|  |  |  |  |
| --- | --- | --- | --- |
| The International Teleocmmunication Union - Connecting the World. | **国 际 电 信 联 盟**  **电信标准化局** | |  |
|  | | 2022年1月28日，日内瓦 | |
| **文号：** | **电信标准化局第365号通函 补遗1**  SG17/XY | **致：**  - ITU-T非洲区域成员  **抄送：**  - 国际电联各成员国主管部门；  - ITU-T部门成员；  - ITU-T部门准成员；  - 国际电联学术成员；  - ITU-T各研究组正副主席；  - 电信发展局主任 | |
| **电话：** | +41 22 730 6206 |
| **传真：**  **电子邮件：** | +41 22 730 5853  [tsbsg17@itu.int](mailto:Tsbsg17@itu.int) |
| **事由：** | **有关采用ITU-T X.1060建议书“创建和运营网络防御中心的框架”评估非洲网络防御中心的调查问卷** | | |
| 尊敬的先生/女士：  继2021年12月3日[电信标准化局第365号通函](https://www.itu.int/md/T17-TSB-CIR-0365/en)发起在线调查问卷后（<https://www.research.net/r/ITUTSG17CDCX1060>），请见本补遗附件A的问卷调查表WORD版本，供偏好/要求离线格式的人员使用。  顺致敬意！  Icon  Description automatically generated电信标准化局主任 李在摄  **附件：**1件 | | | |

**Annex A  
Questionnaire on Assessment of Cyber Defence Centres in Africa Using ITU-T X.1060: Framework for Creation and Operation of a Cyber Defence Centre**

# Section 1: Background

1. **Introduction:**

Along with the development of digitalization, [active defence](https://en.wikipedia.org/wiki/Active_defense) is becoming a top prioritized cybersecurity strategy.

[Recommendation ITU-T X.1060: Framework for creation and operation of a Cyber Defence Centre (CDC)](https://www.itu.int/rec/T-REC-X.1060-202106-I) was newly developed by [ITU-T SG17](https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx) in 2021.

This Recommendation provides a framework to build and manage an entity within an organization that offers security services to manage the cybersecurity risks of its business activities, i.e., a CDC, and to evaluate its effectiveness. It specifies a service portfolio with 54 services in nine categories that a CDC should have in order to implement cybersecurity measures.

Some African delegates (e.g. Kenya, Ghana, Senegal) find ITU-T X.1060 very useful to facilitate cybersecurity capacity building.

1. **Objectives of the survey:**

This survey aims to understand the status for cybersecurity measures related to CDC, including government and private sector Security Operations Centre (SOC), Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT) etc., in African countries who may wish to adopt the X.1060 framework. (This survey may extend to other regions in the future.)

Participants in this survey will become aware of ITU-T X.1060 and use it to assess and plan CDC services to enhance cybersecurity of their organizations.

The survey also seeks to disseminate information on security standards and standardization, and to encourage the involvement of more African countries in standardization activities pursuant to provisions of WTSA Resolution 54 on [*Creation of, and assistance to, regional groups*](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-RES-T.54-2016), Resolution 44 on [*Bridging the Standardization Gap* [*between developing and developed countries*](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-RES-T.44-2016)](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-RES-T.44-2016)*,* and Resolution 58 on [*Encouraging the creation of national computer incident response teams, particularly for developing countries*](https://www.itu.int/pub/publications.aspx?lang=en&parent=T-RES-T.58-2016).

1. **Target Responder:**

This survey will be circulated to ITU African Member States and Sector Members and encourage these ITU Members to share it to non ITU Members in their circles as the first step and ITU-T SG17 will receive the survey results.

This survey should be completed by the designated Chief Security Officer (CSO) or Chief Information Security Officer (CISO) of current SOC, CERT, CSIRT etc. and potential future CDC.

This survey will be dispatched via ITU-T Circular letter to designated focal point (DFP) of ITU Member States in Africa, as well as available online. Please forward the online survey to the above appropriate targeted responders in government, public sector, and private sector.

1. **Survey period:**

TSB Circular arrival date (Nov 2021) - End of March 2021

Please attach the survey and send your response by email to [tsbsg17@itu.int](mailto:tsbsg17@itu.int) by 31 March 2021.

1. **Contact**

ITU-T TSB SG17 secretary at: [tsbsg17@itu.int](mailto:tsbsg17@itu.int)

# Section 2: Survey purpose

**Cyber Defence Centre**

CDC is an entity within an organization that offers security services to manage the cybersecurity risks of its business activities.

As an example, in a general company, business goals are set by the board of directors based on corporate governance, and CISO is assigned as a person who responsible for development and implementation of cyber risk strategies and policies. Cyber Defence Centre (CDC) is an entity that practically oversees and implements security measures under the CISO. (See Clause 7, Fig 1 in X.1060 for details.)

X.1060 provides a framework for organizations to build and manage a Cyber Defence Centre (CDC), and to evaluate its effectiveness. The framework indicates how the CDC should define and implement security services to enable an organization’s security.

The term "CDC" implies a new concept; however, it does not mean that a new organization is required. It may be performed by functions that already exist. Such functions are not necessarily carried out by one independent organization, but it may exist across multiple organizations. In other words, if the services described in X.1060 already exist and the related organizations works together, it could be said that a CDC exist.

