THE WORLD BANK

PRACTITIONER NOTE

# DIGITAL FIRST RESPONDERS

## THE ROLE OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTS) IN DEVELOPING COUNTRIES

June 2024

Cybersecurity MULTI-DONOR TRUST FUND

# Audience and scope

This note intends to provide policy makers in developing countries with a clear understanding of the role and importance of CSIRTs for enhancing cyber resilience. It provides new data and evidence on the status of CSIRT deployment across regions and income groups and outlines practical recommendations on how to establish and operate national CSIRTs, including for costs and staffing. The note does not examine other key dimensions of cyber resilience, such as national cybersecurity strategies and governance models, skills development, and legal frameworks, as these are discussed in other World Bank knowledge products.

# Disclaimer

This note is based on the data available at the time of writing, and reflects evolving international good practices, including experiences in a wide range of countries from different regions. It primarily relies on FIRST membership as a proxy indicator to determine the effectiveness of a CSIRT. The authors of this note recognize that this proxy indicator does not necessarily reflect the reality of every context on the ground. However, while this proxy indicator has limitations, it proves useful and generally accurate in assessing the incident response capacity in countries from various regions and income groups, including in lower-income contexts.

# Acknowledgements

This note was written by Ghislain de Salins, Senior Digital Development Specialist, and Robert Collett, consultant, from the World Bank Digital Development Global Practice, in partnership with Chris Gibson, Serge Droz, Olivier Caleff and Klee Aiken from the global Forum of Incident Response and Security Teams (FIRST). It was reviewed by Giacomo Assenza, Paul Seaden, and Anders Pedersen from the World Bank, as well as by Jean-Robert Hountomey (AfricaCERT) and Vilius Benetis (NRD). It builds on previous publications on incident response capacity building by ITU, OAS, ENISA, GFCE and FIRST (referenced in the last section of this document), among others. The development of this note was funded by the World Bank Cybersecurity Multi-Donor Trust Fund.

# Table of Contents

# Acronyms and abbreviations

| | |
|---|---|
| AFE | EASTERN AND SOUTHERN AFRICA |
| AFW | WESTERN AND CENTRAL AFRICA |
| ANSSI | THE NATIONAL INFORMATION SYSTEMS SECURITY AGENCY (FRANCE) |
| APCERT | ASIA PACIFIC COMPUTER EMERGENCY RESPONSE TEAM |
| CAPEX | CAPITAL EXPENDITURE |
| CDA | CYBER DEFENSE AFRICA |
| CERT | COMPUTER EMERGENCY RESPONSE TEAM |
| CIA | CONFIDENTIALITY, INTEGRITY, AVAILABILITY |
| CIP | CRITICAL INFRASTRUCTURE PROTECTION |
| CIRT | COMPUTER INCIDENT RESPONSE TEAM |
| CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (UNITED STATES) |
| CSF | CYBERSECURITY FRAMEWORK |
| CSIRT | COMPUTER SECURITY INCIDENT RESPONSE TEAM |
| CTI | CYBER THREAT INTELLIGENCE |
| DDOS | DISTRIBUTED DENIAL OF SERVICE ATTACK |
| EAP | EAS0OF THINGS |
| ISAC | INFORMATION SHARING AND ANALYSIS CENTER |
| ISO | INTERNATIONAL ORGANIZATION FOR STANDARDIZATION |
| IT | INFORMATION TECHNOLOGY |
| ITU | INTERNATIONAL TELECOMMUNICATION UNION |
| LAC | LATIN AMERICA AND THE CARIBBEAN |
| LICS | LOW-INCOME COUNTRIES |
| MENA | MIDDLE EAST AND NORTH AFRICA |
| MICS | MIDDLE-INCOME COUNTRIES |
| NCSIRT | NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM |
| NIST | UNITED STATES NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY |
| OAS | ORGANIZATION OF AMERICAN STATES |
| OPEX | OPERATIONAL EXPENDITURE |
| PSIRT | PRODUCT SECURITY INCIDENT RESPONSE TEAM |
| PPPS | PUBLIC-PRIVATE PARTNERSHIPS |
| SAR | SOUTH ASIA REGION |
| SIEM | SECURITY INCIDENT AND EVENT MANAGEMENT |
| SIM3 | SECURITY INCIDENT MANAGEMENT MATURITY MODEL |
| SLAS | SERVICE LEVEL AGREEMENTS |
| SOC | SECURITY OPERATION CENTER |
| SOP | STANDARD OPERATING PROCEDURE |
| TBA | TRUSTBROKER AFRICA |
| TNO | NETHERLANDS ORGANISATION FOR APPLIED SCIENTIFIC RESEARCH |

