International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1060

(06/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

Framework for the creation and operation of a cyber defence centre

Recommendation ITU-T X.1060

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	**X.1050–X.1069**
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
IMT-T SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1060

Framework for the creation and operation of a cyber defence centre

Summary

Recommendation ITU-T X.1060 defines cyber defence centre (CDC) as an entity that plays a central role in an organization to address cybersecurity risks. The three processes of build, management and evaluation that a CDC should practically implement are described as a framework. The services that the organization should have in order to implement more specific cybersecurity measures are also provided.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1060	2021-06-29	17	11.1002/1000/14721

Keywords

Cyber defence centre, CIRT, security operation centre (SOC).

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

Cybersecurity risks in an organization have significant impacts on its overall activities. The risks that organizations face are environmental changes, from both the social and business perspectives, and external pressures by regulations and increased threats. Top management, as the C-suite (CxO), is therefore responsible for managing controls for the entire organization to respond to these risks and changes. As one important aspect of implementing controls in cybersecurity, leadership in development and control security policies in alignment with business objectives is expected and is often provided by the chief security officer (CSO) or chief information security officer (CISO). In order practically to implement security measures, an entity that supports the activities of the CSO or CISO with strategic management at the organizational level is essentially required. This entity is described as a cyber defence centre (CDC) in this Recommendation.

This Recommendation provides a framework for the build and management of a CDC, and evaluation of its effectiveness. The framework indicates how a CDC should determine and implement security services to enable the security of an organization. This framework helps an organization to address its cybersecurity risks.

Recommendation ITU-T 1060

Framework for the creation and operation of a cyber defence centre

1 Scope

This Recommendation establishes a framework for organizations to build and manage a cyber defence centre (CDC), and to evaluate its effectiveness. The framework indicates how a CDC should determine and implement security services to enable the security of an organization.

This Recommendation is intended for those responsible for security at the top management level of an organization, such as the chief security officer (CSO) or chief information security officer (CISO) and security supervisors who assist them.

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 term defined elsewhere:

3.1.1 outsourcing [b-ITU-T X.1053]: When an enterprise contracts out one or more of its internal processes and/or functions to an outside company. Outsourcing moves enterprise resources to an outside enterprise and keeps a retained capability to manage the relationship with the outsourced processes.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cyber defence centre (CDC): An entity within an organization that offers security services to manage the cybersecurity risks of its business activities.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

APT Advanced Persistent Threat

CDC Cyber Defence Centre

CISO Chief Information Security Officer

CSIRT Computer Security Incident Response Team

CSO Chief Security Officer

CxO C-suite

IDS Intrusion Detection System

IPS Intrusion Prevention System

IT Information Technology

SIEM Security Information and Event Management

SLA Service Level Agreement

WAF Web Application Firewall

5 Conventions

None.

6 Structure of this Recommendation

In this Recommendation, a concept of a CDC is explained in clause 7. Clause 8 provides an overview of the framework for creating and operating a CDC. The framework is described in detail in subsequent clauses: CDC build process (clause 9); CDC management process (clause 10); and CDC evaluation process (clause 11). In clause 12, an overall description of security services provided by a CDC is presented as best practice, and each service is described in further detail in Annex A.

7 Overview of a cyber defence centre

Organizations act to make their businesses successful. In order to manage risks to business activities, the CISO formulates security policies, especially from a cybersecurity perspective. A CDC is an entity that implements security policies specifically as CDC services, which consist of security activities that are performed by teams responsible for security. CDC services may specify security functions as capabilities of a system to perform security-related processing. Figure 1 shows stakeholders and their roles for CDC operation.

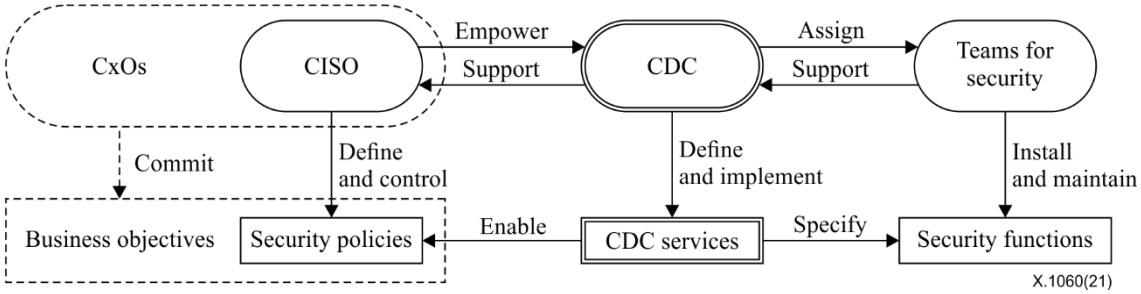

Figure 1 – Stakeholders and their roles for CDC operation

Depending on the size and type of the organization, a CDC may be an independent unit, a committee or a small team. Regardless of its format, it should exist as an entity in the organization, and have the authority and resources to implement security services to enable the organization to be secured. Such security services should be aligned with security policies and ensure the qualities of security activities; the level of each service should be explicitly agreed by a documented arrangement, such as a service level agreement (SLA). The overall quality of a CDC security service is assessed by measures specified in clause 9.4.

