International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1055

(11/2008)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Telecommunication security

Risk management and risk profile guidelines for telecommunication organizations

Recommendation ITU-T X.1055

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

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

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

Recommendation ITU-T X.1055

Risk management and risk profile guidelines for telecommunication organizations

Summary

Recommendation ITU-T X.1055 describes and recommends the processes, techniques and functional profiles for information security risk management for telecommunication to support Recommendation ITU-T X.1051 | ISO/IEC 27011 and other ITU-T Recommendations. These processes and techniques can be used to assess security requirements and risks identified in telecommunication, and help to select, implement and maintain/update appropriate information security risk controls, i.e., the correct information security level. There are many specific methodologies that have been developed to address the requirements for risk management. This Recommendation provides the criteria for assessing and selecting appropriate methodologies for a telecommunication organization. However, this does not aim to propose a specific risk management methodology for telecommunication. In addition, this Recommendation provides several risk profiles both in terms of ITU-T X.1051 management areas as well as telecom specific services areas.

Source

Recommendation ITU-T X.1055 was approved on 13 November 2008 by ITU-T Study Group 17 (2009-2012) under Recommendation ITU-T A.8 procedure.

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/.

CONTENTS

Introduction

Information security risks need to be managed effectively to ensure that organizations and their business is suitably protected from a range of threats. In today's world, telecommunication organizations are operating in a highly dynamic, open and global market place where the boundaries between ICT, services and applications are becoming less defined, with greater complexity and options for information sharing and transfer, on-line business and mobile and wireless services. This computing and networking environment is open to a growing number of risks and threats that can have a dire impact on organizations and their business. Risks to telecommunication networks and services pose growing security threats to telecommunication providers, network and Internet service providers as well as to the businesses and the national infrastructure. This Recommendation provides an overview of the risks that need to be addressed and suitable protections that may be put in place to manage the risks.

Recommendation ITU-T X.1055

Risk management and risk profile guidelines for telecommunication organizations

1 Scope

This Recommendation provides information and advice relevant to the management of information security risks in telecommunication organizations.

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*. <http://www.itu.int/rec/T-REC-X.1051>

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 impact [b-ISO/IEC 27005]: Adverse change to the level of business objectives achieved.

3.1.2 information security risk [b-ISO/IEC 27005]: The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence.

3.1.3 security incident [b-ITU-T E.409]: A security incident is any adverse event whereby some aspect of security could be threatened.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 risk profile: A set of information describing one of the risks identified by a telecommunication organization.

3.2.2 risk of exposure (RoE): Likelihood of a threat being able to expose one or more system vulnerabilities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ADSL Asymmetric Digital Subscriber Line

ASP Application Service Provider

CATV Cable Television

DoS	Denial of Service
ICT	Information and Communication Technology
IT	Information Technology
RoE	Risk of Exposure

5 Conventions

None.

6 Risk management

6.1 Process

The risk management process includes the following steps:

a-1) Assess the risk, considering the following:

- i) Assets and their value or utility.
- ii) Threats and vulnerabilities associated with these assets.
- iii) Risk of exposure of these assets to the threats and vulnerabilities.
- iv) Risk and impacts resulting from this risk of exposure.

a-2) Treat the risk, considering the following:

- i) Identification of available risk management options.
- ii) Selection of preferred risk management option.
- iii) Final risk management decision.

b) Implement the risk management decision, considering the following:

- i) Selection of controls.
- ii) Allocation of resources, roles and responsibilities.
- iii) Implementation of controls.

c) Monitor, review and communicate the risks, considering the following:

- i) Monitoring the risk situation.
- ii) Risk-related measurements.
- iii) Review and re-assessment of the risks.
- iv) Communicate the risks.

d) Update and improve the controls:

- i) Update controls.
- ii) Improve controls.

Figure 1 illustrates the cyclic nature of the risk management process, which aims at achieving effective management and control of information security risks through a continuous improvement system of processes.

