by employees who access information systems of the organization and third parties, including employees of contractors, who come in and out of the organization facilities, are provided. The roles and responsibilities of employees and third parties are described in the information security policy document, job description, contract and/or the additional agreement.

Telecommunications organizations should assign staff with the necessary skills and knowledge for the installation, maintenance and operation of telecommunication facilities. Lack of skills and knowledge causes damage or reduction of the telecommunication services. If possible, the skills and knowledge should be certified by the appropriate authorities.

6.1.2 Segregation of duties

There is no telecommunication-specific implementation guidance in clause 6.1.2 of [ITU-T X.1051].

6.1.3 Contact with authorities

(Refer to control and telecommunications-specific implementation guidance in clause 6.1.3 of [ITU-T X.1051].)

The relevant parties to which the organization is required to give notice or report are specified beforehand, and the communication route (from whom to whom) is provided. Examples of the relevant parties could include police stations, fire stations, hospitals, electric companies, national computer security incident response teams (CSIRTs), information sharing and analysis centres (ISACs) and other telecommunications organizations. Other relevant parties could be external contractors including maintenance companies and press organizations. It is desirable that the list of such addresses and telephone numbers be made available on the premises.

On the other hand, telecommunications organizations should be careful about enquiries originating from the authorities because they should ensure the secrecy of communications and the confidentiality of the information of their subscribers.

6.1.4 Contact with special interest groups

There is no telecommunication-specific implementation guidance in clause 6.1.4 of [ITU-T X.1051].

6.1.5 Information security in project management

There is no telecommunication-specific implementation guidance in clause 6.1.5 of [ITU-T X.1051].

6.2 Mobile devices and teleworking

There is no telecommunication-specific implementation guidance in clause 6.2 of [ITU-T X1051].

7 Human resources security

7.1 Prior to employment

Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

7.1.1 Screening

(Refer to control and telecommunications-specific implementation guidance in clause 7.1.1 of [ITU-T X.1051].)

As for access to information systems by third parties, such as employees of contractors, who work in the organization, procedures of approval are provided after evaluation of the risk assessment. After approval, timing of re-evaluation is provided in order to confirm that standards to continue the approval are satisfied.

In telecommunications organizations, failure of systems critical to providing services or leakage of customer information or communicated information may impact a business greatly. Therefore, telecommunications organizations should check especially the candidatures of persons who operate critical systems, or who have access to customer information or communicated information.

7.1.2 Terms and conditions of employment

(Refer to control and telecommunications-specific implementation guidance in clause 7.1.2 of [ITU-T X.1051].)

The basic principles of information security of the organization are explained to employees when they join the company or are transferred within the organization; a code of conduct to this effect is also applicable to them. The document that describes how to act according to the roles and responsibilities provided in clause 6.1.1 of [ITU-T X.1051] is prepared and presented to employees for their signature. Such examples include content of the written oath, observation of the information security rules of the organization, observation of confidentiality, prohibition of disseminating information assets without permission, restriction on bringing personal property into the organization, and upon retirement, the return of any property belonging to the organization. As for temporary staff and employees of contractors who also work in the organization, the basic principles of information security of the organization are explained and the responsibility of conduct is conveyed. As for employees, signature is obtained in a written oath or a non-disclosure agreement, which confirms the understanding of the explanations and compliance with this principle and code of conduct to perform their roles and responsibilities. For further clarification, refer to control in clauses 6.1.1 and 13.2.4 of [ITU-T X.1051].

The document also states the possibility of disciplinary action in case of violation of the security rules once the employee has signed the written oath. The concrete procedures for disciplinary actions are subject to the rules of employment for employees. When there is no employment relationship with the organization, including temporary staff and employees of contractors, the terms and conditions of employment are substituted by a copy of the written oath concluded between the employee and the company that the employee belongs to (see clause 15.1.2 of [ITU-T X.1051]).

Since maintaining telecommunication services and ensuring that the secrecy of communications are particularly important, telecommunications organizations should clarify those responsibilities in the conditions of employment.

7.2 During employment

There is no telecommunication-specific implementation guidance in clause 7.2 of [ITU-T X.1051].

7.3 Termination or change of employment

There is no telecommunication-specific implementation guidance in clause 7.3 of [ITU-T X.1051].

8 Asset management

8.1 Responsibility for assets

Objective: To identify organizational assets and define appropriate protection responsibilities.

8.1.1 Inventory of assets

(Refer to control and telecommunications-specific implementation guidance in clause 8.1.1 of [ITU-T X.1051].)

Each acquisition of information assets should be listed and recorded in the information asset management inventory. The management inventory mainly describes, in addition to the standard attribute information of the information assets, items which may be reviewed with environmental changes and items needed when the information assets are disposed of (Figure 1).

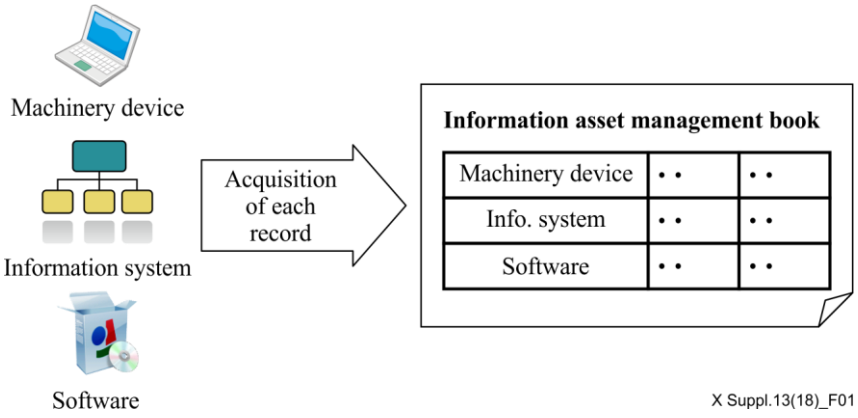

Figure 1 – Information assets recorded in the information asset management book

When new information is made based on a third party's information, an agreement is obtained so as not to violate the third party's intellectual property right.