8 Framework for the creation and operation of a CDC

Figure 2 shows a framework for creating and operating a CDC. The framework includes three processes: build, management, and evaluation. To ensure the organization is secured, a CDC should

be established and appropriately managed. It should be also assessed in a timely and regular manner and continuously improve. This framework enables the organization to maintain security activities.

In the build process, security activities in the organization should be considered. Best practice for CDC security services are listed in Annex A. An organization can establish its own service catalogue by selecting services from the list and adding services specific to the organization. Each service in the catalogue should also establish a profile that includes: owner(s), roles and responsibilities, and type of service assignments (insource, outsource or combinations). Once the service profile is established, the current and target score of each CDC service should be determined for the evaluation process.

The management process has three phases and two cycles. The strategic management phase manages the overall activities of a CDC, the operation phase manages routine work for monitoring and analysis, and the response phase manages emergency responses. Those phases are managed in both short and long cycles; operation and response require timely resolutions in short cycles. Meanwhile, strategic management should consider long-term improvement together with output from short cycles in a long cycle. The long-term improvement typically requires decisions for new business investment and drastic modifications of system architectures.

The evaluation process assesses the catalogue, profile and portfolio of a CDC service (see Figure 4), which should be objectively assessed at each appropriate time.

The evaluation results should be reviewed and reflected in all three CDC processes. A recurring cycle of the build, management and evaluation processes to improve security activities should be established and maintained in the organization.

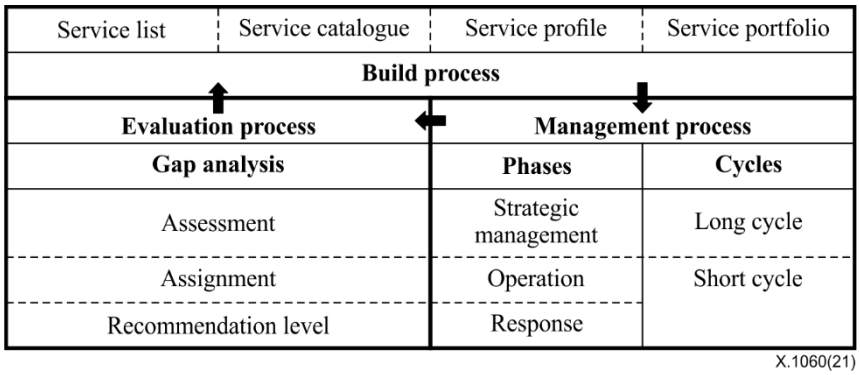

Figure 2 – Framework for the creation and operation of a CDC

9 Build process

9.1 Overview

The CDC has a build process to determine which security services should be implemented in the organization. The candidate services for implementation are selected from the CDC service list, which is based on best practice in the organization. For the CDC service list, see clause 12.

Figure 3 shows the three phases to build services for a CDC.

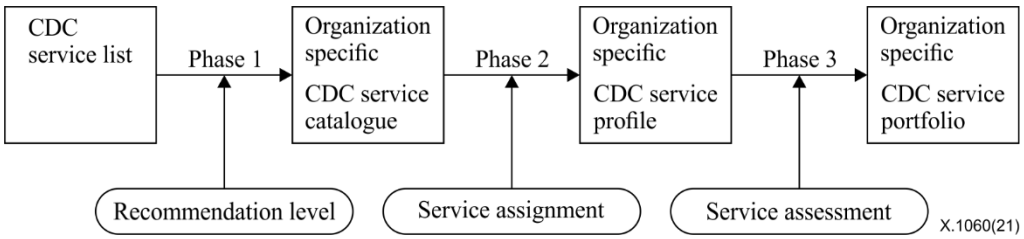

Figure 3 – Phases to build services for CDC

1) Phase 1: Creation of a CDC service catalogue

The organization should firstly create a CDC service catalogue.

In this phase, the candidate services for implementation are extracted from the general service list. Details of the general list are described in clause 12. If there are missing services, such services should be newly defined and added to the CDC service catalogue.

2) Phase 2: Creation of a CDC service profile

For the services listed in the CDC service catalogue, the organization should determine the roles and responsibilities of teams who provide the services. In this phase, the CDC service assignment described in clause 9.3 should be considered.

The organization should thus produce the CDC service profile.

3) Phase 3: Creation of a CDC service portfolio

After deciding the CDC service profile, the organization should measure the current service score (As-is) of each service and set a medium- or long-term target service score (To-be).

Once the levels of As-is and To-be are set, the organization should produce the CDC service portfolio.

Figure 4 shows an example matrix of CDC services. This matrix will be filled after phases 1 to 3.

