International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1057

(05/2011)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Asset management guidelines in telecommunication organizations

Recommendation ITU-T X.1057

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	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1057

Asset management guidelines in telecommunication organizations

Summary

Recommendation ITU-T X.1057 provides guidelines for securely managing various assets, including electronic information, paper, and IT systems in telecommunication organizations. This Recommendation also describes the main activities and methods for implementing asset management on the basis of the PDCA (Plan – Do – Check – Act) process model.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1057	2011-05-29	17

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

© ITU 2012

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

Table of Contents

Recommendation ITU-T X.1057

Asset management guidelines in telecommunication organizations

1 Scope

Telecommunication organizations should have very high goals for operating and managing their various assets, for providing customer services and for directly or indirectly supporting their business. It is necessary to protect those assets critical to telecommunication organizations in order to ensure that the operations and services of the telecommunication business are not compromised.

This Recommendation provides an overview of processes and methods that need to be addressed in place to identify, classify, evaluate and maintain the assets that telecommunication organizations own. This Recommendation also suggests some templates as a method for managing assets.

2 References

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

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

[ISO/IEC 27000] ISO/IEC 27000:2009, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 asset [ISO/IEC 27000]: Anything that has value to the organization.

NOTE – There are many types of assets, including:

a) information (2.18);

b) software, such as a computer program;

c) physical, such as computer;

d) services;

e) people, and their qualifications, skills, and experience; and

f) intangibles, such as reputation and image.

3.1.2 policy [ISO/IEC 27000]: Overall intention and direction as formally expressed by management.

3.1.3 telecommunications equipment room [ITU-T X.1051]: A part of general building such as a room where equipment for providing telecommunications business are sited.

3.1.4 telecommunications facilities [ITU-T X.1051]: Machines, equipment, wire and cables, physical buildings or other electrical facilities for the operation of telecommunications.

3.1.5 user [ITU-T X.1051]: Person or organization who utilizes information processing facilities or systems, e.g., employee, contractor or third party user.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 asset manager: A person or an organization who is designated by an asset owner for secure management and protection of the asset.

3.2.2 asset owner: A person or an organization who has the ownership and a final obligation of asset management such as asset acquisition, permit of asset use, disposal or discard of asset, etc.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AMP	Asset Management Process
AP	Access Point
AVL	Asset Value Level
CCTV	Closed Circuit Television
CMTS	Cable Modem Termination System
DBMS	Database Management System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ESM	Enterprise Security Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISMS	Information Security Management System
IT	Information Technology
NAS	Network Access Server
NMS	Network Management System
NTP	Network Time Protocol
OS	Operating System
PC	Personal Computer
PDCA	Plan – Do – Check – Act
RAS	Remote Access Server
R&R	Role and Responsibility
SLA	Service Level Agreement
UPS	Uninterruptible Power Supply
VPN	Virtual Private Network
WAS	Web Application Server

5 Conventions

None.

6 Overview of asset management

An asset is a component or part to which an organization directly assigns a value. An organization includes its assets having their own unique values from the various viewpoints of business, financial affairs, reliability and so on. It can be said that the main information and communication facilities within the scope of the ISMS (information security management system) have higher values than other assets. When accidents happen, such assets have great influences on not only users but organization business. Therefore, these assets have high protection priorities. Most organizations strive to find the best methods to identify the main assets that have high protection priorities. The goal of asset management is to identify and protect the most critical components of the organization so that they offer services to their business without any problem. Regarding the importance of assets, a function based on main services and the value of the business should be considered, covering:

- impact on service – Service scope which each asset affects;
- loss of profit – Degree of financial loss;
- loss of customer – Possibility of customer loss;
- image – Damage of an organization's image.