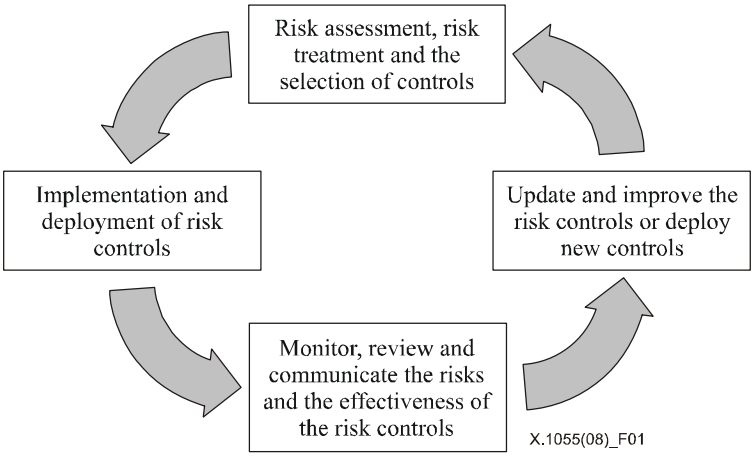

Figure 1 – Risk management process

6.2 Risk categories

Risk categories may include the following.

6.2.1 Information systems risk

Information used by telecommunication organizations includes that related to customers, staff, operations and communications, network services, and so on, all of which are at risk. This includes sensitive and critical information as well as personal data.

6.2.2 Human resources risk

Telecommunication organizations staff needs to be trained, competent and qualified in many areas of the business. They need to take charge of roles and responsibilities that are security-related.

6.2.3 Operational risk

The operational side of the telecommunication system needs to be efficient, effective and protected against the risk of being compromised.

6.2.4 Network services risk

The network services provided by a telecommunication organization need to be delivered in such a way that they are protected against the risk of being compromised.

6.2.5 IT services risk

The technology deployed by a telecommunication organization for their business and their customers needs to be reliable, robust and secure.

6.2.6 Physical risk

The physical locations, sites, buildings, computer rooms and switching centres need to be physically secured against the threats.

6.2.7 Compliance risk

Telecommunication organizations need to ensure that they are compliant with the laws and regulations that apply in the jurisdictions in which they are operating and providing services. This should include those laws and regulations that particularly apply to information security and the telecommunication organizations.

6.3 Risk components

6.3.1 Assets

The following is based on clause 7.1.1 of [ITU-T X.1051]:

Those assets which are critical to the telecommunication organization need to be protected in order to ensure that the operations and services of the telecommunication business are not compromised.

Thus, telecommunication organizations should make an inventory of assets. There can be many types of assets, including:

– Information: Communication data, routing information, subscriber information, blacklist information, registered service information, operational information, trouble information, configuration information, customer information, billing information, customer calling patterns, customer geographical locations, traffic statistical information, contracts and agreements, system documentation, research information, user manuals, training material, operational or support procedures, business continuity plans, emergency plan fallback arrangements, audit trails and archived information.

– Software assets: Communication control software, operation management software, subscriber information management software, billing software, application software, system software, development tools and utilities.

– Hardware assets: Switches, cables, terminal equipment, computer equipment (e.g., servers and personal computers/workstations), removable media and other equipment.

– Services: Fixed telephone service, mobile telephone service, optical subscriber line/ADSL service, leased line/data circuit service, Internet connection service, data centre service, CATV service, content delivery service, ASP service and customer services, including billing service, call centre service.

– Facility and supporting utility system: Building, electrical equipment, air-conditioning equipment, fire extinguishing equipment.

– People: Customer service staff, telecommunication engineers, IT support staff and staff for third party service providers.

– Intangibles: Organization control, know-how, reputation and image of the organization.

6.3.2 Threats

Threats may include the following.

6.3.2.1 Threats to confidentiality

– Eavesdropping.

– Electromagnetic radiation.

– Malicious code.

– Masquerading of user identity.

– Misrouting/rerouting of messages.

– Software failure.

– Theft.

– Unauthorized access to computers, data, services and applications.

– Unauthorized access to storage media.

6.3.2.2 Threats to integrity

– Unauthorized modification of information.

– Deterioration of storage media.