Service	Recommendation level	Service assignment	Service score	
			As-is	To-be
Service ex.1	Basic	Insourcing (AB Dept.)	3	5
Service ex.2	Standard	Outsourcing (Z-MSSP)	2	4
Service ex.3	Advanced	Unassignable	1	2

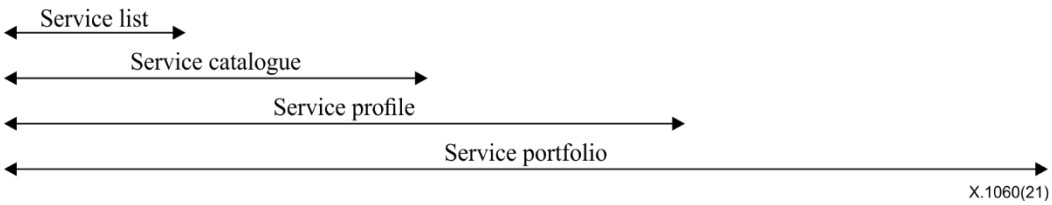

Figure 4 – Services matrix for a CDC

9.2 CDC service recommendation level

To implement the most appropriate CDC services for an organization, the necessity of each service can be considered at the five levels listed in Table 1. The priority of service implementation can be clarified by measuring the levels.

Table 1 – CDC service recommendation level

Weight	Description
Unnecessary	Services deemed unnecessary
Basic	Minimum services to be implemented
Standard	Services that are generally recommended for implementation
Advanced	Services required to achieve a higher-level CDC cycle
Optional	Services arbitrarily selected according to the expected form of CDC

9.3 CDC service assignment

The organization should clarify specifically which team should implement the CDC service. Depending on the capabilities to implement the services in the organization, the organization should determine CDC service assignment, which might include outsourcing. See Table 2.

Table 2 – CDC service assignment

Type	Description
Insourcing	Services are provided by a team within the organization. The organization should specify the team in charge.
Outsourcing	Services are provided by a team outside of the organization. The organization should specify the outsourcer.
Combination	The organization uses insourcing and outsourcing together. A responsible team and a contractor should be specified by the organization.
Unassigned	Although the organization recognises a service, but there is no assignee in the organization.

When using outsourcing, the points A) and B) should be clarified.

A) Nature of information handled

The organization should classify the nature of the information handled, including definitions or distinctions of “internal” and “external” to the organization. For example, in the case of incidents, information including the damage or impact by an attack should be considered internal, while information on the attack itself is considered to be external.

B) Need for specialized security skills

The organization should consider whether specialized skills in the security field are required to provide the service.

CDC services can be classified into quadrants I) to IV) based on these two indicator points. See Figure 5.

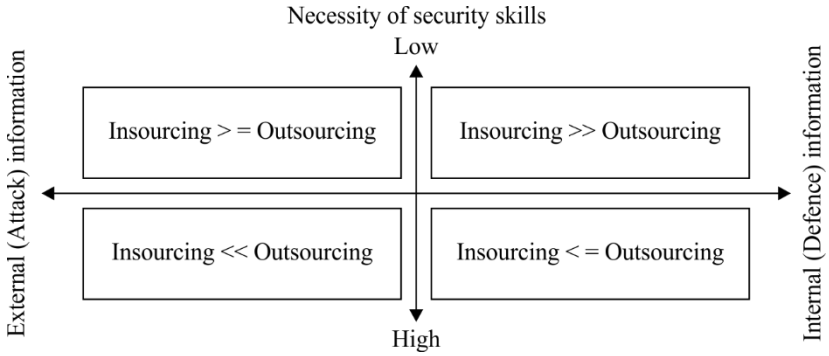

Figure 5 – Sourcing quadrants

I) Insourcing >> Outsourcing

When security expertise is not required to handle confidential information within the organization, insourcing is optimal, and outsourcing is not preferred.

II) Insourcing >= Outsourcing

If the required expertise is not so high, although it is information external to the organization, activity and management should be performed mainly by the organization and with support provided by outsourcing.

III) Insourcing << Outsourcing

In order to deal with information, mainly on attacks, that is external to the organization, the service should be implemented by an organization with specialized skills (e.g., outsourcing). Unless experts with specialized skills are available internally, it is hard for an organization to implement the service by itself.

IV) Insourcing <= Outsourcing

When specialized skills are required to handle internal information within an organization, activity should be performed mainly by a specialized organization (e.g., outsourcing), which the organization should manage and support.

9.4 CDC service assessment

When the CDC service portfolio is created, the implementation status in As-is and To-be of each service should be assessed using the service scores listed in Table 3. It should be noted that different service types, e.g., insource and outsource, should be assessed by the criteria assigned for service scores.

Table 3 – CDC service scores

For insource	
Documented operation is authorized by CISO or other organizational director who has appropriate responsibilities	+5 points
Operation is documented and others can play the role of existing operator	+4 points
Operation is not documented, and others can play the partial role of existing operator temporarily	+3 points
Operation is not documented, and the existing operator can play role	+2 points
Operation is not working	+1 point
Decided not to implement by insourcing	N/A

For outsource	
Content of service and expected output are understood and their outputs are as expected	+5 points
Content of service and expected output are understood but their outputs are not as expected	+4 points
Either content of service or expected output is not understood	+3 points
Both content of service and expected output are not understood	+2 points
Nether output nor report is not reviewed	+1 point
Decided not to implement by outsourcing	N/A

10 Management process

CDC enables security activities throughout the organization by implementing the CDC management process including three phases and two cycles shown in Figure 6.