Telecommunications organizations own many specific assets compared to general organizations. More specific guidance on asset management is found in [b-ITU-T X.1057].

8.1.2 Ownership of assets

There is no telecommunication-specific implementation guidance in clause 8.1.2 of [ITU-T X.1051].

8.1.3 Acceptable use of assets

There is no telecommunication-specific implementation guidance in clause 8.1.3 of [ITU-T X.1051].

8.1.4 Return of assets

There is no telecommunication-specific implementation guidance in clause 8.1.4 of [ITU-T X.1051].

8.2 Information classification

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

8.2.1 Classification of information

(Refer to control and telecommunications-specific implementation guidance in clause 8.2.1 of [ITU-T X.1051].)

Information is classified in terms of business impact and the extent of caution in handling information. Classification guidelines should provide methods and approval procedures for classifying, transferring, retaining and disposing of information, depending on the level of sensitivity and criticality. For the classification of personally identifiable information (PII), legal requirements should be taken into consideration.

The sensitivity and criticality of information is often classified into three to five levels. The scope of disclosure (access rights) of information is set depending on the level of sensitivity and criticality. Moreover, the retention period of information is set in consideration of the deterioration of the sensitivity and criticality level of information as time passes.

In cases of disclosure and retrieval of information of a high degree of importance, approval is obtained from the person in charge depending on the level of sensitivity and criticality.

In general, there are no universal rules for classifying information into several levels; such rules depend on the status of each organization. [b-ITU-T X.1057] provides an example of the asset value level. However, telecommunications organizations should classify the information on secrecy of communication as high severity level. Telecommunications organizations should distinguish essential communications from other communications.

8.2.2 Labelling of information

There is no telecommunication-specific implementation guidance in clause 8.2.2 of [ITU-T X.1051].

8.2.3 Handling of assets

There is no telecommunication-specific implementation guidance in clause 8.2.3 of [ITU-T X.1051].

8.3 Media handling

There is no telecommunication-specific implementation guidance in clause 8.3 of [ITU-T X.1051].

9 Access control

9.1 Business requirement for access control

Objective: To limit access to information and information processing facilities.

9.1.1 Access control policy

(Refer to control and telecommunications-specific implementation guidance in clause 9.1.1 of [ITU-T X.1051].)

The policy that allows users access to the information and the information system is set and documented, as per the requirements in the business and the risk assessment. Usually, the detailed rules are provided in the access control manual, and the policy of access control is stated at the beginning.

The account management policy to firmly implement the access control is provided. For example, management/review/deletion of the user account, management of the administrator account and the method to assign a tentative password are given.

The policy for granting account application and the confirmation procedure are set to limit the access to the information system. Moreover, the details of the tasks of the person in charge who performs the work are provided.

In some cases, telecommunications organizations should give the appropriate access control rules for equipment having many users. For example, the root privilege of an operating system in a mobile phone should not be given to users in order to protect it from being misused or abused.

9.1.2 Access to networks and network services

There is no telecommunication-specific implementation guidance in clause 9.1.2 of [ITU-T X.1051].

9.2 User access management

There is no telecommunication-specific implementation guidance in clause 9.2 of [ITU-T X.1051].

9.3 User responsibilities

There is no telecommunication-specific implementation guidance in clause 9.3 of [ITU-T X.1051].

9.4 Systems and application access control

There is no telecommunication-specific implementation guidance in clause 9.4 of [ITU-T X.1051].

10 Cryptography

There is no telecommunication-specific implementation guidance in clause 10 of [ITU-T X.1051].

11 Physical and environmental security

11.1 Security areas

Objective: To prevent unauthorized physical access, damage and interference in the organization's premises and information processing facilities.

11.1.1 Physical security perimeter

(Refer to control and telecommunications-specific implementation guidance in clause 11.1.1 of [ITU-T X.1051].)

The area where important information and information processing facilities are set up is protected by physical security means. The security level can be improved by providing multiple nest structures. A physical security including this control is often summarized as the "physical security manual".

The boundary of the protected area and the general area is separated such as by a wall, an entrance with any security guard, or doors with a lock or card lock. Further, entrances are illuminated during the night so that trespassing is easily detected.

When a building is newly set up, specifications must include that it meets the security level of the organization. Moreover, in case of transfer to another building or demolition of the building, there needs to be a recorded track that confirms that information assets have been moved safely or disposed of in order to prevent loss of those information assets.

Telecommunication facilities and customer facilities should be clearly separated by physical barriers in order to prevent maintenance staff from entering the telecommunication area. If possible, facilities should be installed on a different floor.

11.1.2 Physical entry controls

(Refer to control and telecommunications-specific implementation guidance in clause 11.1.2 of [ITU-T X.1051].)

Entry into the area which requires high level of security is limited to the person who is authorized access by the administrator, and a record is retained in the administration register. If possible, equipment that automatically administers the entry of each individual should be set up. This history

is saved for a certain period of time to perform a follow-up survey if an information security incident occurs.

The profile of the administrator who authorizes access to the area which requires a high level of security (building, office, server room, etc.) is described in physical and environmental security rules.

As for employees and contracting persons, the procedures concerning issuance and return of building admission cards and correspondences in case of loss are provided. The number of admission cards in use and those returned is confirmed by periodic review of the record taken at the time of issuing and returning of the card (see Figure 2).

