International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1059

(10/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

Recommendation ITU-T X.1059

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	**X.1050–X.1069**
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	X.1700–X.1729

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

Recommendation ITU-T X.1059

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

Summary

Recommendation ITU-T X.1059 provides guidance for telecommunication organizations on the risk management of their assets globally accessible in IP-based networks, the assets which are exposed directly to hackers and attackers. These assets may also be connected to the traditional (and even old) assets of legacy telecommunication networks, which might have some design level vulnerabilities that could be difficult to fix. Therefore, it would be practical to consider all the assets globally accessible in IP-based networks (AGIT) of a telecommunication organization as a whole, and to introduce some specific security controls to continuously reduce the overall risks and to strengthen the overall security of telecommunication services and networks.

It is suggested that the proposed controls be applied with high priority to assets globally accessible in IP-based networks. The controls might also be applicable to other assets.

History

Edition	Recommendation	Approval	Study Group	Unique ID[*]
1.0	ITU-T X.1059	2019-10-29	17	11.1002/1000/14045

Keywords

Assets survey, risk identification, risk management.

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

FOREWORD

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

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

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

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

NOTE

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

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

INTELLECTUAL PROPERTY RIGHTS

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

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

Table of Contents

Page

Introduction

Telecommunication organizations have become more progressive to leverage the benefits of both legacy and Internet services. Some of these organizations have transferred their legacy services to the Internet, such as using Internet protocol (IP) technology to provide voice services instead of using circuit-switched technology and even integrating voice services such as voice over long-term evolution (VoLTE) with ordinary voice over IP (VoIP). Some organizations have merged Internet flexibility into legacy services, for example, by enabling customers to use web portals to send messages out to the mobile terminals or to check messages and missed calls. Some organizations also utilize the Internet to provide customer self-service experiences, for example, by allowing customers to update their contracts and to make transactions online.

During this transformation process, a large number of assets are deployed by telecommunication organizations to bridge the physical network boundary between IP-based networks and telecommunication networks capabilities. Securing these assets, globally accessible in IP-based networks, has become one of the most obvious challenges for security management teams and the risk management of these assets could be a priority or primary concern for telecommunication organizations.

Recommendation ITU-T X.1059

Implementation guidance for telecommunication organizations on risk management of their assets globally accessible in IP-based networks

1 Scope

This Recommendation identifies threats and challenges that could arise when telecommunication network assets are globally accessible in IP-based networks. It also provides best practices and guidance for the implementation of security controls for the risk management of these 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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 control [b-ISO/IEC 27000]: Measure that is modifying risk.

NOTE 1 – Controls include any process, policy, device, practice, or other actions which modify risk.

NOTE 2 – Controls may not always exert the intended or assumed modifying effect.

3.1.2 impact [b-ITU-T X.1055]: Adverse change to the level of business objectives achieved.

3.1.3 risk profile [b-ITU-T X.1055]: A set of information describing one of the risks identified by a telecommunication organization.

3.1.4 risk of exposure [b-ITU-T X.1055]: Likelihood of a threat being able to expose one or more system vulnerabilities.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 assets globally accessible in IP-based network: Hardware and software assets that can be reached or connected by an Internet protocol (IP) or a uniform resource locator (URL) address or a certain client, etc., through the infrastructure of public IP networks.

3.2.2 AGIT profile: A set of information describing an asset globally accessible in IP-based networks for telecommunication organizations (AGIT) identified as belonging to a telecommunication organization.

3.2.3 residual risk: An old risk that cannot disappear or a new risk that appears after risk treatment.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AGIT	Assets Globally accessible in IP-based network for Telecommunication organizations
DDoS	Distributed Denial of Service
IP	Internet Protocol
IT	Information Technology
OS	Operating System
PII	Personally Identifiable Information
RoE	Risk of Exposure
SMS	Short Message Service
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VoIP	Voice over IP
VoLTE	Voice over Long-Term Evolution
VPN	Virtual Private Network
WWW	World Wide Web

5 Conventions

None.

6 Overview of risk management for AGIT

This Recommendation provides implementation guidance of risk management for a specified category of assets which are globally accessible in IP-based network (AGIT) as defined in clause 3.2.1.