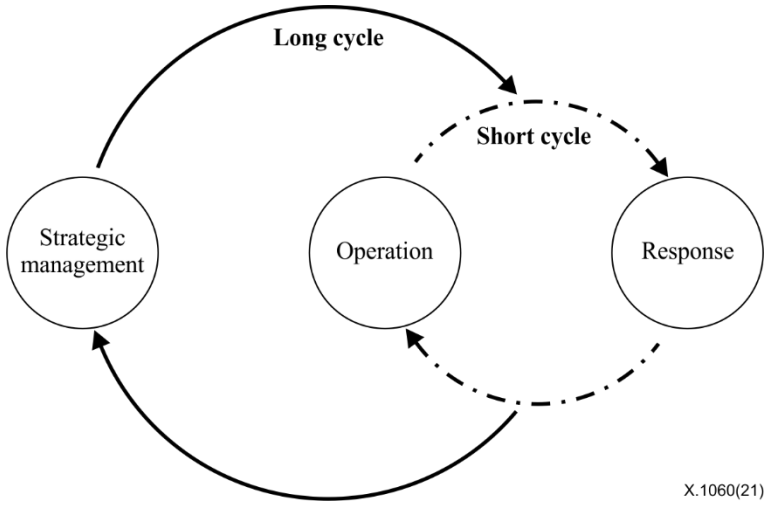

Figure 6 – CDC management process

(1) Strategic management phase

Strategic management has responsibility and accountability for all strategic services relevant to definitions, design, planning, management, certification, etc. that ensure the long-term development of CDC.

(2) Operation phase

The maintenance of the introduced framework should be performed in the operation phase. This is the work at the ordinary or usual time and it typically includes routine activities, e.g., analysis of incident detection, and monitoring and maintenance of security response systems. The team that performs such operations is often called a security operations centre (SOC).

(3) Response phase

An incident response should be executed when an event is detected by the analysis in the operation phase. This phase is always an emergency. Those responding to the incident are often called the computer security incident response team (CSIRT).

The input to the response phase is not limited to that from the operation phase, but the team should also cover responses to reports or notifications from third parties.

A) Short cycle

Operation and response are performed daily. In those processes, problems in the business process and issues in the security response system always appear. Therefore, continuous improvement to resolve those issues, e.g., simple automation of simple tasks, improvement of tools to analyse accuracy and review of report items, are necessary within the resources (people, budget, system) allocated in a short cycle.

B) Long cycle

A review that requires the allocation of new resources should be applied to a long cycle.

If any issues that cannot be solved by the current system are found when reviewing the short cycle, the response should be a long-term perspective and plan, e.g., the introduction of a new security product, a drastic review of security policies and a large-scale configuration change in the security systems.

11 Evaluation process

11.1 Overview

The catalogue, profile and portfolio of the CDC service that are formulated in the build process should be evaluated in a timely and regular manner. Figure 7 depicts a process for evaluating CDC services.

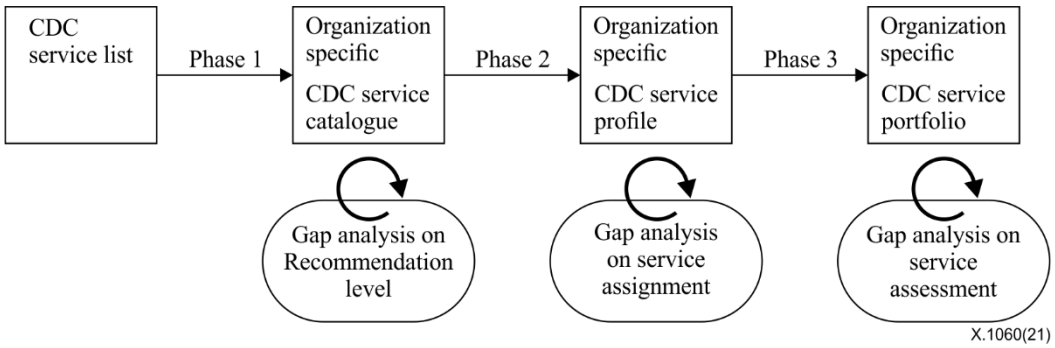

Figure 7 – CDC evaluation process

11.2 CDC service catalogue evaluation

A gap analysis on the CDC service recommendation level should be performed. A review is required due to changes in the environment and threats, particularly, "unnecessary" services should be re-examined and reviewed to ensure no omissions. The CDC service catalogue should be evaluated when the business introduces changes, such as starting new business activities, and response to new risks and threats.

11.3 CDC service profile evaluation

A gap analysis on CDC service assignments should be performed. By deciding service assignments, "unassignable" can be eliminated, and the organization can expect to improve maturity level by reviewing them. The CDC service profile should be evaluated when organizational changes, such as internal organization changes for insource type and outsourcer changes for outsource type, occur.

11.4 CDC service portfolio evaluation

A gap analysis on the CDC service score of individual services should be performed. The difference between the target score in To-be and the score in As-is should be clarified so that the organization can focus on what needs to be improved, confirm the CDC service score again and extract issues. The CDC service portfolio should be evaluated on a regular basis.

12 CDC service categories and service list

The CDC service categories and list are required in the build and management processes (see clauses 9 and 10).