– Malicious code.
– Masquerading of user identity.
– Misrouting/rerouting of messages.
– Repudiation.
– Software failures and vulnerabilities.
– Supply failures (power, air conditioning).
– Technical failures and vulnerabilities.
– Transmission and communication errors.
– Unauthorized access to computers, data, services and applications.
– Use of unauthorized programs and data.
– Unauthorized access and modification to storage media.
– User errors.

6.3.2.3 Threats to availability

– Destructive attacks.
– Denial of service attacks.
– Deterioration of storage media.
– Failure of communication equipment and services.
– Physical damage due to fire, flood, explosions or earthquakes.
– Maintenance errors.
– Malicious code.
– Misrouting or rerouting of messages.
– Misuse of resources.
– Software failures and vulnerabilities.
– Supply failure (power, air conditioning).
– Failures of back-up systems.
– Technical failures and vulnerabilities.
– Theft.
– Masquerading of user identity.
– Traffic overloading.
– Transmission errors.
– Unauthorized access to computers, data, services and applications.
– Use of unauthorized programs and data.
– Unauthorized access to storage media.
– User errors and mistakes.

6.3.3 Vulnerabilities

Vulnerabilities describe a state or condition in the system where there is something lacking, incomplete or faulty. For example, software vulnerability could be lines of code which have errors in them and this presents a weakness that could be exploited by an attacker or might result in an accidental threat of system failure. Other examples of vulnerabilities include:

– Lack of user training.
– Lack of procedures or badly written procedures.

– Weak access control mechanisms.
– Badly configured network routers, gateways or firewalls.
– Lack of user authentication methods.
– Lack of business continuity or contingency arrangements.
– Outdated software patches.

6.3.4 Risks

6.3.4.1 General

The following lists give some of the generic risks that telecommunication organizations might face. More specific detail and account of these risks can only be derived by looking deeper into the operational and business environment where these risks might arise.

6.3.4.2 Loss of confidentiality

The loss of confidentiality may lead to:

– Loss of public confidence or deterioration of public image.
– Legal liabilities, including those that may arise from breach of data protection law.
– Adverse effects on organizational policy.
– Endangerment of personal safety.
– Financial loss.

6.3.4.3 Loss of integrity

The loss of integrity may lead to:

– Incorrect decisions being made.
– Fraud.
– Disruption of business functions.
– Inability to perform critical tasks.
– Degradation in services.
– Network robustness and reliability.
– Public and staff safety.
– Depletion of public confidence or deterioration of public image.
– Financial loss.
– Legal liabilities, including those that may arise from breach of data protection law.

6.3.4.4 Loss of availability

Loss of availability of applications, services or information, where business functions and processes are interrupted, would result in response or completion times not being met.

The extreme form of loss of availability could result in permanent loss of data and/or physical destruction of hardware or software. Loss of availability may lead to:

– Incorrect decisions being made.
– Inability to perform critical tasks.
– Depletion of public confidence or deterioration of public image.
– Reduction in the quality and delivery of services.
– Denial of network services.
– Financial loss.

– Legal liabilities, including those that may arise from breach of data protection law and not meeting service level agreements.
– Significant recovery costs.

6.3.4.5 Loss of accountability

Loss of accountability may lead to:

– System manipulation by users.
– Fraud.
– Industrial espionage.
– Untraceable actions.
– False accusations.
– Legal liabilities, including those that may arise from breach of data protection law.

6.3.4.6 Loss of authenticity

Loss of authenticity may lead to:

– Fraud.
– A valid process being used with invalid data, leading to a misleading result.
– Manipulation of the organization by outsiders.
– Industrial espionage.
– False claims and accusations.
– Legal liabilities, including those that may arise from breach of data protection law.

6.3.4.7 Loss of reliability

Loss of reliability of systems may lead to:

– Fraudulent activities.
– Lost market share and customer confidence.
– Demoralized staff.
– Unreliable services.
– Legal liabilities, including those that may arise from breach of data protection law.