6.1 Concept of asset management process

In general, an asset has value if it is actively used for business and services in an organization. Asset management refers, from the viewpoint of information security, to the appropriate handling and protection measures considering the asset value in the scope defined by telecommunication organizations. In order to systematically and securely manage the various and large number of assets included in an organization, the assets should be managed according to an asset life cycle, which corresponds to a process of acquisition or generation, change, disposal or destruction of the asset. In an organization, while a series of management processes is applied on assets, it is required that certain standards and rules be determined. The asset management process and its alignment to the PDCA model is described in Figure 1.

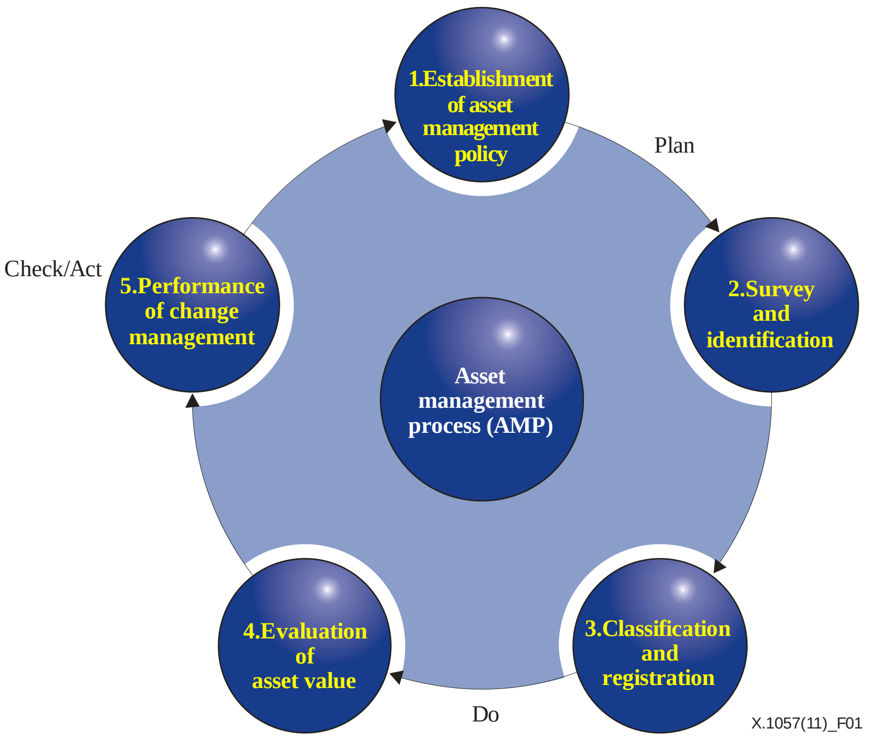
1.Establishment of asset management policy
Plan
2.Survey and identification
3.Classification and registration
Do
4.Evaluation of asset value
5.Performance of change management
Check/Act
Asset management process (AMP)
X.1057(11)_F01

Figure 1 – Concept of AMP

6.2 Main activities in the asset management process

There are five steps in the asset management process. Some important activities in each step are required for performing asset management. The key activities in each step are:

a) Establish the policy for asset management:

   i) define procedures and methods for handling the assets;

   ii) appoint the asset manager responsible for the management of assets;

   iii) define the classification criteria in consideration of asset type;

   iv) define the criteria for evaluating the asset value level;

   v) define the role and responsibility of the asset manager;

   vi) define the range or scope of the asset to be managed.

b) Survey and identify the assets:

   i) survey all assets comprehensively in the established scope of asset management;

   ii) recognize and select the assets to be managed;

   iii) cooperate with related teams or departments when surveying assets;

   iv) give a name to the identified asset and create an asset register or inventory.

c) Classify and register the assets:

   i) draw up an asset list based on the predefined criteria for asset classification;

   ii) register the basic and additional maintenance information of each asset (see Appendix II);

   iii) consider the grouping strategy and label for identified assets by using physical or logical means, for effective handling.

d) Evaluate the importance level for the asset:

   i) assess the importance of the asset with respect to the security requirements;

   ii) grant the value level to each asset in order to apply the appropriate security measures;

iii) always reassess the value of the the asset, if its status has changed.

e) Perform change management:

i) periodically check the status of assets;

ii) update the results to an asset register, if the status of any asset has changed;

iii) find and report new issues for improving the asset management policy and process.