6.1 Processes

In general, assets globally accessible in IP-based network for telecommunication organizations (AGIT) include the following six risk management processes (see Figure 6-1):

1) Risk assessment
2) Risk evaluation
3) Risk treatment
4) Monitoring and review
5) Communication and consultation
6) Recording and reporting

As part of the risk management lifecycle, AGIT risk management processes from 1 to 3 should be executed in a pre-defined order. The processes of 5, 6 and 7 should provide a feedback mechanism and should work in parallel throughout the whole cycle as shown in Figure 6-1.

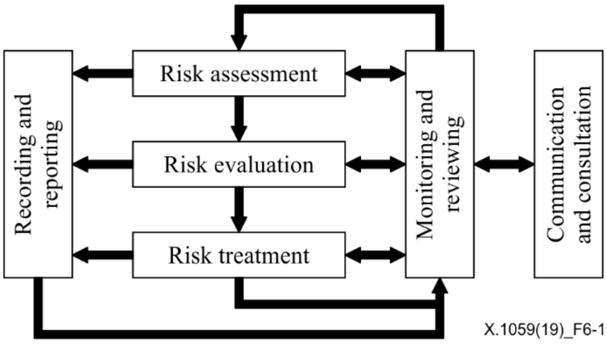

Figure 6-1 – AGIT risk management process model

6.2 Phases and steps

Each process in the AGIT risk management process model has one or more phases and/or steps. Figure 6-2 illustrates the phases and steps of process 1 to 3 (defined in clause 6.1).

The risk assessment process has two phases, which are risk identification and risk analysis. In the risk identification phase, there are five steps as listed below:

1) Identification of AGIT

2) Identification of threats

3) Identification of in-use controls

4) Identification of vulnerabilities

5) Identification of impacts

The two steps involved in the risk analysis phase are the preliminary analysis and the detailed analysis. The risk evaluation process has only one step, that is, risk evaluation. The risk treatment process has two steps, which are emergent treatment and regular treatment. The phases and the steps should be executed in a pre-defined order as shown in Figure 6-2.

Similar to the risk evaluation process, the other three processes – the monitoring and review process, the communication and consultation process, the recording and reporting process – all have only one step respectively.