6.3.5 Risk of exposure

When a threat is able to exploit vulnerability within the telecommunication system, the consequence can be a security incident. The conditions need to be right in order for the threat to be realized. This brings about a risk of exposure (RoE) in the telecommunication organization.

RoE = Likelihood of the threat being able to expose one or more system vulnerabilities

Figure 2 illustrates how the RoE changes as the level of threat and vulnerability changes.

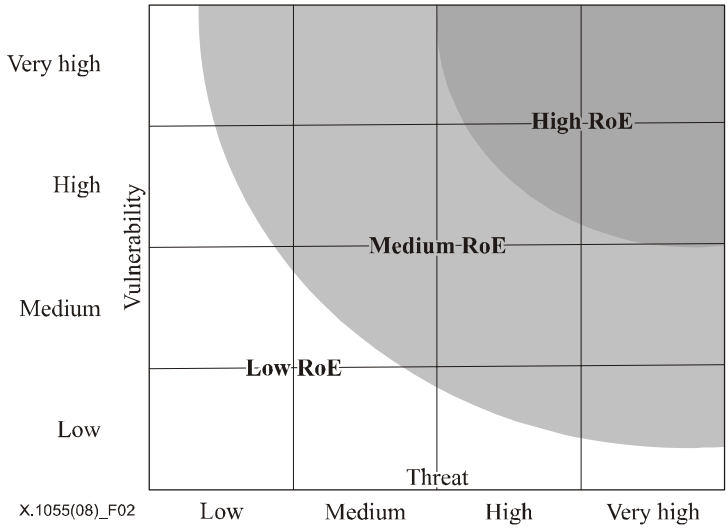

Figure 2 – RoE according to change of threat and vulnerability

6.4 Risk assessment and risk treatment

The goal of risk assessment is to produce a list of risks that the telecommunication organization is facing or is likely to face. This list should be prioritized to ensure that the most serious risks are dealt with first.

This assessment will firstly consider the telecommunication assets which are critical for providing and maintaining network operations and delivering network services.

Secondly, the assessment will consider the threats and vulnerabilities that are associated with the assets under assessment.

Finally, the results of this work will go towards calculating the levels of risk which the telecommunication organization is facing. These risk levels can be derived by considering the RoE level and the potential impact that the telecommunication organization might suffer if the risk of a threat exploiting vulnerability actually takes place.

$$\text{Risk} = \text{RoE} \times \text{impact}$$

Figure 3 illustrates various bands of risk as the level of RoE and impact changes.

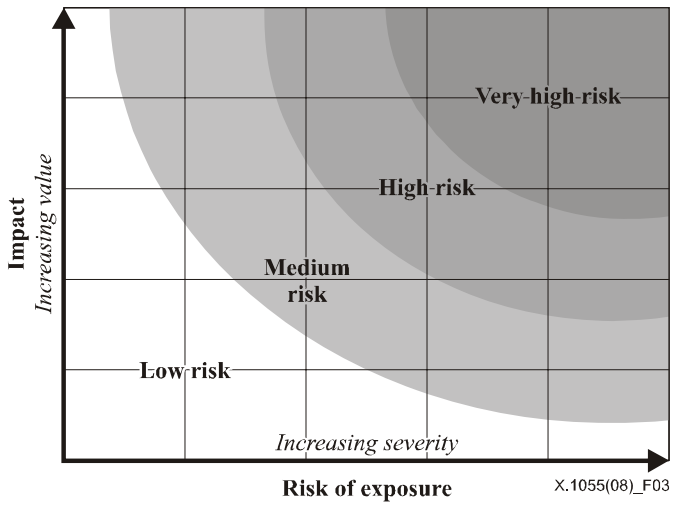

Figure 3 – Risk according to change of RoE and impact

Using the risk treatment process, the telecommunication organization needs to decide how to deal with the results presented from the risk assessment. One common way is to reduce the risks to an acceptable level. Other treatment options can be found in [b-ISO/IEC 27001], including:

– Avoid the risk by modifying, changing or avoiding the activity that causes the risks.

– Accept/retain the risk knowingly and objectively by the telecommunication organization.