When the date and time of entry and departure of the visitors are recorded, the recording paper should be prepared separately for each visitor.

An example of strong entry controls for operation rooms and control centres to operate telecommunication facilities is biometrics.

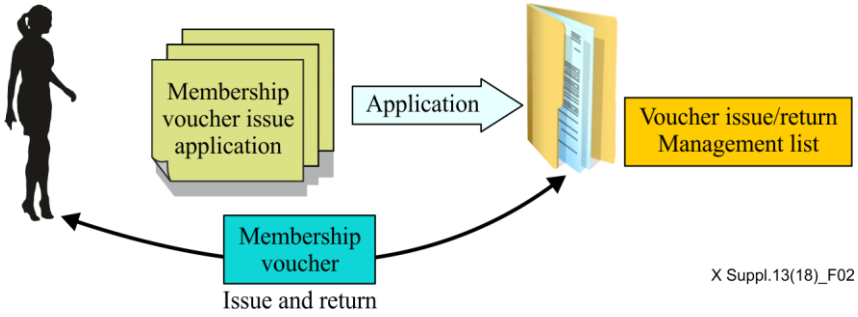

Figure 2 – A record of issuance and return of admission cards

11.1.3 Securing offices, rooms and facilities

There is no telecommunication-specific implementation guidance in clause 11.1.3 of [ITU-T X.1051].

11.1.4 Protecting against external and environmental threats

There is no telecommunication-specific implementation guidance in clause 11.1.4 of [ITU-T X.1051].

11.1.5 Working in secure areas

There is no telecommunication-specific implementation guidance in clause 11.1.5 of [ITU-T X.1051].

11.1.6 Delivery and loading areas

There is no telecommunication-specific implementation guidance in clause 11.1.6 of [ITU-T X.1051].

11.2 Equipment

Objective: To prevent loss, damage, theft or the compromise of assets and interruption to the organization's operations.

11.2.1 Equipment siting and protection

(Refer to control and telecommunications-specific implementation guidance in clause 11.2.1 of [ITU-T X.1051].)

When equipment is installed, it should be protected from physical and environmental threats as well as human threats.

Concrete examples of physical and environmental threats are earthquakes, fires and suspension of electrical power supply and air conditioning. Eating, drinking and smoking are prohibited near important equipment.

Examples of human threats include unauthorized intrusion by any external parties and unauthorized access by any internal person.

Examples of measures of how to protect customer information stored in the telecommunications organizations' systems are as follows:

– equipment should be installed in a locked rack;
– laptop computers should be secured by a wire lock;
– USB ports which are not in use should be blocked physically.

11.2.2 Supporting utilities

(Refer to control and telecommunications-specific implementation guidance in clause 11.2.2 of [ITU-T X.1051].)

Supporting utilities refers to infrastructure facilities such as electricity and air conditioning, necessary for the operations of the equipment. Using the facilities of the organization as well as using the services provided by a third party may be considered. Measures are implemented in order to maintain the operation of the facilities in case of failure of the supporting utilities.

As for electric power equipment, a private electric generator is installed. It is also considered that improvement of the reliability of the power receiving system and priority supply of fuel for the electric generator are included in the agreement and concluded with an electric company or fuel supply company.

Deploying power supply cars as well as private electric generators is effective to prevent power failures in isolated areas such as mobile base stations.

11.2.3 Cabling security

(Refer to control and telecommunications-specific implementation guidance in clause 11.2.3 of [ITU-T X.1051].)

As for the cable for communication or the cable for electricity which connects between information systems, protection measures are taken against interception or damage.

In order to protect cable wiring, it is considered that telecommunications equipment is stored in a rack and locked or cable wiring is installed inside the double floor (Figure 3). During construction, if cable wiring is left on the floor as it is, it may result in an accident. When wiring the cable temporarily, appropriate measures are taken, including passing it overhead and temporarily fixing it in order that the cable is not loosen.

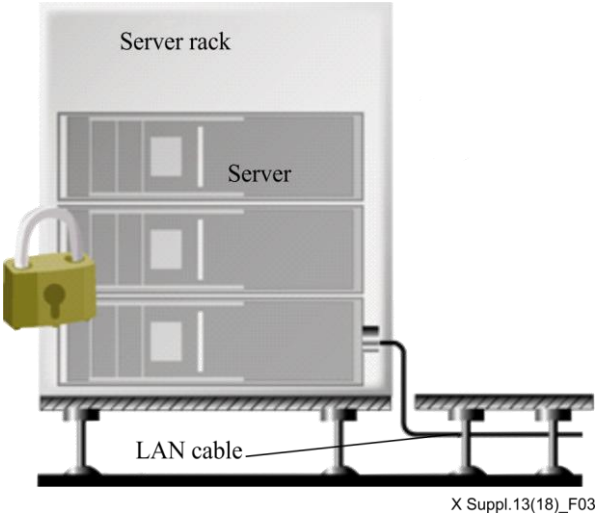

Figure 3 – Cable wiring installed inside the double floor

11.2.4 Equipment maintenance

There is no telecommunication-specific implementation guidance in clause 11.2.4 of [ITU-T X.1051].

11.2.5 Removal of assets

There is no telecommunication-specific implementation guidance in clause 11.2.5 of [ITU-T X.1051].

11.2.6 Security of equipment and assets off-premises

There is no telecommunication-specific implementation guidance in clause 11.2.6 of [ITU-T X.1051].

11.2.7 Secure disposal or re-use of equipment

There is no telecommunication-specific implementation guidance in clause 11.2.7 of [ITU-T X.1051].

11.2.8 Unattended user equipment

There is no telecommunication-specific implementation guidance in clause 11.2.8 of [ITU-T X.1051].