7 Asset management process

7.1 Establishment of asset management policy

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

a) A procedure should be established for managing the assets according to their lifecycle, including creation and registration, change, and disposal of the assets.

b) An asset manager having the role of asset owner for security purposes should be assigned.

c) Assets should be classified and managed by their types so as to systematically manage the assets. In this case, consistent criteria in consideration of the asset types managed by each telecommunication organization should be prepared, for the purpose of effective asset classification.

d) The criteria for evaluating the importance of the identified asset should be established and the criteria for assigning a security level to the assets should be established, for the purpose of managing the assets in accordance with the security level of the assets.

e) The asset owner is comprehensively responsible for the corresponding assets. The asset owner may appoint and entrust the asset manager to manage them. The appointed asset manager should be able to acquire the responsibility of asset protection and to continuously maintain the asset security.

f) The asset manager should define the range or scope of the asset to be managed, in relation to the application of asset management policies. When defining the scope of asset management, it is necessary to consider all aspects of the organization's business and the security of the assets.

7.2 Survey and identification

There are very many assets, such as IT systems, in telecommunication organizations. In order to effectively protect the assets, it is first necessary to survey and identify overall assets within the security boundary established for risk analysis, including an evaluation of the value of the assets. Fundamentally, it is one of the substantial activities for the valuation of each asset.

a) One of the roles of an asset manager is to identify the total assets included in an organization and to recognize the assets to be protected. The asset manager surveys and identifies all valuable assets, including intangible assets such as sensitive personal data, system configuration files, etc., as well as tangible assets such as IT systems.

b) In this survey process, the asset manager should also check the status of the assets such as in-use, unused, disposal, etc., for managing newly acquired assets as well as the existing ones.

c) When surveying the assets, a team or department having the authority of asset management should keep in close cooperation with teams or departments related to installation and operation.

d) The asset manager should create an asset register or inventory for continuous maintenance of asset information collected in this survey process. The asset manager also gives a name to each of the identified assets to be managed.

7.3 Classification and registration

Assets identified within the established asset boundary are classified by their types as defined in the asset classification criteria. There are classifications by asset items and business process. Classification and registration activities for assets mean that those assets should be managed in the asset register. One of the important considerations is to determine the number of classification categories and the benefits to be gained from their use.

a) The asset manager should classify the identified assets by their types in accordance with the criteria for asset classification established by the organization. The asset manager should define the basic and additional maintenance information based on the asset attributes, according to the type of asset.

b) The asset manager should check whether an asset operator appropriately identifies and classifies the assets. Then the asset manager manages collectively the assets by registering the assets in the asset register.

c) Registering the assets includes additional records as well as the basic information to be managed by the corresponding asset type. The additional records depend on the maintenance information based on the attributes of each asset.

d) It is possible to treat the assets as one group having the same asset type, the same security characteristic and the same importance level in order to improve the management of a vast number of assets.

e) Identified and classified assets are required for labelling. Labelling uses a physical label. The asset label includes basic maintenance information related to asset types such as asset code, asset name, asset value level. For assets that cannot be physically labelled, such as documents in electronic form, it is possible to use electronic means for labelling. Where labelling is not feasible, other means for designating the classification of information can be applied, e.g., via procedures or metadata.