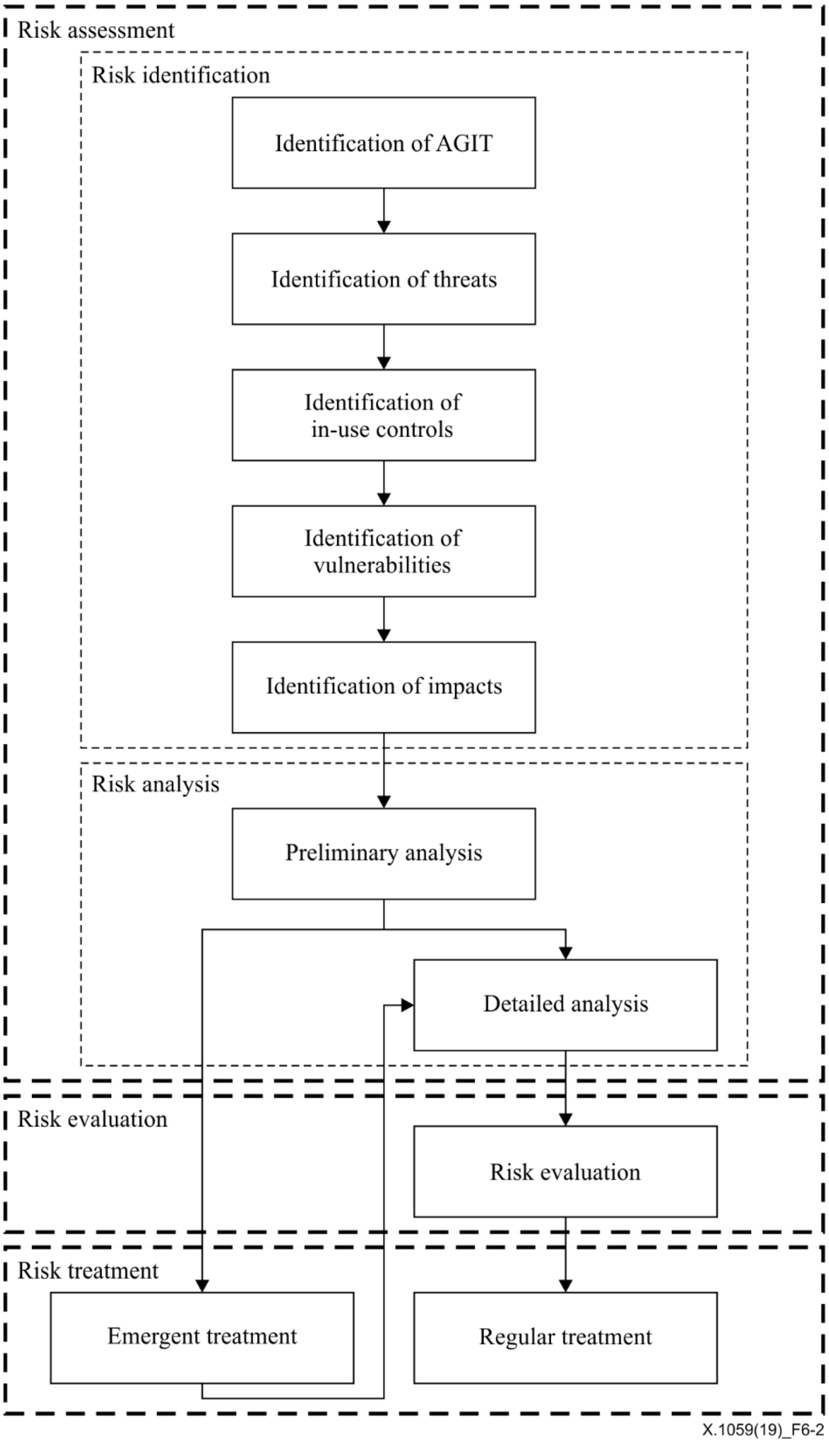

Figure 6-2 – Phases and steps in AGIT risk management process model

6.3 Structure of the description of the AGIT risk management process

The description and the recommended implementation guidance for the steps in the AGIT risk management process model are provided in clauses 7 to 12. The description introduces the generic understanding, practices and briefs for the measures of improvement. The implementation guidance provides detailed information on how to improve the implementation with best practices specific to AGIT with the recommended inputs and outputs.

7 Risk assessment

7.1 Risk identification

7.1.1 Identification of AGIT

7.1.1.1 Description

AGIT include hardware and software assets that can be reached over or are connected by an IP address or uniform resource locator (URL) address or certain clients, etc., through the infrastructure of public IP networks.

Generally, the value of hardware and software assets depends on the business activity (or process) that they carry, the information that they store, cache or transfer, and their position in the network and service topologies.

AGIT open the capabilities of telecommunication networks by carrying key business activities to globally accessible IP-based networks and transferring communication content and exchanged information which could contain personally identifiable information (PII) and confidential data. AGIT, deployed naturally at the boundary of intranets, could have many connections to entities of legacy networks which provide telecommunication services. Accordingly, AGIT are valuable assets for telecommunication organizations. In practice, it is useful and effective to categorize and identify these assets as one 'whole' entity with similar security and risk management tasks.

This step is to identify and confirm all existing AGIT and their profiles. In general practices, identification of hardware and software assets relies on the inventory of purchases, network blueprints and system design, and the verification of physical or logically deployed entities. Based on these, more efforts to identify AGIT in a more accurately and timely manner would be recommended, which could help resolve the following challenges:

– The number of AGIT could be enormous, for example, hundreds in a large telecommunication organization. These AGIT could be distributed sparsely in dozens of intranets and in several telecommunication networks;

– Rapid developments in the business environment could compel operations departments to update the deployment of AGIT and diversify open-service capabilities dynamically and continuously. It is unrealistic to require operations' staff to understand the security effects of every business process and keep the security team informed as well;

– The common inputs may not be adequate to determine the necessary features and attributes of AGIT which could lead to inadequacy in the identification of risks and vulnerabilities so that AGIT could not be secured to an acceptable level.