CDC service has nine service categories:

A) strategic management of CDC;

B) real-time analysis;

C) deep analysis;

D) incident response;

E) checking and evaluation;

F) collection, analysis and evaluation of threat intelligence;

G) development and maintenance of CDC platforms;

H) support of internal fraud response;

I) active relationship with external parties.

A. Strategic management of CDC

This category includes policies and resource planning for all security activities mentioned in categories A) to I) in the organization including a CDC in order to ensure its stable operation.

B. Real-time analysis

This category constantly monitors and analyses logs and data from various systems, such as network devices, servers and security products. The goal is to discover threats in real time, which can lead to a rapid and appropriate incident response.

C. Deep analysis

This is a category related to the incident, such as investigating the affected systems, reviewing the compromised data, and analysing the tools and methods used in the attack.

The aim is to elucidate the full scope of the incident and identify the impact.

D. Incident response

This category takes specific actions based on the results of real-time analysis and threat information to deter and eliminate threats.

It aims to minimize the impact on the system and the business, including coordination and reporting with stakeholders.

E. Checking and evaluation

This category is for vulnerability assessment of systems to be protected, and incident response training and its evaluation. The purpose of this category is to improve the level of security.

F. Collection, analysis and evaluation of threat intelligence

This category collects threat information on vulnerabilities and attacks (external intelligence) that is available on the Internet and handles information on real-time analysis and incident response (internal intelligence).

The objective is to improve the accuracy of real-time analysis and incident response, and to improve security assets.

G. Development and maintenance of CDC platforms

This category manages, improves or develops new systems (e.g., security products, log collection databases and operational systems) that are necessary for security response.

The aim is to achieve a smooth and sustainable security activities in other categories.

H. Support of internal fraud response

This category collects audit data to support responses to internal fraud.

The purpose of this category is to support response and resolution of internal fraud by providing logs and analysis.

I. Active relationship with external parties

This category includes coordination and collaboration with internal stakeholders and external organizations.

The objective is to improve the security level of the organization, increase the value of the security to the organization, thus further developing and strengthening the organization.

Figure 8 shows service categories mapping with the management processes, and Table 4 lists the services.

Detailed descriptions of each service in a CDC service list are provided in Annex A.