7.4 Evaluation of asset value

To determine measures required to adequately secure an asset, the asset should be evaluated and classified according to its evaluation results. For granting each asset's value, it can be evaluated based on three primary security requirements; confidentiality, integrity, and availability. Assessing the value of the assets is the first task in performing all risk analyses.

a) The ultimate purpose of evaluation of an asset is to allocate a value to the asset that indicates the importance of the asset. This value then helps organizations to decide how much protection is required to safeguard the asset. The greater the value of the asset, the greater the protection required. When the asset is destroyed or its security is compromised, there is an impact on the organization. This impact can be very severe to the operations of the organization. For example, if a piece of malware spreads through a network management system, it could destroy many electronic information assets that are critical to the effective management and operation of the network and the provision of customer services. Therefore, it is important that asset valuation be carried out on all the critical assets.

b) The AVL can be computed according to the results of the evaluation by the asset owner. For example, an electronic information asset may have three different values representing the importance of the confidentiality of, of the integrity of, and of the availability of the asset. Based on these three values, a combined asset value can be calculated which indicates the maximum level of security required of the asset. Three integer numbers (e.g., from 3 to 1) can be estimated to reflect the importance of an asset in terms of confidentiality, integrity and availability. After calculation, an AVL can be finally obtained according to the following formula.

AVL (Asset Value Level) = C (Confidentiality) + I (Integrity) + A (Availability)

c) The criteria for asset evaluation can be changed according to the telecommunication organizations' security policies, system environment, etc. It is more reasonable to make the evaluation criteria objective and measurable.

d) After evaluation, the asset value level is determined and the result is added to an asset register.

7.5 Performance of change management

An asset manager should periodically check and update the status of the asset register. A key purpose for follow-up and update is to check whether or not each asset is well managed according to its security level.

a) The asset manager should periodically check and update the status of assets based on the asset management plan. If there is any change to the assets, the asset manager should again assess the value of the corresponding asset and update the changes to the asset register.

b) When an asset is newly acquired or generated, the asset is recorded and managed through some activities that include the identification of the asset, classification, evaluation of importance, and determination of security level.

c) If unused assets are found in the process of the periodical check, the asset manager should decide the treatment of those assets with the asset-related departments or teams.

d) The asset manager should remove the records of the asset from the asset register when the assets are disposed of.

e) The asset manager may continue to find new issues in the process of asset management. It is necessary to document the information that would be helpful for improving asset management and reflect any new issues in the asset policies of the organization.

8 Telecommunication asset classification

The asset management process defined in clauses 6 and 7 is applicable to telecommunication organizations as well to all other organizations. The main difference in relation to asset types in telecommunication organizations with respect to other organizations is that focus is placed on telecommunication-specific assets. For example, most organizations will have general IT assets such as PCs, servers, network devices, and commonly used office application software; whereas telecommunication organizations would be dealing with those assets specific to running, operating, and managing mobile, satellite and fixed networks.

8.1 General and telecommunication specific assets

Table 1 shows how to classify the various assets by asset type. This table also provides examples of general and telecommunication-specific assets that organizations need in order to apply the asset management process defined in clause 6.

Table 1 – Examples of general and telecommunication-specific asset

Asset type	Description	Examples	
		Telecommunication specific	General
Electronic information	Information stored in electronic form	Telecommunication service customer information (database), network session and access log, network configuration files, service use and access policies, etc.	Database (office DB, etc.), data files (office policy and guidelines, CCTV log, etc.), system files (configuration files, log files, etc.), etc.
Paper	Paper information, which means documents or records to be produced and used in tasks	Contracts and agreements including SLAs, network architecture diagrams, IP address lists, cabling diagrams, server system diagrams, network operating system manuals, etc.	Contracts and agreements, system documents (network configuration diagrams, user manuals, etc.), etc.
Software	Software developed for commercial use or for internal use	Network operating system, network scanner, early warning detection tool and utilities, audit trail software, etc.	Application software (office applications, etc.) , system software (OS, DBMS, vulnerability scanner, etc.), development tools and utilities, etc.
Hardware	Server and network devices used for internal and external services or businesses	Server (DNS server, DHCP server, log server, authentication server, NTP server, NMS server, monitoring server, etc.), network and communications equipment (backbone router, switch, CMTS, NAS/RAS, AP, modem, etc.), security equipment (ESM, firewall, IPS, IDS, VPN, virus wall, vaccine, etc.), mobile systems, satellite systems (stations), microwave systems, transmission system, etc.	Server (web server, DB server, WAS, log server, backup server, storage, etc.), mainframes, network and communications equipment (switch, etc.), security equipment, desktops, workstations, laptops, handhelds, etc.
Facility	Place in which systems are installed and operated, which include physical spaces and various supporting equipment rooms	Cabling facilities, network management and monitoring facilities, telecommunication equipment room, Internet data centre, etc.	Office building, server room, paper room, electrical equipment room, etc.
Supporting utility system and equipment	Equipment used for supporting information system operation, which include power supply, air-conditioning equipment, etc.	Mobile, satellite and fixed network supporting utilities (generator, UPS, etc.), etc.	Electrical equipment, air-conditioning equipment, fire extinguishing equipment, CCTV, etc.