7.1.1.2 Implementation guidance

AGIT profiles, business activities open to globally accessible IP-based networks, assigned public IP segments, etc., could be useful inputs to this step.

Continuous education and training should be necessary for operations departments to achieve and agree that any adjustments and updates related to AGIT could risk the established security environment and increase the risk level of many systems in the intranets (or private networks). The applicable standards should be established and operations departments should be required to check security issues ahead of conducting any change related to AGIT.

Approval or maintenance systems could be adopted to allow operations departments to manage changes and keep security teams informed. The use of administrator's privilege could permit security teams to follow changes and compare them to the system conditions of (suspicious) AGIT precisely and thoroughly, and then to update the AGIT profiles.

Cyclic scans from globally accessible IP-based networks could be used to identify unknown public IP addresses and transmission control protocol/user datagram protocol (TCP/UDP) ports in use. Tracing and questioning these new identifications could lead to the discovery of unknown AGIT. Identifying the disappearance of in-use public IP addresses or TCP/UDP ports could lead to the removal of known AGIT.

Cyclic analysis of mirrored network traffic or service logs in the intranets could assist in identifying unknown communication pairs among public IP addresses and private IP addresses to locate unknown AGIT or update the profiles of known AGIT.

Results obtained by scans or analysis could lead to the identification of reasonable or acceptable operations related to AGIT. However, they could also lead to the identification of effects caused by (suspicious) incidents. The security team would therefore need to confirm the information from multiple sources to cross-check these clues prudently.

Changes or adjustments to business activities could be the most common cause of newly discovered AGIT. It should be necessary to consult operations departments to correctly understand the relevance of these AGIT.

The implementation of this control would identify a list of AGIT profiles which should be shared among stakeholders, such as security teams and network managers.

7.1.2 Identification of threats

7.1.2.1 Description

This step is to identify all direct and indirect threats against AGIT with several aspects such as threat type, affected AGIT, potential damage, etc. In general practices, threats against assets should be identified based on threat motivation and the asset's value. Historical incidents, expertise and regulation concerns should play key roles in clarifying the threat and the asset's value. The identification process could be conducted for each asset.

Some specific practices in this control should be recommended for better efficiency based on security trends and common features of AGIT.

The input of identification of threats should be AGIT profiles, threats information from external and internal sources (e.g., historical incidents, expertise) which can help analyse the threat level of each AGIT.

7.1.2.2 Implementation guidance

A list of AGIT profiles and threat information from external and internal sources (e.g., historical incidents and expertise) could be useful inputs to this step.

The exchange of threats intelligence could become a routine practice for more and more telecommunication organizations. A piece of well-built threats intelligence could depict a threat with its motivation and source by standardized language and could even verify itself. Though threats intelligence could hardly affect the classification of generic threats, it could help to identify ignored or new individual threats, which could help to evaluate the risk of exposure (RoE) and the impact to subsequent controls. The exchange of threats intelligence could be considered as a kind of import of external expertise.

With the existence of confirmed vulnerabilities belonging to the services or entities of legacy telecommunication networks, there could be no acceptable treatment to the risks if only legacy telecommunication networks are considered. Therefore, it is recommended to skip the process of risk treatment and consider these kinds of risks on the AGIT supporting business activities of legacy telecommunication networks. This practice integrates risk transfer with greater efficiency. These kinds of risks could be considered as indirect risks against AGIT.

As the value of AGIT relies mainly on the business activities and information supported by the AGIT, it should be efficient to group AGIT supporting similar business activities and information together and to identify the threats as a group.

Under the classification of generic threats, some individual threats against AGIT are identified as follows:

– Failure of business capabilities:
  - basic telecommunication network service failure;
  - voice and short message service (SMS) hijack (deciphering users' chats, eavesdropping, spam messages, pseudo base station);
  - distributed denial of service (DDoS) attacks.

– Decline of customer satisfaction:
  - poor service quality;
  - network paralysis on a massive scale;
  - service unable to respond.

– Business information systems security:
  - PII leakage (account, location, authentication, bill and other information);
  - identity impersonation;
  - unauthorized behaviour;
  - computer virus.