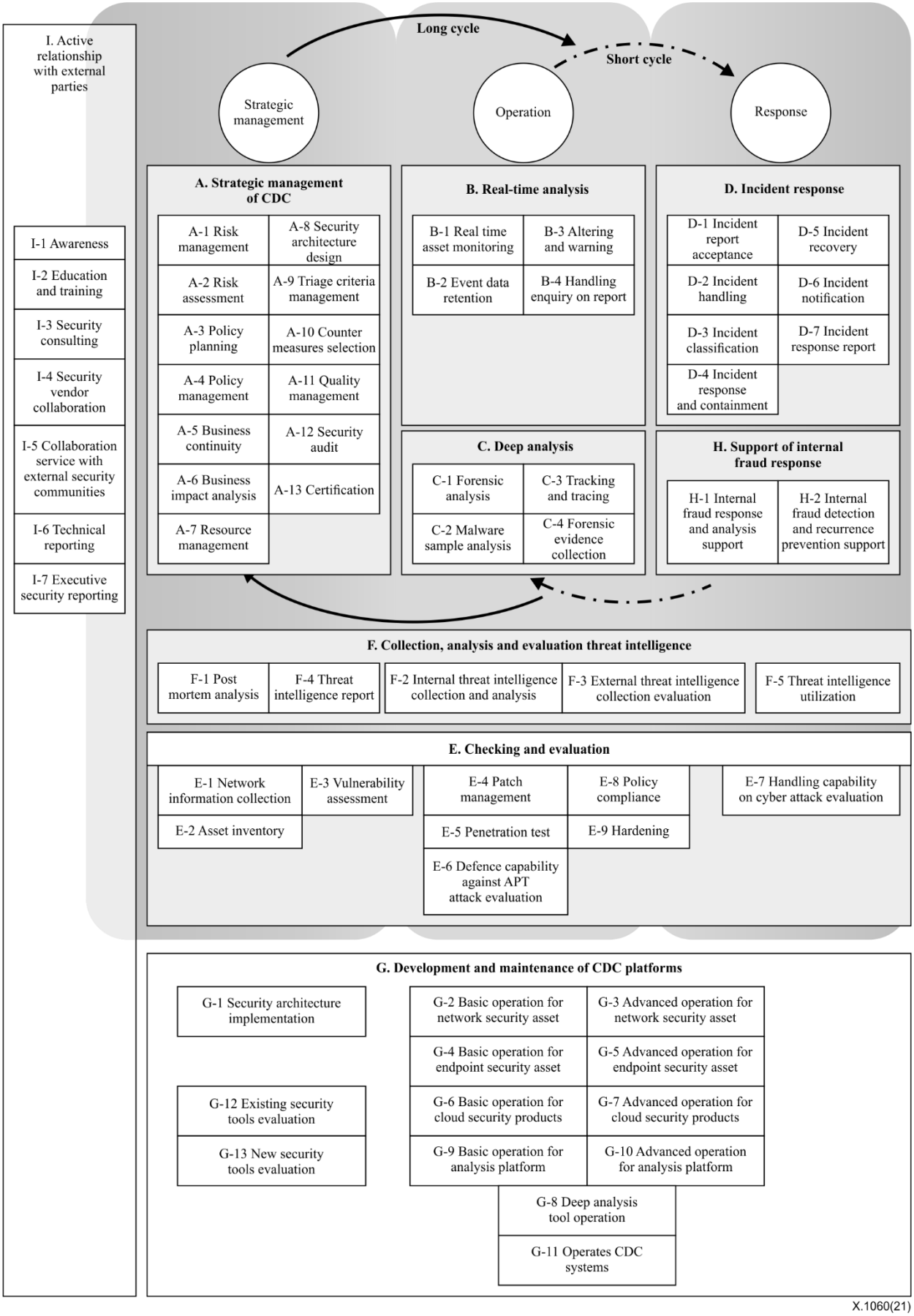

Figure 8 – CDC service categories

Table 4 – CDC service list

A	**Strategic management of CDC**
A-1	Risk management
A-2	Risk assessment
A-3	Policy planning
A-4	Policy management
A-5	Business continuity
A-6	Business impact analysis
A-7	Resource management
A-8	Security architecture design
A-9	Triage criteria management
A-10	Counter measures selection
A-11	Quality management
A-12	Security audit
A-13	Certification
B	**Real-time analysis**
B-1	Real-time asset monitoring
B-2	Event data retention
B-3	Alerting and warning
B-4	Handling enquiry on report
C	**Deep analysis**
C-1	Forensic analysis
C-2	Malware sample analysis
C-3	Tracking and tracing
C-4	Forensic evidence collection
D	**Incident response**
D-1	Incident report acceptance
D-2	Incident handling
D-3	Incident classification
D-4	Incident response and containment
D-5	Incident recovery
D-6	Incident notification
D-7	Incident response report
E	**Checking and evaluation**
E-1	Network information collection
E-2	Asset inventory
E-3	Vulnerability assessment
E-4	Patch management
E-5	Penetration test
E-6	Defence capability against APT attack evaluation
E-7	Handling capability on cyberattack evaluation
E-8	Policy compliance
E-9	Hardening

F	**Collection, analysis and evaluation threat intelligence**
F-1	Post-mortem analysis
F-2	Internal threat intelligence collection and analysis
F-3	External threat intelligence collection and evaluation
F-4	Threat intelligence report
F-5	Threat intelligence utilization
G	**Development and maintenance of CDC platforms**
G-1	Security architecture implementation
G-2	Basic operation for network security asset
G-3	Advanced operation for network security asset
G-4	Basic operation for endpoint security asset
G-5	Advanced operation for endpoint security asset
G-6	Basic operation for cloud security products
G-7	Advanced operation for cloud security products
G-8	Deep analysis tool operation
G-9	Basic operation for analysis platform
G-10	Advanced operation for analysis platform
G-11	Operates CDC systems
G-12	Existing security tools evaluation
G-13	New security tools evaluation
H	**Support of internal fraud response**
H-1	Internal fraud response and analysis support
H-2	Internal fraud detection and reoccurrence prevention support
I	**Active relationship with external parties**
I-1	Awareness
I-2	Education and training
I-3	Security consulting
I-4	Security vendor collaboration
I-5	Collaboration service with external security communities
I-6	Technical reporting
I-7	Executive security reporting

Annex A

CDC service list with descriptions

(This annex forms an integral part of this Recommendation.)

A.1 Category A: Strategic management of CDC

A.1.1 A-1. Risk management

The risk management service is to achieve coordinated activities including A-2 to A-13 to direct and control an organization with regard to risk.

A.1.2 A-2. Risk assessment

The risk assessment service provides a snapshot of the risk level of an organization in terms of assets, threats and security measures.

A.1.3 A-3. Policy planning

The policy planning service is supporting all the activities of defining specific security policies, compiling the guidelines.

A.1.4 A-4. Policy management

The policy management service is to achieve periodic reviews for evaluation of policy and organization rules, to comply with new or external requirements (e.g., regulations and guidelines).

A.1.5 A-5. Business continuity

The business continuity service supports the operational functions necessary to ensure correct implementation and execution of the business continuity plan of an organization.

A.1.6 A-6. Business impact analysis

The business impact analysis service is to achieve a systematic assessment of the possible impacts resulting from various events or scenarios. This service helps organizations understand the scale of loss that could occur. It may cover not only direct financial loss, but also other impacts, such as loss of stakeholder confidence and reputational damage.

A.1.7 A-7. Resource management

The resource management service plans resources (personnel, budget, systems, etc.) to support security activities and allocates them appropriately to each service.

A.1.8 A-8. Security architecture design

The security architecture design service is to establish an architecture to secure the business. Development and maintenance of CDC platforms (category G) can be achieved by compiling various security measurements that consider system design and constraints of business processes (e.g., supply chain).

A.1.9 A-9. Triage criteria management

The triage criteria management service is to set specific triage (response priority) criteria for events (e.g., incidents, vulnerabilities found, threat information discovered) under the agreed scope in the overall policy.

A.1.10 A-10. Counter measures selection

The counter measures selection service is to support all activities of countermeasure selection for triage criteria (A-9) and of the best technologies with respect to all dispositions of security.