– Transfer the risk, for example, by insurance or by contracting out the risks. Note that even though this is an option, the telecommunication organization is ultimately responsible for the risks of the organization and its customers.

To reduce the risks, a system of controls should be selected and implemented as appropriate to the operational environment of the telecommunication organization. [ITU-T X.1051] provides a comprehensive list of controls. This list of controls may need to be supplemented with additional controls defined in other standards.

7 Risk profiles

7.1 Definition

A risk profile is a set of information describing the risks identified that are specific to an area of business interest to a telecommunication organization. This might be a profile of a specific service, application or technology related to the organization's business. Each profile is intended to be a tool that allows managers to make decisions about how to manage and handle the identified information security risks.

Each profile consists of several entries described in clauses 7.3 and 7.4. A set of profiles should be developed in the first stage of the risk management process (see Figure 1).

7.2 Use of profiles

Risk profiles inform the overall process of risk management and help to prioritize the information security risks.

Risk profiles also provide information relevant to risk management. Based on a risk profile, decisions can be made regarding whether to conduct a quantitative/qualitative risk assessment, gather more information or perform some immediate risk management activity.

Risk profiles provide a focus to prioritize resources and actions. They can also be used as a benchmarking tool alongside the risk assessment process and other process tools such as gap analysis methods and scorecards.

Profiles provide a basis for risk management metrics and measurements to be established and implemented.

7.3 Risk profile hierarchy

Risk profiles can be hierarchically categorized into four types as depicted in Figure 4. For a telecommunication organization, this hierarchical concept can be applied to their business when developing risk profiles.

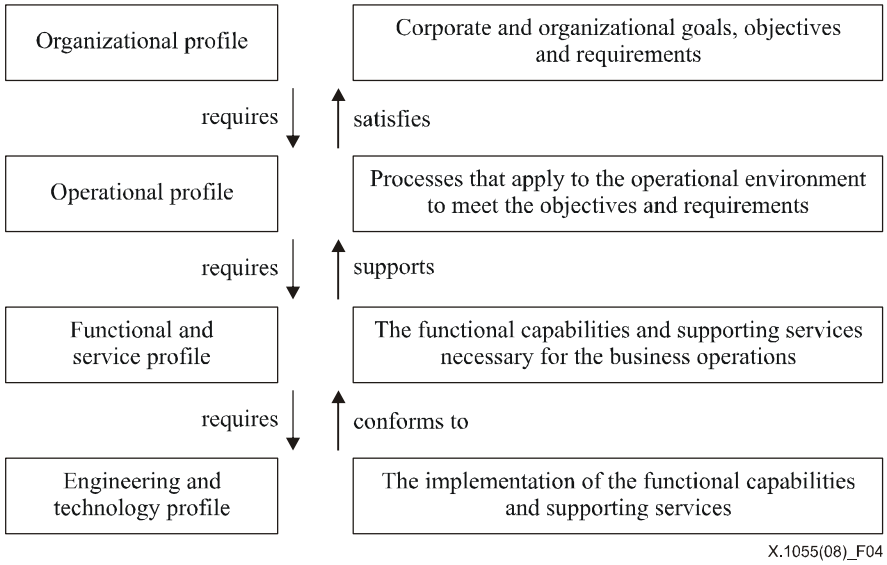

Figure 4 – Hierarchical concept of risk profiles

7.3.1 Organizational profile

This is a high level profile, which reflects the corporate responsibilities for information security risk policy on the basis of governance and the need to protect the organization's information assets. This profile outlines what the telecommunication organization expects to achieve in order to protect its business from a compromise.

NOTE – "Information security risk policy" should be a part of information security policy for telecommunication organizations.

7.3.2 Operational profile

This type of profile reflects operational information security risk policy to satisfy the requirements and objectives of the organization. It outlines what the telecommunication organization needs to achieve to protect its business from a compromise. It should reflect what operational processes, applications and services are at risk.

7.3.3 Functional/service profile

This type of profile reflects the information security risk policy at the functional and supporting services level. This profile should outline the potential risks considering the operational needs of the telecommunication organization and what to achieve in order to protect the operational side of its business. It should reflect which information security risks are inherent at the functional and supporting service levels.