12 Operations security

12.1 Operational procedures and responsibilities

Objective: To ensure correct and secure operations of information processing facilities.

12.1.1 Documented operating procedures

(Refer to Control and Telecommunications-specific implementation guidance in clause 12.1.1 of [ITU-T X.1051].)

As for information systems and network equipment where complicated operations are required that might seriously impact the running of the operations, operating procedures are created for reference by relevant users at any time. Procedures are updated whenever there is a change. Moreover, when performing a series of works which may possibly change the configuration and effect on operation, the operating procedures are verified beforehand and documented.

In application service provider (ASP) business, there are cases where documented procedures are created for each service or operation.

The incident, emergency or crisis handling procedures should quickly be invoked to allow telecommunications organizations to recover from system failures or service degradation. Those procedures should also be tested periodically.

12.1.2 Change management

(Refer to control and telecommunications-specific implementation guidance in clause 12.1.2 of [ITU-T X.1051].)

When information processing equipment and information systems are operating normally, this is considered a stable state. Conversely, when problems occur at the time of execution of some changes, such as changing settings and patching information systems, this is considered a defect. Therefore, at the time of making changes, the implementation plan of the change is made, and prior verification of the change and any event at the time of failure of change are investigated. It is also useful to define procedures in order to restore them to the state before the change is made. In particular, when there is a risk of serious damage, approval procedures are also provided.

When the information system is temporarily suspended for repair of defects, it is best to choose a timeslot when user access is at its lowest. The scheduled start and end time for repairs to be carried out should be specified as well as the extent of the effects. The relevant persons affected by this interruption of services should be notified beforehand in order to minimize the impact on the continuity of services and operation.

Installation, relocation and removal of facilities often cause a change to telecommunication infrastructure such as network topology. Since these changes may result in serious disruption, telecommunications organizations should take extreme care to avoid that disruption.

12.1.3 Capacity management

There is no telecommunication-specific implementation guidance in clause 12.1.3 of [ITU-T X.1051].

12.1.4 Separation of development, testing and operational environments

(Refer to control and telecommunications-specific implementation guidance in clause 12.1.4 of [ITU-T X.1051].)

To maintain security, environments for development, testing and operation are separated. In the development environment, setting for performance verification may be different from that of the commercial environment. In the testing environment, performance under normal and anomalous situations may be verified by executing testing with different loads. To remove this mutual dependency of each environment, the physical environment is separated.

Care should be taken that not only the physical environment is separated but also the settings are separated logically. For example, an access account is not commonly used in each environment, or different IP addresses are assigned to equipment in each environment. Moreover, setting mistakes are prevented by keeping separate setting files for each environment.

When real data are used as the test data in test and development environments, sensitive information (such as personal information or telecommunication records) should be sanitized.

The data which are no longer needed should be deleted immediately.

12.2 Protection from malware

There is no telecommunication-specific implementation guidance in clause 12.2 of [ITU-T X.1051].

12.3 Back-up

There is no telecommunication-specific implementation guidance in clause 12.3 of [ITU-T X.1051].

12.4 Logging and monitoring

Objective: To record events and generate evidence.

12.4.1 Event logging

(Refer to control and telecommunications-specific implementation guidance in clause 12.4.1 of [ITU-T X.1051].)

Procedures to obtain audit logs of system usage are provided to confirm the effectiveness of access control concerning system usage and to investigate any information security incident when it occurs. The procedures include objective items and retention period of logs.

Examples of objective items for log collection include firewall, servers, gate devices and monitoring cameras. Logs which have a high level of confidentiality are stored in a dedicated server on the segment to which access is impossible from outside.

Telecommunications organizations should establish the data retention period correctly, depending on its purpose. Keeping sensitive data for an extended period of time increases the risk of its disclosure or misuse.

12.4.2 Protection of log information

There is no telecommunication-specific implementation guidance in clause 12.4.2 of [ITU-T X.1051].

12.4.3 Administrator and operator logs

There is no telecommunication-specific implementation guidance in clause 12.4.3 of [ITU-T X.1051].

12.4.4 Clock synchronization

There is no telecommunication-specific implementation guidance in clause 12.4.4 of [ITU-T X.1051].

12.5 Control of operational software

Objective: To ensure the integrity of operational systems.

12.5.1 Installation of software on operational systems

(Refer to control and telecommunications-specific implementation guidance in clause 12.5.1 of [ITU-T X.1051].)

If operational software is implemented or added, there is a possibility of an increased risk to the system in operation. Therefore, procedures to minimize the risk are provided.

The procedures include appointment of the management administrator for operational software, change and addition of operational software with the approval of the security administrator, and retention of the old version of the operational software for a certain period of time as a precautionary measure in case of any accidents.

Telecommunication service systems, such as a switching facility, may receive unexpected data from other systems. Upon software installation, the test scenario should cover all possible paths to avoid unexpected failure of the systems.

12.6 Technical vulnerability management

Objective: To prevent exploitation of technical vulnerabilities.

12.6.1 Management of technical vulnerabilities

There is no telecommunication-specific implementation guidance in clause 12.6.1 of [ITU-T X.1051].

12.6.2 Restrictions on software installation

(Refer to control and telecommunications-specific implementation guidance in clause 12.6.2 of [ITU-T X.1051].)

12.7 Information systems audit considerations

Telecommunication-specific implementation guidance is not included in clause 12.7 of [ITU-T X.1051].

13 Communication security

13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

13.1.1 Network controls

There is no telecommunication-specific implementation guidance in clause 13.1.1 of [ITU-T X.1051].

13.1.2 Security of network services

(Refer to control and implementation guidance in clause 13.1.2 of [ITU-T X.1051].)

