

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

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

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/>.

© ITU 2021

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

Table of Contents

		Page
1	Scope	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Structure of this Recommendation	2
7	Overview of a cyber defence centre	2
8	Framework for the creation and operation of a CDC	2
9	Build process	3
	9.1 Overview	3
	9.2 CDC service recommendation level.....	4
	9.3 CDC service assignment.....	5
	9.4 CDC service assessment.....	6
10	Management process	7
11	Evaluation process.....	8
	11.1 Overview	8
	11.2 CDC service catalogue evaluation.....	8
	11.3 CDC service profile evaluation	8
	11.4 CDC service portfolio evaluation.....	8
12	CDC service categories and service list.....	9
	Annex A – CDC service list with descriptions	13
	A.1 Category A: Strategic management of CDC	13
	A.2 Category B: Real-time analysis	14
	A.3 Category C: Deep analysis	14
	A.4 Category D: Incident response	15
	A.5 Category E: Checking and evaluation	15
	A.6 Category F: Collection, analysis and evaluation threat intelligence	16
	A.7 Category G: Development and maintenance of CDC platforms	17
	A.8 Category H: Support of internal fraud response.....	18
	A.9 Category I: Active relationship with external parties.....	18
	Bibliography.....	20

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.

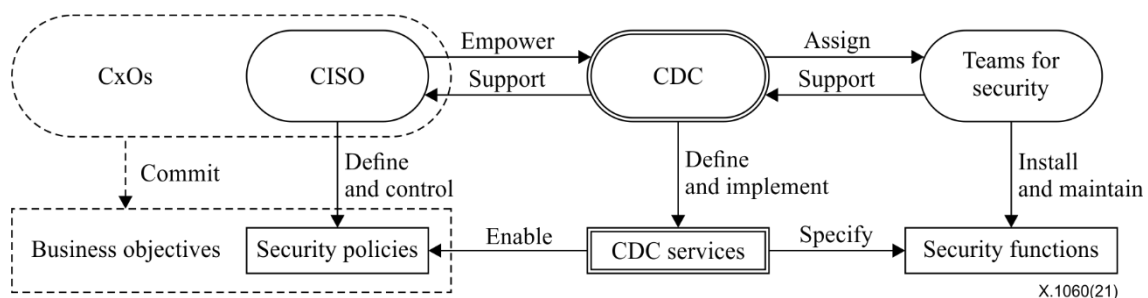


Figure 1 – Stakeholders and their roles for CDC operation

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

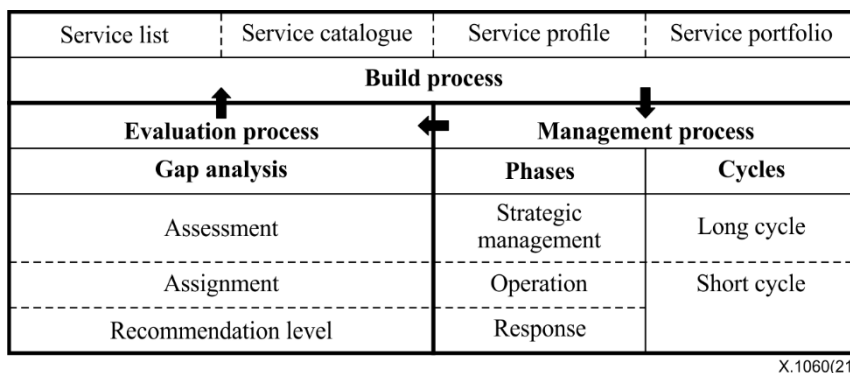
be established and appropriately managed. It should be also assessed in a timely and regular manner and continuously improve. This framework enables the organization to maintain security activities.

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.



X.1060(21)

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.