The implementation of this control should identify a list of threats, their sizes and their sources.

7.1.3 Identification of in-use controls

7.1.3.1 Description

This step identifies the function, scale and scenario of every effective control and identifies improper controls for later vulnerabilities identification. This control helps to avoid wasting resources on risk treatment and discovers shortages of in-use controls. In generic practices, the identification of in-use controls could be a combination of document reviews, staff interviews and in-field tests.

Some specific practices of this control are recommended to better support other controls, such as the identification of vulnerabilities.

7.1.3.2 Implementation guidance

A list of AGIT profiles, in-use controls documentation, personnel responsible for controls and other in-use controls could be useful inputs to this step.

It should be necessary to qualify personnel responsible for a control to operate the control correctly and within a reasonable period of time.

There should be pre-defined scenarios or contexts in which a control works well. It is important to use the AGIT profiles to verify if the current information technology (IT) environment, regulations and human resources could match a pre-defined scenario. If a mismatch occurs, the control could be labelled as an improper one for further analysis in subsequent step.

Whether or not the scale of a control could cover all necessary AGIT should also be checked. If a control covers an AGIT which has no corresponded risks, the control could be labelled as an improper or redundant one. If controls were designed to treat the same risks and cover the same AGIT, these controls could be labelled as improper or duplicated ones for further analysis in the process of risk treatment to check the possibility of cost savings.

To determine if common and necessary controls are in use, the following should be verified:

- physical security: The condition of hardware in a working environment, hardware anti-theft measures, visit authentication of physical space, etc.;
- network security: Management of network topology and network devices, network access controls (e.g., firewalls, intrusion detection systems, virtual private networks (VPNs)), system access authentications, etc.;
- data security: Read/write access control, backup policies, security storage of confidential data and files, etc.;
- system security: Access policies for world wide web (WWW) services, security policies for databases, mail systems and web application servers, etc.

When identifying vulnerabilities, improper controls could also be discovered. Therefore, it could be useful to adopt one or more small iterations between the identification of in-use controls and that of vulnerabilities.

Finally, the implementation of this control should identify all the effective and improper controls with explicit reasons.

7.1.4 Identification of vulnerabilities

7.1.4.1 Description

This practice is to identify the vulnerabilities with timely verification and rigorous confirmation with the intention of examining the assets and exposing the weakness in case of an attack. While, in generic practice, expertise should be good for human-related vulnerabilities and (automatic) test tools should be efficient and necessary to verify the vulnerabilities of IT listed in the database of known vulnerabilities. Furthermore, the research by experts could be the only way to discover unknown-till-now vulnerabilities.

Some specific practices in the control should be recommended to enhance the timeliness and the practicability.

7.1.4.2 Implementation guidance

The list of AGIT profiles, in-use controls and improper controls could be useful inputs for this control.

An intact and accurate database of vulnerabilities should be helpful to develop a tools set to verify the existing of vulnerabilities in an efficient way.

Similar to the practice in the identification of threats, for better handling of risk treatment, the confirmed vulnerabilities of legacy telecommunication networks could be protected by AGIT supporting the business activities through the legacy telecommunication networks.

A continuous exchange of threat intelligence with good quality should be important to enable security teams to respond against the new vulnerability in a timely manner. A piece of well-built threats intelligence could contain the proof-of-concept code and the required conditions (such as, operating system (OS) type and OS version) of a new vulnerability to assist in verifying it. An expert could use the code with minor adjustments to make a tool to test the effectiveness.

Once the vulnerability of an AGIT is confirmed, it could be deduced directly that the other AGIT, having the same system conditions, could also have the same vulnerability. While, it could be more rigorous in practice with the consideration of the importance of AGIT, that is, if the same vulnerability cannot be confirmed in another AGIT but having similar configuration and context, then perhaps the vulnerability could be considered as an "upcoming" one. For example, as a service-level vulnerability is confirmed in Linux OS with core 3.05, then the same vulnerability could be considered as an upcoming vulnerability in Linux OS with core 4.01 as well.

The implementation of this control should finally identify an up-to-date list of (close to be) confirmed vulnerabilities belonging to AGIT.