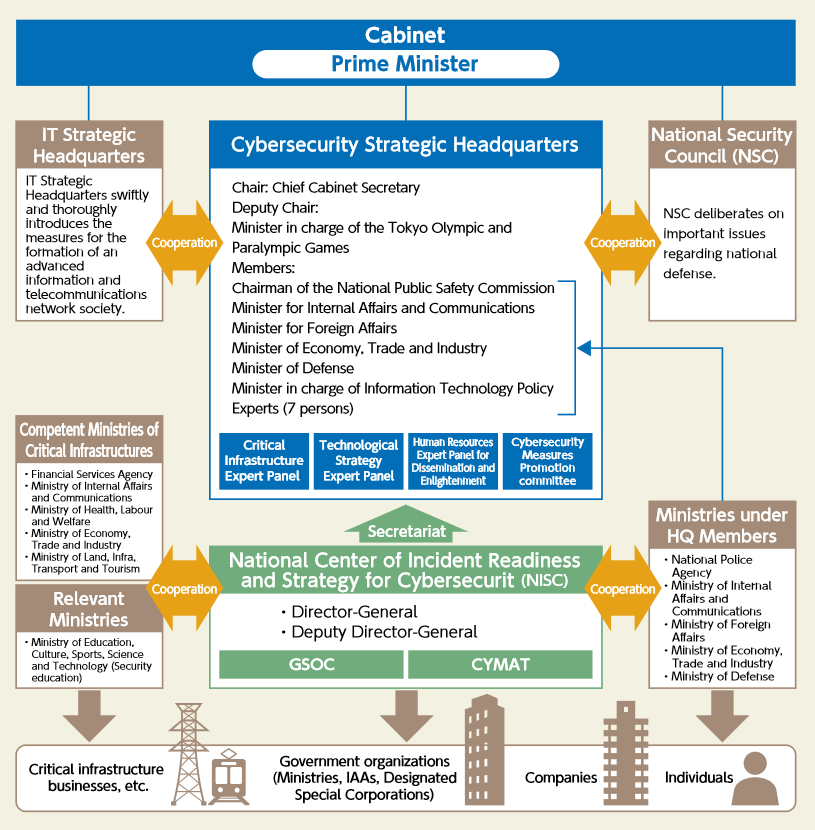
CDC is a rather broader concept than groups currently called SOC, CERT or CSIRT. CDC includes them as a part of the CDC services. The need for CDC as the new concept arises from the fact that threats to information systems can cause serious impacts not only to the systems but also to physical, social, and human aspects; Risks in the cyber domains are having a greater impact on privacy, national security, and economic stability than ever before. Hence, the concept of CDC become so important as an organization to counter these broader impacts that are not limited to information systems.

In order to achieve such cyber risk management, it is important to provide individualized security services and continuously improve those services through integrated management. (See Clause 10 X.1060)

Example: CDC at the national level in Japan

Diagram

Description automatically generated



# Section 3: Questionnaire

Please answer the following 23 questions with reference above CDC and [ITU-T Recommendation X.1060](https://www.itu.int/rec/T-REC-X.1060-202106-I).

Important note: ITU-T Recommendation X.1060 is available for public access in 6 official UN languages (Arabic, Chinese, English, French, Russia and Spanish) at: <https://www.itu.int/rec/T-REC-X.1060-202106-I>. It is recommended to have a complete view of [ITU-T Recommendation X.1060](https://www.itu.int/rec/T-REC-X.1060-202106-I) before start filling this Questionnaire.

1. **Does your organization have cybersecurity strategy or security policy?**

If yes, please describe briefly or indicate URL:

1. **Is there a legal requirement to establish an organization/unit responsible for CDC services (for more detailed explanation about ‘services’ referred in this survey, please see Q8-Q16 later)? If yes, Please provide the link to the law.**
2. **Does your organization have any CDC related service(s), Yes or No?**

If Yes, please specify these services in Q8-Q16. [continue to Q5].

1. **If No, do you plan to implement any of these services, Yes or No?**

If yes, [continue to Q5].

If No, [jump to Q22 (skip the substantive questions of this survey)

1. **Is there an entity within your organization) that is responsible for CDC services? When was it established? Please indicate (x).**

( ) No specific entity (CDC)

( ) 0-2 years

( ) 2 - 4 years

( ) more than 4 years

1. **To whom are these CDC services provided (members), multi-choice?**

( ) internal to my organization [to fill in plain text]

( ) external to my organization [to fill in plain text]

1. **Does your organization have a designated Chief Security Officer (CSO) or Chief Information Security Officer (CISO)?**

Yes | No

Q8 -Q16. (9 categories) **Indicate the** CDC **service**(**s**) **that ha**sbeen **implemented** in your organization **(ref. Table I: Service Catalogue of** [**ITU-T Recommendation X.1060**](https://www.itu.int/rec/T-REC-X.1060-202106-I)**)**

1. **Indicate the service assignment of each CDC service offered (insourcing, outsourcing, combinations, or unassigned) (ref. Table 2 – CDC Service assignment** [**ITU-T Recommendation X.1060**](https://www.itu.int/rec/T-REC-X.1060-202106-I)**)**
2. **Indicate the current score of each CDC service offered (ref. Table 3 - CDC Service scores of** **[ITU-T Recommendation X.1060](https://www.itu.int/rec/T-REC-X.1060-202106-I))**
3. **Indicate the targeted score of each CDC service offered (ref. Table 3 - CDC Service scores of** [**ITU-T Recommendation X.1060**](https://www.itu.int/rec/T-REC-X.1060-202106-I)**).  
   Do you have additional services not covered in ITU-T X.1060 CDC service catalogue** (ref. Q8-Q16)?
4. **Do you have a management process for continuous improvement in place, as outlined in** [**ITU-T Recommendation X.1060**](https://www.itu.int/rec/T-REC-X.1060-202106-I) **Clause 10?**
5. **Do you have any comment?**
6. **Responder**

Organization type: [governmental org/private company]

Organization name, website

Responder’s Position:

Responder’s Contact (e-mail: if possible):

**Thank you for your cooperation. The result will be analysed and reflected future plan for implementation of CDC.**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_