When using network services, verification is made to ensure that the security function provided by the service satisfies the requirements of the organization. For example, network services in this

context include line services (Ethernet, virtual private network (VPN)), IP telephone services, meeting services and content delivery services.

For the verification that the security function is well maintained, execution of audits and reviews is provided beforehand. In particular, when using network services provided by a third party, an agreement with the third party is concluded concerning the procedures.

Telecommunications organizations could also be in a position to provide network services to their customers. Therefore, ensuring not only the availability of network services but also the confidentiality of the user's communication (for example, session initiation protocol (SIP), for voice over Internet protocol (VoIP) service and VoIP traffic) are important.

13.1.3 Segregation in networks

(Refer to control and telecommunications-specific implementation guidance in clause 13.1.3 of [ITU-T X.1051].)

When the network is built, unnecessary accesses can be limited by portioning the domain of each group, and expansion of damage can be prevented by separating the network in abnormal cases.

A network is roughly divided into the network outside the company (internet connection, etc.) and the in-house network. Further, the in-house network is divided into the company-wide network and the network of each department. Network interactions are partitioned and connected by routers, switches, firewalls, etc.

It is recommended that the purpose of each network, that is, the idea of its connection framework and available network services should be provided. Available network devices and the method to set up the demilitarized zone (DMZ) are given as examples of the idea of a connection framework. Moreover, as examples of network services, the enumeration of the hypertext transfer protocol (HTTP), simple mail transfer protocol (SMTP), file transfer protocol (FTP), etc. at the protocol level is considered.

13.2 Information transfer

Objective: To ensure information security events and weaknesses associated with information.

13.2.1 Information transfer policies and procedures

There is no telecommunication-specific implementation guidance in clause 13.2.1 of [ITU-T X.1051].

13.2.2 Agreements on information transfer

There is no telecommunication-specific implementation guidance in clause 13.2.2 of [ITU-T X.1051].

13.2.3 Electronic messaging

There is no telecommunication-specific implementation guidance in clause 13.2.3 of [ITU-T X.1051].

13.2.4 Confidentiality or non-disclosure agreements

There is no telecommunication-specific implementation guidance in clause 13.2.4 of [ITU-T X.1051].

14 Systems acquisition, development and maintenance

14.1 Security requirements of information systems

There is no telecommunication-specific implementation guidance in clause 14.1 of [ITU-T X.1051].

14.2 Security in development and support processes

There is no telecommunication-specific implementation guidance in clause 14.2 of [ITU-T X.1051].

14.3 Test data

There is no telecommunication-specific implementation guidance in clause 14.3 of [ITU-T X.1051].

15 Supplier relationships

15.1 Information security in supplier relationships

Objective: To ensure protection of the organization's assets that is accessible by suppliers.

15.1.1 Information security policy for supplier relationships

(Refer to control and telecommunications-specific implementation guidance in clause 15.1.1 of [ITU-T X.1051].)

15.1.2 Addressing security within supplier agreements

(Refer to control and telecommunications-specific implementation guidance in clause 15.1.2 of [ITU-T X.1051].)

As for temporary staff and employees of the entrusted company who have not concluded an agreement with the organization, requirements concerning information security are described in the agreement with the company they belong to. This includes that a written oath concerning the information security observance is signed between the companies that the temporary staff belongs to or the contractor and the employee (see clause 8.1.3 of [ITU-T X.1051]).

Execution of the information security audit on a third party to whom work is consigned is described in the agreement. Moreover, the timing in which the information security audit is executed is provided. Additionally, items concerning improvement of information security maintenance are described in the agreement.

When telecommunications organizations allow a third party to access the organization's assets, it is possible that the third party could, through negligence or malice, suspend telecommunication services or degrade their quality. Telecommunications organizations should consider those concerns when making agreements with third parties.

15.1.3 Information and communication technology supply chain

There is no telecommunication-specific implementation guidance in clause 15.1.3 of [ITU-T X.1051].

15.2 Supplier service delivery management

There is no telecommunication-specific implementation guidance in clause 15.2 of [ITU-T X.1051].

16 Information security incident management

16.1 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach to the management of information security incidents including communication on security events and weaknesses.

16.1.1 Responsibilities and procedures

(Refer to control and telecommunications-specific implementation guidance in clause 16.1.1 of [ITU-T X.1051].)

With respect to the report of occurrence of information security incidents, the countermeasures are implemented promptly and precisely. Moreover, the response procedures of the organization are provided to be used as a learning experience from the information security incident (Figure 4).

The response procedures can be broadly classified into in-house procedures and external procedures. Examples of in-house procedures are in-house escalation of occurrence situations, analysis/specification of causes and scale of damage, investigation/indication of re-occurrence prevention measures, confirmation of validity of re-occurrence prevention measures, etc.

It is also recommended that the possible information security incidents are categorized into patterns, and the response procedures are considered based on the scale of the damage. Examples of information security incident patterns are cyber-attacks including virus, denial of service/distributed denial of service (DoS/DDoS), failure of information systems, loss/theft of information assets and leakage of personal information. Examples of external procedures involve contacting the relevant parties, creation of news releases, apologies and reports to clients or other related persons.

In some cases, it is the customers who notify the incident to the telecommunications organizations. Therefore, the information on reporting procedures from customers should be published. Since it is difficult to deal with all customers' reports when a major failure happens, telecommunications organizations should prioritize customer reporting in advance.