7.1.5 Identification of impact

7.1.5.1 Description

In generic practices, impacts should be identified under different incident scenarios. Therefore, establishing typical scenarios should be fundamental to process the identification, and the security team should take full consideration of the cost of overall aspects (such as time, economy and reputation, etc.) to clarify the impact of every scenario.

There would be no specific practices recommended in the control.

After the identification of impact, the whole process of the risk identification should be completed. All the outputs of the previous four steps of risk identification (clauses 7.1.1 to 7.1.4) should be organized hierarchically as risk profiles, where each is a set of information describing one of the risks identified by a telecommunication organization.

7.2 Risk analysis

The methodology of risk analysis includes qualitative and quantitative method which are widely accepted.

In risk analysis for AGIT, risks are classified into emergent risks and regular risks, which should be treated differently. A risk should be regarded as an emergent risk if the risk can cause great damage in a short period of time. Otherwise, the risk should be regarded as a regular risk. The telecommunication organizations could set up their own criteria to determine which risks should be treated as emergent risks. The others are regarded as regular risks.

A preliminary analysis is used to sort out the emergent risks before a detailed analysis is undertaken. If a risk conforms to the criteria of emergent risks, it should be an emergent risk that needs to be treated in time with little cost consideration. Emergent risks should be taken directly to the risk treatment process, and the risk evaluation process could be neglected for time saving.

After the preliminary analysis, a detailed analysis is carried out to go through all the regular risks and the residual risks left by the emergent treatment (in clause 8.1). Limited by human resources, budget and technologies, it could be inevitable to prioritize the treatment order of every risk. Therefore, the detailed analysis should calculate/estimate a risk level for every risk as the output. The risk level is an indicator determined by the impact and the RoE of every risk.

7.2.1 Preliminary analysis

7.2.1.1 Description

A preliminary risk analysis is a quick response to the emergent risks as some severe incidents could happen soon or may have happened. Usually the origin of an emergent risk should be more malicious and the scale of the impact on AGIT should be larger when compared with the regular risks. In this case, the preliminary risk analysis could assist the security team to make a decision to initiative a series of quick and efficient controls to deter or delay the escalation of the impact.

7.2.1.2 Implementation guidance

The qualitative method should be fit for this control. Before executing a preliminary risk analysis, some inspection criteria should be established beforehand to clarify whether a risk is an emergent risk or a regular one. A questionnaire tool could help to build the criteria. The questions in the questionnaire could help the security team to understand the seriousness and the urgency of a risk quickly and reasonably. The following questionnaire could be considered as a common base for further customization:

– Can the risk cause massive network or render services unavailable or interrupted for a long period of time?

– Can the risk cause massive PII or confidential information leakage?

– Can the risk cause high frequency of identity impersonation or service abuse?

– Can the risk cause the hijack of a large scale of assets?

The questions above should be answered by the security team according to the up-to-date information, historical statistics and their expertise. The inspection criteria could be settled, for example, based on the answers of the questionnaire.

If a risk conforms to the criteria, it should be an emergent risk and the emergent treatment in clause 9.2 should be its next process. Otherwise, it should be a regular risk and should naturally go through the process of a detailed analysis.

7.2.2 Detailed analysis

7.2.2.1 Description

A detailed analysis provides a comprehensive breakdown of the risks and concludes the risk level based on the calculation or the estimation of the RoE and the impact of the risks under different scenarios. The regular risks and the residual risks after the emergent treatment should be the objects of the analysis. The corresponding risk profiles should be necessary inputs.

7.2.2.2 Implementation guidance

The threats frequency and the ease of vulnerabilities should be taken into account to determine the RoE under every scenario.

The risk levels should be aggregated under the unit of a group of AGIT that share a highly similar scenario, which means the same threat, the same (up-coming) vulnerabilities and a similar context. The aggregated risk levels could reflect better the effects of the scale of threats.

Regardless of whether or not the quantitative method or the qualitative method is adopted by the detailed analysis, some kind of automated tools set should be useful to enhance the quality and the efficiency of the analysis.