A.1.11 A-11. Quality management

The quality management service is to check problems in the quality of security activities, whether or not they have a negative impact for business (e.g., usability, productivity) over a period of time (e.g., one week or one month).

A.1.12 A-12. Security audit

The security audit service systematically and measurably audits how an organization implements security policies and controls at a specific site or time. CDC staff are indirectly involved in audit activities in order to provide necessary information and evidence of implemented state of controls.

A.1.13 A-13. Certification

The certification service supports activities necessary for an organization to conform to various standards and certification schemes.

A.2 Category B: Real-time analysis

A.2.1 B-1. Real time asset monitoring

The real-time asset monitoring service is to supervise and analyse systems status or suspicious activities from logs and network flows, and supporting triage as incident or event for gathering information needed.

A.2.2 B-2. Event data retention

The event data retention service collects and centrally stores events gathered in the process of security monitoring and analysis.

A.2.3 B-3. Alerting and warning

The alerting and warning service notifies the internal function involved of events that highlight potential risks to information assets (e.g., security devices alert, security bulletins, vulnerabilities and spreading threats).

A.2.4 B-4. Handling enquiry on report

The handling enquiry on report service is to respond to enquiries about data and reports regarding analysis.

A.3 Category C: Deep analysis

A.3.1 C-1. Forensic analysis

The forensic analysis service analyses digital evidence that is gathered from security assets and relates to an event to assist in determining what happened.

A.3.2 C-2. Malware sample analysis

The malware sample analysis service is to analyse malware, programs or scripts deployed by attackers that are found during each forensic process.

A.3.3 C-3. Tracking and tracing

The service is the capability of an organization to track and trace the source of any attacks on its infrastructures, which is a critical success factor to reduce further occurrences and prevent security incidents. An acknowledged ability to track and trace both internal and external attackers (e.g., cyber attribution) can pre-empt future attacks.

A.3.4 C-4. Forensic evidence collection

The forensic evidence collection service collects and conserves digital electronic evidence related to an assessed incident, and develops and maintains validity of evidence ("evidence chain of custody").

A.4 Category D: Incident response

A.4.1 D-1. Incident report acceptance

The incident report acceptance service is to receive analytical reports of operations. However, it may receive reports from another organization within the company or from an outside organization.

A.4.2 D-2. Incident handling

The incident handling service is to deal with accepted incidents and coordinates activities including D-3 to D-7.

A.4.3 D-3. Incident classification

The incident classification service is to classify an incident to contribute to a common understanding of the types of incident that occur and what causes them.

A.4.4 D-4. Incident response and containment

The incident response and containment service is to contain an incident before it spreads through all resources and increases the damage to or impact on them.

A.4.5 D-5. Incident recovery

The incident recovery service is to support the restoration of the functionality of a target to its normal system operability.

A.4.6 D-6. Incident notification

The incident notification service is to communicate the occurrence of an incident to incident response teams and other concerned groups.

A.4.7 D-7. Incident response report

The incident response report service is to achieve the completion and distribution of the report of a closed incident response (if countermeasure efforts are protracted, it will be handed over to the strategic management of CDC (category A)). If CDC staff need a report of current status during handling of an incident, this service distributes an interim report.

A.5 Category E: Checking and evaluation

A.5.1 E-1. Network information collection

The network information collection service is to receive an overview of the network configuration that is to be protected.

A.5.2 E-2. Asset inventory

The asset inventory service is to achieve information management relevant to the census of systems, assets and applications that constitute the overall business infrastructure within the scope of CDC support.

A.5.3 E-3. Vulnerability assessment

The vulnerability assessment service is to examine networks, systems and applications to identify vulnerabilities, determines how they can be exploited and recommends how the risks can be mitigated.

A.5.4 E-4. Patch management

The patch management service is to support the installation of any security patches required, while the availability of information technology (IT) service is maintained.

A.5.5 E-5. Penetration test

The penetration test service is to reveal security vulnerabilities that could be exploited by attackers and highlights possible methods of compromise (e.g., threat-led penetration test).

A.5.6 E-6. Defence capability against ATP attack evaluation

The defence capability against advanced persistent threat (ATP) attack evaluation service is to measure the resistance of an organization to targeted attacks while conducting targeted email training and social engineering tests.

A.5.7 E-7. Handling capability on cyberattack evaluation

The handling capability on cyber-attack evaluation service is to confirm whether actual security response activities based on a scenario that assumes an attack has occurred can be activated and whether the incident can be brought to an end without delay (called a cyber-attack response exercise).

A.5.8 E-8. Policy compliance

The policy compliance service is to support the verification of conformity to and compliance with predefined security policies.

A.5.9 E-9. Hardening

The hardening service is to optimize IT component configuration to identify, evaluate and apply systems security configurations, and to mitigate or eliminate the risk of attacks.

A.6 Category F: Collection, analysis and evaluation threat intelligence

A.6.1 F-1. Post-mortem analysis

The post-mortem analysis service describes resolution of an incident to ensure review and improvement of the processes and tools for CDC staff.