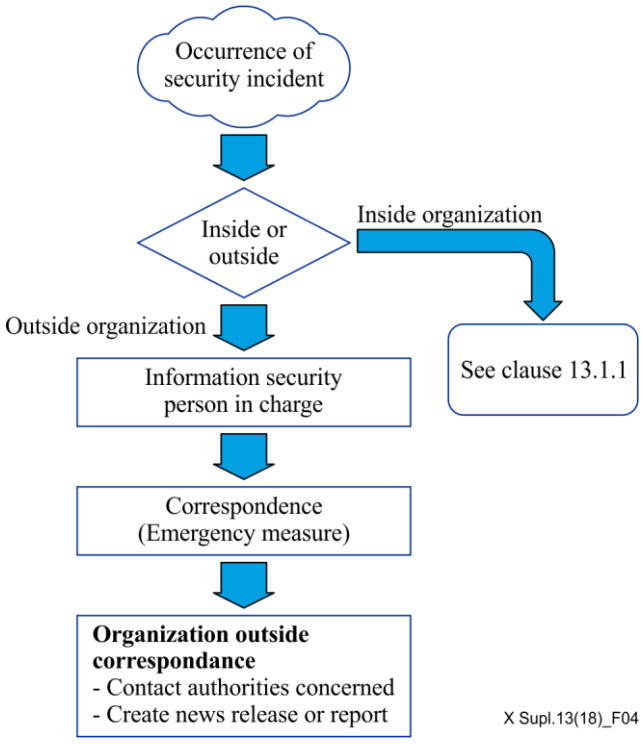

Figure 4 – Response procedures to information security incidents

16.1.2 Reporting information security events

There is no telecommunication-specific implementation guidance in clause 16.1.2 of [ITU-T X.1051].

16.1.3 Reporting security weaknesses

There is no telecommunication-specific implementation guidance in clause 16.1.3 of [ITU-T X.1051].

16.1.4 Assessment of and decision on information security events

(Refer to control and telecommunications-specific implementation guidance in clause 16.1.4 of [ITU-T X.1051].)

16.1.5 Response to information security incidents

(Refer to control and telecommunications-specific implementation guidance in clause 16.1.5 of [ITU-T X.1051].)

16.1.6 Learning from information security incidents

(Refer to control and telecommunications-specific implementation guidance in clause 16.1.6 of [ITU-T X.1051].)

When a series of countermeasures immediately after the occurrence of the information security incident are completed, an information security incident report is created so that it can be used as a reference at a later date.

Examples of descriptions in the information security incident report are attributes of the event (date and time of occurrence, target information assets, reported by, damage scale), details of the event, response measures, operational costs for the response, cause analysis, details of corrective measures and validation of effectiveness of the corrective measures.

Since the information security incident report contains information about the vulnerabilities of the organization, this information security incident report should be handled carefully.

16.1.7 Collection of evidence

There is no telecommunication-specific implementation guidance in clause 16.1.7 of [ITU-T X.1051].

17 Information security aspects of business continuity management

17.1 Information security continuity

Objective: Information security continuity should be embedded in the organization's business continuity management systems.

17.1.1 Planning information security continuity

There is no telecommunication-specific implementation guidance in clause 17.1.1 of [ITU-T X.1051].

17.1.2 Implementing information security continuity

(Refer to control and telecommunications-specific implementation guidance in clause 17.1.2 of [ITU-T X.1051].)

In the business continuity plan created by the organization, the information security incident is assumed as one of the risks and response measures before and after the incident are established. The effect of the risk on business processes is studied based on the business impact analysis. In the event of interruption, the time required to recover the connection within the organization and with other organizations, or with external companies, is calculated and the final target recovery time is set. Furthermore, measures to realize the target recovery time are studied and implemented. Moreover, in performing the plan, a schedule is prepared based on the time and budget.

Examples of realizing information availability include the establishment of a secondary server and duplexing of the data centre.

In developing and implementing the business continuity plan, telecommunications organizations should consider that a critical part of the communication (in accordance with the rules and regulations, such as emergency calls and public service calls) should be restored in preference to full recovery of services.

17.1.3 Verify, review and evaluate information security continuity

There is no telecommunication-specific implementation guidance in clause 17.1.3 of [ITU-T X.1051].

17.2 Redundancies

Objective: To ensure the availability of information processing facilities.

17.2.1 Availability of information processing facilities

(Refer to control and telecommunications-specific implementation guidance in clause 17.2.1 of [ITU-T X.1051].)

18 Compliance

There is no telecommunication-specific implementation guidance in clause 18 of [ITU-T X.1051].

Appendix I

Telecommunications extended control set

This appendix provides a users' guide for the telecommunications extended control set that is described in Annex A of [ITU-T X.1051]. The structure of the appendix follows that of Annex A of [ITU-T X.1051].

TEL.9 Access control

TEL.9.1 Network access control

Objective: To prevent unauthorized access to networked services.

TEL.9.5.1 Telecommunications carrier identification and authentication by users

(Refer to control and implementation guidance in clause TEL.9.5.1 of [ITU-T X.1051].)

When common equipment connected to multiple telecommunications organizations is employed, a method by which the applicable telecommunication provider is identified and authenticated by the user should be adopted.

The following descriptions are for Internet service providers (ISPs).

– For example, multiple providers can be selected at the access point of the public wireless local area network (LAN) that is commonly used by providers. Authentication is required to guarantee that the provider that offers such access points is the telecommunication provider having the contract where the user is connected. Moreover, when the service of the provider that offers the access point is used, the telecommunication provider is authenticated. Service set identifier (SSID) and multi-SSID are examples of the authentication methods.

TEL.11 Physical and environmental security

TEL.11.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

TEL.11.1.7 Securing communication centres

(Refer to control and implementation guidance in clause TEL.11.1.7 of [ITU-T X.1051].)