8 Risk evaluation

8.1 Description

Risk evaluation is a process to decide which of the risks should be treated based on the outputs of the risk analysis. To make the decision, the risk levels should be compared with the organization risk acceptance criteria. The risk acceptance criteria should involve the basic business requirements that the AGIT should fulfil. If a risk level or an aggregated risk level shows that an AGIT or a group of AGIT cannot comply with the risk acceptance criteria, the risk should be treated.

Risk acceptance criteria should be established based on several factors, such as:

– maximum tolerance of downtime;

– maximum tolerance of intangible assets loss (such as business reputation, trade secrets);

– maximum tolerance of monetary loss.

The output of the risk evaluation could be a list of risk over the acceptance level and a corresponded priority.

There would be no specific practices recommended in the control.

9 Risk treatment

9.1 Overview

Risk treatment for AGIT is a process to implement extra or new controls to reduce all the risk levels to no more than an acceptance level. In the risk treatment, the security team should determine what kind of methods should be adopted and how to conduct it properly. There are four kinds of generic risk treatment methods that could be considered, that is, risk modification, risk retention, risk avoidance, and risk sharing. The risk treatment could apply one or more methods flexibly to treat all the risks over the acceptance level according to the priority.

The steps of the process should be divided into the emergent treatment and the regular treatment. Besides, the residual risks after the risk treatment should be considered in the monitoring and review process.

9.2 Emergent treatment

9.2.1 Description

Emergent treatment is to address the emergent risks. The primary goal of the emergent treatment is to deter or delay the escalation of the impact in time. The emergent treatment should be proactive and usually adopt the methods of the risk modification and the risk avoidance. After rapidly implementing some effective controls to temporarily secure the AGIT, the residual risks should again be taken through the detailed analysis process for further risk management.

9.2.2 Implementation guidance

With the consideration of the special positions of the AGIT, the technical controls inside of AGIT could always be the most ideal choice to treat the risks. The usual technical controls could be the software/firmware patches, the system configuration adjustment, the access control upgrade, and network topology optimization, etc. However, an ideal control might not be available in time, because it could require time to be designed, developed and tested in the field. Therefore, some preliminary controls could be adopted to degrade the risk level away from the emergent level. In practice, the following measures could be frequently used:

- to block the malicious sources;
- to filter the specified traffic in a dedicated way with performance loss;
- to partially disable some of the capabilities of the AGIT or the business activities through the AGIT.

In some cases, there could be no internal controls (such as patches and configuration optimization) in the near future to fix the vulnerability. In this regard the security team could consider the treatment method according to the following aspects:

- potential consequence if the AGIT is shutdown or replaced;
- potential consequence if the business activities through the AGIT is offline;
- capabilities and performance loss to deploy external measures temporarily to shield the AGIT in order to degrade the RoE.

In some serious cases, there could be no reasonable or acceptable controls to apply. Thus, the risk retention method should be adopted and close monitoring should be extremely important in the process of the risk monitor and review.

After the emergent treatment, there could be a high possibility of residual risk. Therefore, the residual risks with the corresponding controls could be the output, which should be subjected to further detailed analysis.

9.3 Regular treatment

9.3.1 Description

Regular treatment is a process to treat risk over the acceptance level. To evaluate the outcome of treatment, risk tolerance level is introduced which describes the maximum residual risk that organizations can endure after the risk treatment. Unless organizations choose to accept the risk, all the risks should be treated effectively to a tolerance level. If more than one controls exist that can successfully treat the risk, these controls should be evaluated based on the cost-effectiveness.

The old risk that cannot disappear or a new risk that appears after risk treatment is defined as the residual risk. As the residual risks might change over time, they should be monitored and reviewed, as recommended in clause 9.

9.3.2 Implementation guidance

If a risk belongs to many AGIT, a comprehensive and iterative in-field test should be necessary for the controls that could treat the risk. Controls should be applied to every AGIT that has the risk in accordance with carefully assigned priorities. Based on the priority, a small group of representative AGIT should be selected first to conduct the in-field test.

In some cases, there could be no controls to modify the risk level of a risk so that other risk treatment method has to be selected. A honeypot net which is dedicated to the risk could be adopted as a combination of risk retention and risk avoidance.

Some kind of automated tools could be helpful to conduct the necessary deployment of some technical controls and monitor the progress of the risk treatment especially as the treatment faces a large scale of AGIT.