7.3.4 Engineering/technology profile

This type of profile is a report which provides technical information as background to the risks outlined in the other three types of profile. As such, it is distinct from the other profiles and reflects the problems of technology and information security risks, and the secure implementation and deployment of such technology. This profile should reflect the policies of the telecommunication organization to conform to their requirements and objectives through the chain of other profiles. It should reflect the risks to be considered with an engineering/technology view.

7.4 Profile template

All the relevant information for each risk should be gathered from various sources, including vulnerability reports, security incident notes, etc.

Table 1 is a template for a risk profile. An example of risk profiles is given in Annex A.

Table 1 – Profile template

Profile type	[Organizational, operational, functional/service or engineering/technology]
Specific scope and context	[Specific definition of the profile in the context of the telecommunication system]
Business objectives and requirements	[For example, organizational, governance, legislative and regulatory, operational and/or services]
Risk category	[see clause 6.2]
Risks and impacts	[A risk has two contributing factors, one expressing the impact if the risk occurred, and one expressing the likelihood that the risk might occur – see clauses 6.3-6.4]
RoE	[RoE has also two contributing factors, one expressing the threat for the asset, and one expressing the vulnerability of the asset – see clause 6.3.5]
Commentary and other information	[For example, a technical report outlining the risk problem in more detail]
Profile identifier	[For the purpose of identifying the risk profile for maintenance, the profile should have an identifier]
Version and date	[For maintenance, the profile should be managed by using the profile version and the date when it was developed]
Author/owner	[Individual or role that is in a position to develop the risk profile]

7.5 Development and maintenance of risk profiles

Developing the risk profile should be carried out in conjunction with the risk assessment process. The output of the risk assessment should be documented in line with the template of risk profile. The risk profiles should be used to provide a focus to prioritize resources and actions against the risks.

Even when the risk profiles have been developed, the risks facing the telecommunication organizations are not static. The risks should be carefully monitored not only for the effectiveness of the risk assessment process, but also for risk response. Any changes detected in the risks should be promptly reflected and updated in the risk profiles. Where appropriate, the risk profiles should then be reviewed to ensure the most appropriate actions (risk treatments) are being adopted.

Annex A

Risk profile example

(This annex forms an integral part of this Recommendation)

The following example shows how to use a risk profile regarding managed data services and DoS attacks.

Profile type	Functional/service
Specific scope and context	Customer-managed data services
Business objectives and requirements	Availability of system facilities to ensure continuity and quality of service and to avoid a denial of service incident.
Risk category	IT and network services
Risks and impacts	• Breaches of contractual obligations. • Breach of legislation or regulations. • Destruction or loss of customer information. • Loss of services to customers. • Unauthorized access and use of telecommunication systems. • Use of network facilities in an unauthorized way. • Spam attacks. • Misuse and unauthorized control on network and IT facilities. • Malicious code. • Disruption of business. • Loss to customer productivity and business.
RoE	Without a high degree of effective information security management in place as well as a security technology being properly deployed, the risk of a denial of service attack is high or even very high. There may be different levels of risk depending upon which of the risks are more likely and how effective or otherwise the existing information security controls are at countering these risks. A full risk assessment into this application case will be able to determine which of the above risks are problems. The impact on the business could be catastrophic in terms of business relations and trust with customers, possibly legal issues, brand and reputation, damage and many other dire outcomes.
Commentary and other information	See attached technical report on denial of service problems.
Profile identifier	xxx-xxx-xxx
Version and date	Version 1.0 and dd-mm-yyyy
Author/owner	xxxxx

Bibliography

[b-ITU-T E.409] Recommendation ITU-T E.409 (in force), *Incident organization and security incident handling: Guidelines for telecommunication organizations*. <http://www.itu.int/rec/T-REC-E.409>

[b-ISO/IEC 27001] ISO/IEC 27001:2005, *Information technology – Security techniques – Information security management systems – Requirements*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103>

[b-ISO/IEC 27005] ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42107>

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2009