To provide stable telecommunication services continuously, telecommunication equipment is set up in the building where physical security is assured. In this case, the physical security includes robust foundations, implementation of measures to address natural disasters such as earthquake, flood and storm, fireproof measures, structural tolerance to heavily-weighted floors and structures not adjacent to facilities where dangerous articles are preserved. The selection of a location that can be easily accessed in an emergency situation is also considered.

The following descriptions are for ISPs and ASPs.

– When moving into a building designed and constructed for the installation of telecommunication facilities (for instance, a telecommunications organizations' building), it may be considered that physical security measures have been implemented on the premises. If the establishment of the telecommunication equipment at the data centre has been done by a third party such as an Internet data centre (IDC), implementation of the physical security is required and described in the specifications (see clause 6.2.3 of [ITU-T X.1051]). When

physical security specifications are not mentioned in the agreement, moving into the third party's building should be postponed.

The following descriptions are for IDCs.

– When moving into a building designed and constructed for the installation of telecommunication facilities (for example, a telecommunications organizations' building), it may be considered that the physical security measures have been implemented. Displays of any element that might indicate its existence should be avoided to prevent one from considering it as a data centre building.

– When moving into a newly constructed building or using a floor with a large surface area, telecommunications organizations participation in the design stage and floor construction is important to ensure physical security and satisfaction of the organization's requests.

TEL.11.1.8 Securing telecommunication equipment room

(Refer to control and implementation guidance in clause TEL.11.1.8 of [ITU-T X.1051].)

To provide stable telecommunication services continuously, the telecommunication equipment is set up in a room where physical security is assured. In this context, the physical security measures include a "no entry" sign by unauthorized third parties, safeguards against floods or falling objects due to earthquakes, measures against static electricity and use of flame resistant or non-flammable material for floors, walls, ceilings and ducts with fire prevention measures.

The following descriptions are for ISPs and ASPs.

– When using a floor with a large surface area in a newly constructed building, the design stage of the building and floor construction is important so that physical security is assured and requirements of the organization have been met. Moreover, it is recommended to verify that the room is protected from strong electromagnetism by an electromagnetic shield.

– To prevent fire from damaging cables and spreading, fire prevention measures on cables, ducts and other related items should be taken according to the relevant legislation or regulations. Moreover, spreading of fire can be prevented by physically dividing the server rooms into individual blocks.

– Though halon fire extinguishing equipment has been in use as fire extinguishing equipment, nitrogen fire extinguishing equipment is also used. Moreover, it is also effective to introduce a mechanism for early fire detection, even though the air conditioner is circulating air in the room.

– To prevent equipment from being damaged due to the occurrence of static electricity, in addition to establishing a static electricity removal mat in the equipment room or wearing antistatic shoes when entering the room, wearing an antistatic strap is essential when touching the device or touching a frame earth before doing any preparatory work.

– In choosing a data centre, issues such as management of secure room entry and exit and prevention of illegal intrusion, and implementation of measures concerning redundancy of air-conditioning and power supply are considered.

The following descriptions are for IDCs.

– To prevent fire from damaging cables and spreading, fire prevention and fireproof measures on cables, ducts and other related items should be taken according to the relevant legislation or regulations. Moreover, spreading of fire can be prevented by physically dividing the server rooms into individual blocks.– Though halon fire extinguishing equipment has been used as fire extinguishing equipment, nitrogen fire extinguishing equipment is also used. Moreover, it is also effective to introduce a mechanism for early fire detection, even though the air conditioner is circulating air in the room.

– To prevent equipment from being damaged due to the occurrence of static electricity, in addition to establishing the static electricity removal mat in the equipment room or wearing antistatic shoes when entering the room, wearing an antistatic strap is essential when touching the device or touching a frame earth before doing any preparatory work.

TEL.11.1.9 Securing physically isolated operation areas

(Refer to control and implementation guidance in clause TEL.11.1.9 of [ITU-T X.1051].)

To provide telecommunication services, in case telecommunication equipment is set up outdoors, the equipment should be designed and operated in such a way that physical security of those facilities is maintained. As is normally the case, the maintenance worker of the organization cannot maintain and monitor the equipment daily; it is therefore required to ensure remote control of the equipment to detect problems. An example is a base station for mobile phones.

The following description is for ISPs.

– An ISP, which has access points of wireless LANs, implements measures to protect access point equipment. An ISP, which uses access points of wireless LANs offered by third parties, requires the third party's implementation of measures to protect access point equipment, as described in the specifications, and verifies the details of the implementation (see clause 6.2.3 of [ITU-T X.1051]).

TEL.11.3 Security under the control of other party

Objective: To protect equipment located outside of the telecommunications organizations' premises (e.g., co-locations) against physical and environmental threats.

TEL.11.3.1 Equipment sited in other carrier's premises

(Refer to control and implementation guidance in clause TEL.11.3.1 of [ITU-T X.1051].)

When setting up devices in other vendors' premises, telecommunications organizations should protect the selected location to reduce risks caused by environmental threats and illegal access.

The following descriptions are for ISPs and ASPs.

– When renting a floor unit in another vendor's building, intruder access can be prevented by ensuring that the elevator cannot stop at the rented floor. Also, in case of renting a portion of a floor, environmental threats can be reduced by partitioning the room individually and isolating the power supply and network.

TEL.11.3.2 Equipment sited in user premises

(Refer to control and implementation guidance in clause TEL.11.3.2 of [ITU-T X.1051].)

When telecommunications organizations set up their own devices in the area of the subscriber to connect to telecommunication devices of the subscriber, those devices should be protected to reduce risks caused by environmental threats and dangers and the possibility of unauthorized access.

The following descriptions are for ISPs.