A.6.2 F-2. Internal threat intelligence collection and analysis

The internal threat intelligence collection and analysis service is to gather information (internal intelligence) on real-time analysis and incident response.

A.6.3 F-3. External threat intelligence collection and evaluation

The external threat intelligence collection and evaluation service is to gather information (external intelligence), such as new vulnerabilities, attack trends, malware behaviour and malignant Internet protocol addresses or domain information.

A.6.4 F-4. Threat intelligence report

The threat intelligence report service is to compile internal and external threat information and document it, including all details.

A.6.5 F-5. Threat intelligence utilization

The threat intelligence utilization service is to achieve compilation and dissemination of threat information for all categories of security response.

A.7 Category G: Development and maintenance of CDC platforms

A.7.1 G-1. Security architecture implementation

The security architecture implementation service is to implement the security architecture designed by strategic management of CDC (category A) by using assets.

A.7.2 G-2. Basic operation for network security asset

The basic operation for network security asset service is to operate network devices, such as firewalls, intrusion detection system/intrusion prevention system (IDS/IPS), web application firewall (WAF) and proxies.

A.7.3 G-3. Advanced operation for network security asset

The advanced operation for network security asset service is to create custom signatures of an organization for products with attack detection capabilities, such as IDS/IPS and WAF, and applies them if the signature provided by the vendor is insufficient.

A.7.4 G-4. Basic operation for endpoint security asset

The basic operation for endpoint security asset service is to operate countermeasure products, such as anti-virus software, at endpoints.

A.7.5 G-5. Advanced operation for endpoint security asset

The advanced operation for endpoint security asset service is to detect suspicious program activity within the endpoint using its protection product, and collects and analyses registry status, process execution, etc. If needed, the service establishes customised indicators of compromise to enable endpoint detection.

A.7.6 G-6. Basic operation for cloud security products

The basic operation for cloud security products service is to operate security services in a cloud.

A.7.7 G-7. Advanced operation for cloud security products

The advanced operation for cloud security products service is to create custom signatures of an organization for security services in a cloud with attack detection capabilities. If the signature provided by a vendor is insufficient, the service applies custom signatures.

A.7.8 G-8. Deep analysis tool operation

The deep analysis tool operation service is to operate tools used in deep analysis, such as digital forensics and malware analysis.

A.7.9 G-9. Basic operation for analysis platform

The basic operation for analysis platform service is to operate analytical infrastructure that stores the log data required and enables the analysis to be performed routinely, mainly in real-time analysis, such as security information and event management (SIEM).

A.7.10 G-10. Advanced operation for analysis platform

The advanced operation for analysis platform service is to achieve more detailed and accurate analysis using the organization's own systems to retain system logs and packet capture data that commercial SIEMs cannot capture, and develops customized analysis algorithms and logic for these data, as well as the system.

A.7.11 G-11. Operates CDC systems

The operates CDC systems service is to operate systems that perform the tasks required for security response operations, such as the various security response tools previously described, the production of various reports, the response to enquiries, and the vulnerability management system.

A.7.12 G-12. Existing security tools evaluation

The existing security tools evaluation service is to verify the impact on other systems and operations, mainly in terms of availability, when upgrading or changing the settings of existing security-enabled tools.

A.7.13 G-13. New security tools evaluation

The new security tools evaluation service is to design and install new security assets, if new measures are needed in security activities.

A.8 Category H: Support of internal fraud response

A.8.1 H-1. Internal fraud response and analysis support

The internal fraud response and analysis support service is to support the organization responding to internal fraud when it is discovered, by organizing its activities from the logs collected by the security activities.

A.8.2 H-2. Internal fraud detection and reoccurrence prevention support

The internal fraud detection and reoccurrence prevention support service is to analyse the details of internal fraudulent activities that have been discovered, and considers whether it is possible to detect them from the logs, and if so, implements the detection logic.

A.9 Category I: Active relationship with external parties

A.9.1 I-1. Awareness

The awareness service is to precisely create awareness for the relevant staff across and in relation to the CDC, promotes the utilization of the correct tools, best practice, policies and resources to ensure protection of the business assets.

A.9.2 I-2. Education and training

The education and training service is to support specialized training activities in the areas of security for staff in the organizations that the CDC supports.

A.9.3 I-3. Security consulting

The security consulting service provides consultancy services to the various business functions with regards to security.

A.9.4 I-4. Security vendor collaboration

The security vendor collaboration service is to build a direct line of communication with the provider of a security product or service purchased, requests a response to any deficiencies found in the security response and exchanges positive feedback on areas for improvement.

A.9.5 I-5. Collaboration service with external security communities

The collaboration service with external security communities is to exchange information proactively by participating in external communities. Such information can reflect on the security activities.

A.9.6 I-6. Technical reporting

The technical reporting service is to provide reports of the results of monitoring and management activities. These activities help to show the security level of systems and IT infrastructure.

A.9.7 I-7. Executive security reporting

The executive security reporting service is to produce periodic reports and statistical analysis to top management to highlight the security level and indicators of operational performance of an organization.

Bibliography

[b-ITU-T X.1053] Recommendation ITU-T X.1053 (2017), *Code of practice for information security controls based on ITU-T X.1051 for small and medium-sized telecommunication organizations*.

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, 2021