Appendix I

Example of evaluation of an asset value level

(This appendix does not form an integral part of this Recommendation.)

The following example shows how to determine the asset value level (security level) by evaluating each asset's importance.

a) Assessing the value of an asset is accomplished based on the criteria predefined in the organization. For example, the scale of any asset's importance can be given from 3 to 1 for each evaluation item, such as confidentiality, integrity and availability. After computation, the final evaluation result of each asset lies between 3 and 9.

Security requirement	**Description**	**Level (Scale)**
C (Confidentiality)	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	High (3)
	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Medium (2)
	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Low (1)
I (Integrity)	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	High (3)
	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Medium (2)
	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Low (1)
A (Availability)	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.	High (3)
	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	Medium (2)
	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	Low (1)

b) The AVL of an asset depends on the evaluation result of the asset's importance. The AVL is divided into five levels according to the total evaluation result of each asset.

AVL [a] **(Security level)**	**Evaluation results of security requirements** **(Sum)**
Very High	9
High	7-8
Medium	6
Low	4-5
Very Low	3

[a] AVL (Asset Value Level) = C (Confidentiality) + I (Integrity) + A (Availability)

Appendix II

Example of asset maintenance information

(This appendix does not form an integral part of this Recommendation.)

The following example shows basic and additional items to be maintained according to the asset type.

Asset type	Asset maintenance information	
	Basic	Additional
Electronic Information	Asset code, asset name (electronic information name), electronic information type, security level, asset purpose, owner, manager	Related applications, creation date, etc.
Paper	Asset code, asset name (paper name), paper type, security level, asset purpose, owner, manager, location	Custody period (date), creation date, etc.
Software	Asset code, asset name, software type, security level, asset purpose, user, owner, manager, related server	Model name, product name, software version, manufacturer, product name, acquisition date, maintenance period, etc.
Hardware	Asset code, asset name, hardware type, server type, security level, asset purpose, user, owner, manager, location	Model name, OS, OS version, main data, installed applications (version), host name, manufacturer, product name, acquisition date, maintenance period, etc.
PC	Asset code, asset name, asset purpose, security level, user, owner, assigned task,	Model name, OS, OS version, manufacturer, product name, acquisition date, maintenance period, etc.
Facility	Asset code, asset name, asset purpose, model name, ownership type (direct ownership/lease), maintenance type (direct maintenance/lease), security level, user, owner, manager, location	Manufacturer, provider, etc.
Supporting utility system and equipment	Asset code, asset name, asset purpose, model name, ownership type (direct ownership/lease), maintenance type (direct maintenance/lease), security level, user, owner, manager, location	Manufacturer, product name, acquisition date , etc.
People	Department (team), R&R (role and responsibility), task, qualifications, contact points (phone, address, e-mail, etc.)	Skills, know-how, knowledge, experience, etc.

Appendix III

Example asset register

(This appendix does not form an integral part of this Recommendation.)

The following example shows a register form available for managing the assets in organizations.

Asset maintenance information							**Asset value evaluation**				
Asset code	Asset type	Asset name	Asset purpose	Asset owner	Asset manager	Asset user	Confidentiality (C)	Integrity (I)	Availability (A)	Sum (total)	Asset value level (security level)

Bibliography

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

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2012