– Examples of devices installed in the subscriber's area include rental devices, such as rental routers and set-top boxes. In this case, even though the location of the installation of these devices is decided by the subscriber, their installation should conform to the recognized standards.

– Management of rental devices is the responsibility of the subscribers, and response measures in case of defects are also specified in the subscriber's contract. Modifications to the terms of the rental devices are also specified in the agreement.

TEL.11.3.3 Interconnected telecommunications services

(Refer to control and implementation guidance in clause TEL.11.3.3 of [ITU-T X.1051].)

In providing interconnected telecommunication services, telecommunications organizations should clearly define boundaries and interfaces with other operators.

The following description is for ISPs.

– As for peer-to-peer connections, in case of abnormal traffic from other vendors, measures such as blocking the device port and changing the routing are considered to protect the telecommunications organizations' network. It is always necessary to monitor traffic from connected peers.

TEL.13 Communications and operations management

TEL.13.1 Network security management

Objective: To ensure the protection of information in networks and its supporting information processing facilities.

TEL.13.1.4 Security management of telecommunications services delivery

(Refer to control and implementation guidance in clause TEL.13.1.4 of [ITU-T X.1051].)

Telecommunications organizations define the security level of the telecommunication services they provide to the subscribers and explain the terms of reference of telecommunication services before providing those services. Telecommunications organizations adequately maintain and manage the telecommunication services. The organization's security rules and handling policies of personal information are stipulated in the service clauses or the subscriber's contract.

The following descriptions are for ISPs.

– Information to educate users is posted on the organization's website so as to avoid using the Internet for criminal purposes and damages due to spam and viruses.

– A measure against spam is often executed as a basic service menu.

The following descriptions are for IDCs.

– Measures that may be taken in case of flaws in the subscriber's contract in order to make it possible to suspend or cancel the usage.

– Measures concerning spam, DDoS and vulnerabilities may be taken at the responsibility of the users.

– Constant monitoring is necessary so that traffic is not congested at the connection with a higher backbone. If traffic congestion occurs, provision of stable services is maintained by increasing bandwidth, cooperating with higher backbone providers or the like.

– It is recommended to prepare spare cables in the server room.

TEL.13.1.5 Response to spam

(Refer to control and implementation guidance in clause TEL.13.1.5 of [ITU-T X.1051].)

To maintain an e-mail friendly environment, measures against spam are provided and proper controls, such as the introduction of technology to block spam, are implemented.

The following descriptions are for ISPs.

– Prohibited acts are stipulated in the subscriber's contract. Measures against nuisance acts are published on the homepage. Measures against spam are also published on the homepage as one of the measures against nuisance acts.

– In cases where spam e-mails are sent by subscribers in the company, standards are set, and the sender is specified to promptly abort the transmission. In this case, notices from users and reports from the person in charge of support are referred to. The contract may be cancelled by providing standards concerning contract cancellation.
– In cases where spam e-mails are sent by other providers having mutual connections, a request is made for the provider to stop sending spam e-mails.

TEL.13.1.6 Response to DoS/DDoS attacks

(Refer to control and implementation guidance in clause TEL.13.1.6 of [ITU-T X.1051].)

For a stable provision of telecommunication services, policies against DoS/DDoS attacks are provided and appropriate measures are implemented.

The following descriptions are for ISPs.

– Traffic is constantly monitored and when a DoS/DDoS attack is detected, technical measures are voluntarily implemented. The measures taken in the case of an attack from within the company network or from networks of other companies are separately provided. Detailed measures, such as reduction of traffic (port closure, use of firewall and intrusion prevention system, IPS) can be taken and collaboration between providers can occur.
– Measures are provided in case of bot virus infection. For example, verification of true or false information, establishment of measures and procedures to correspond with subscribers, are given.
– An ISP which implements measures when the network bandwidth becomes insufficient due to DoS/DDoS attack is selected and described in the contract (see clause 6.2.3 of [ITU-T X.1051]).

TEL.18 Compliance

TEL.18.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations related to information security and of any security requirements.

TEL.18.1.6 Non-disclosure of communications

(Refer to control and implementation guidance in clause TEL.18.1.6 of [ITU-T X.1051].)

In accordance with legislation or regulations of the country or region where telecommunication services are provided, the telecommunications organizations shall protect the privacy of the communications they handle. The protection of the privacy of communications is also described in the rules of employment. Furthermore, subject to applicable legislation or regulations, the obligation to protect the privacy of communications continues even after the engagement with the telecommunications organization is terminated.

TEL.18.1.7 Essential communications

(Refer to control and implementation guidance in clause TEL.18.1.7 of [ITU-T X.1051].)

It is desirable that telecommunications organizations give priority to communications of emergency situations such as natural disasters, accidents or the probability of such occurrences. Important communications in this context refer to communications related to the prevention of disasters or disaster relief (e.g., securing transportation, communications, electrical supplies or preservation of public safety).

TEL.18.1.8 Legality of emergency actions

(Refer to control and implementation guidance in clause TEL.18.1.8 of [ITU-T X.1051].)

When prompt support is required in the event of emergency situations such as cyber-attacks, it is desirable that the measures taken are the most appropriate ones.

Measures to be taken in case of power failure, cable disconnection, fire, earthquake, temporary breakdown of equipment and information leakage are provided in the business continuity plan.

Incidents occurring on a daily basis are dealt with in accordance with the predefined procedures and the contract terms.

Any other emergency incidents are dealt with in accordance with the business continuity plan. The procedure is provided after confirming its appropriateness with the person in charge of legal affairs in the organization, if necessary.

The possibility of disconnection of services in case of emergency is mentioned in the subscriber's contract. The appropriateness of the rules is confirmed with the person in charge of legal affairs in the organization.

Bibliography

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

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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	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, 2018