The output of the regular treatment could be a list of controls and their corresponding residual risks.

10 Monitoring and review

10.1 Description

Monitoring is a process incorporating two fundamental aspects, that is, the effects of controls on the risks and the compliance of the management processes and the regulation rules. Reviewing is a process to obtain an overview the effectiveness of the risk management objectives and identify the obvious changes continuously.

The output of the control should have a direct effect on whether or not to re-initiate the whole processes of the risk management or just a part of it.

10.2 Implementation guidance

The process should focus on the imperative changes compared with the boundary and the estimation of the risk management. The possible changes could include:

– the impact actually caused by the security incidents far exceeds the risk acceptance level;

– any important changes in the regulation environment;

– new threat intelligence identifies a new vulnerability that could expose a large scale of AGIT to a new threat and an old threat;

– the evolution of the business activities changes the context of a large quantity of AGIT.

The practice should ensure that the risk management policies and controls are fully understood by business staffs and are executed correctly and efficiently. The practice should also ensure that the risk management process and the related criteria are still appropriate for the organizations' business environment and current security situation worldwide.

11 Communication and consultation

11.1 Description

Communication is a process to bring relevant stakeholders to acquire sufficient information and expertise and to understand the status of risks in general. Consultation is a process whereby agreement is sought with the relevant stakeholders with respect to the application and cost of a particular control.

To assist the step of emergent treatment and risk treatment, specific practice regarding the communication and consultation process should be recommended.

11.2 Implementation guidance

As the security team realizes that an emergent treatment should be necessary, an active and close communication and consultation should be initialized at the same time that a technical solution is under planning. Such kind of activity might not be led by the security team but by some high-level manager or supervisor.

Furthermore, communication and consultation could utilize different areas of expertise to define an objective and quickly raise awareness of an emergent risk and evaluate its consequences from the perspective of business, reputation, regulation, etc. Support from related departments and top management could help assign resources for the security team to execute an emergent treatment and even decrease the criticism after the treatment.

The security team should keep all the relevant stakeholders informed of the progress of an emergent treatment and the final achievements.

12 Recording and reporting

12.1 Description

Recording is a process to document all the necessary information of the entire risk management process. Reporting is a process to provide the materials to support the communication or making a decision for the improvement of risk management.

Specific recording and reporting practices should be recommended to assist in the evaluation of risk management, and to promote the understanding of the security-related practices.

12.2 Implementation guidance

Recording and reporting should be key to evaluate the quality of the whole risk management process. Recording all the meaningful activities with related data should be helpful to calculate indicators, make conclusions and generate reports. It could be useful for AGIT to collect and link the necessary data to support the calculation of the following indicators:

- the survival time before a vulnerability disappears in all AGIT;
- the loss caused by a threat and vulnerability pair after the risk retention was adopted at least in part of AGIT;
- the interval of a same vulnerability discovered again in the next AGIT after the first one was confirmed;
- the frequency of a disappeared-once vulnerability discovered again;
- the reliability and the effectiveness of a control adopted in the related AGIT.

There are various concrete methods to collect data and calculate the indicators above depending on the management objectives and the technical situation.

Some practices, such as large-scale vulnerability scanning, in the procedure of risk identification could be aggressive or even invasive. This may also be the case for the procedure of risk treatment.

Sometimes, they could have some negative effects and trigger security alerts. Therefore, recording and reporting should be a mandatory tool for the security team to clarify the true intention inside or outside of the team if any confusion or dispute happens. For example, recording and reporting could help clarify whether a suspicious invasion was an authorized test or a true act of hacking.

A well-designed mechanism and information system should be helpful to disseminate and analyse the information gathered by recording and reporting in long term with the full consideration of the confidentiality and the privacy.

Bibliography

[b-ITU-T X.1051] Recommendation ITU-T X.1051 (2016), *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[b-ITU-T X.1055] Recommendation ITU-T X.1055 (2018), *Risk management and risk profile guidelines for telecommunication organizations*.

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

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

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

[b-ISO/IEC 27005] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

[b-ISO 31000] ISO 31000:2018, *Risk management – Guidelines*.

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2020