# Executive summary

- **Computer Security Incident Response Teams (CSIRTs) are the digital equivalent of firefighters and other first responders.**
- **CSIRTs are key to the foundation of any national cybersecurity ecosystem.** In addition to incident response, they can provide trainings, raise awareness, and facilitate community building. However, they do not engage in law enforcement or policy development.
- **There is a strong correlation between a country's robust incident response function and its overall cybersecurity capacity.** In Western and Central Africa, for example, the four countries that score highest in the International Telecommunication Union (ITU) Global Cybersecurity Index (GCI) are also the ones with a fully operational CSIRT.[1]
- **While more than 500 CSIRTs have been established in high-income countries, only six low-income countries have a fully operational CSIRT.** On average, middle-income countries only have one operational CSIRT.
- Compared with the estimated annual costs of cybersecurity incidents (up to 3 percent of GDP), **investing in incident response stands out as yielding remarkable returns for economic development overall.**
- **Investments in establishing, enhancing, and operating CSIRTs should be further prioritized in developing countries.**
- **In low-income countries, governments should focus on establishing and operationalizing the national CSIRT (nCSIRT) function.** At its inception, the nCSIRT can focus on providing services solely to the government or to certain operators of critical infrastructures.
- **In middle-income countries, governments should strengthen their nCSIRT function and establish a robust network of sectoral CSIRTs** dedicated to critical infrastructure protection.
- **Newly established CSIRTs should "start small"** by focusing on a few constituents and a limited set of core services, especially in lower-income contexts. They can grow over time to adjust to evolving context, demand, and resources.
- **The use of open-source tools** and resources developed by the practitioner community can help to reduce initial investment and operating costs for CSIRTs.
- **Participation in international and regional incident response networks is essential** to secure "quick wins" (e.g., peer-to-peer learning) and rapidly build capacity in newly established CSIRTs.
- **Some innovative models (e.g., Public-Private Partnerships (PPPs)) are being implemented** and could facilitate knowledge transfer and reduce the initial public investments needed to establish CSIRTs.

1 In the context of this note, FIRST membership is used as a proxy indicator to determine the effectiveness or presence of a CSIRT in a given country.

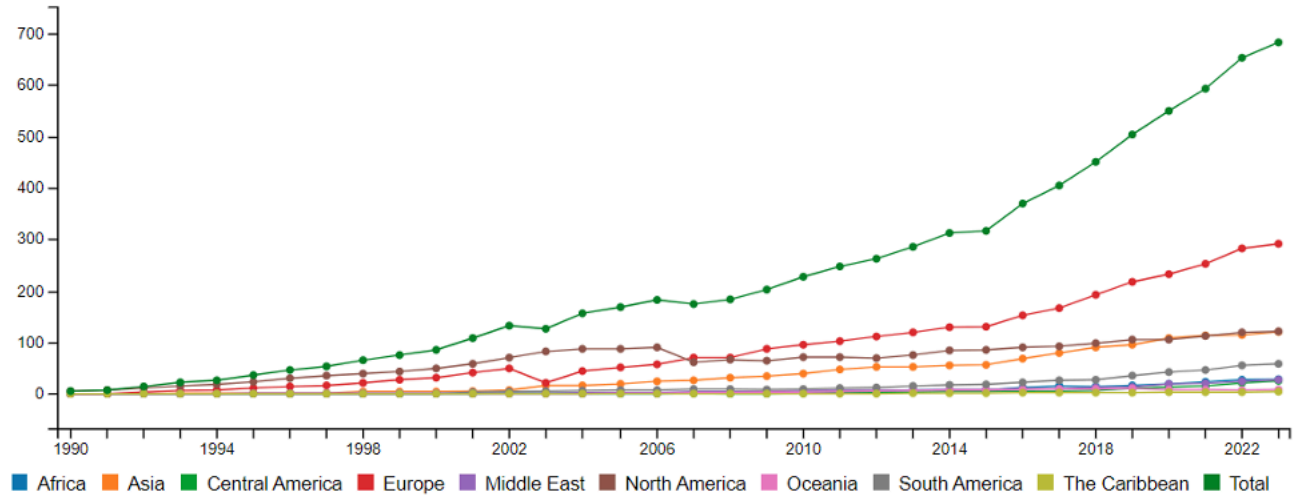
# Introduction

The impact of cybersecurity incidents continues to increase, with **annual costs to society representing up to 3 percent of GDP** (World Bank, 2024 (forthcoming)). In developed and developing countries alike, critical sectors such as healthcare, energy, and transport are increasingly hit by cybersecurity incidents. For most governments and organizations across the world, the relevant question is no longer *if* a cybersecurity incident will happen but rather *when*.

**As a result, governments have been investing significantly in their capacity to detect and respond to cybersecurity incidents.** While firefighters and healthcare emergency workers are the typical first responders for incidents in the physical world, the staff of Computer Security Incident Response Teams (CSIRTs) are the standard first responders in the digital realm.

**CSIRTs cooperate at the international level through the Forum of Incident Response and Security Teams (FIRST),** as well as through various regional organizations such as Africa Computer Emergency Response Team (AfricaCERT), TrustBroker Africa, CSIRTAmericas or APCERT (for Asia-Pacific). FIRST was established soon after the Morris worm significantly disrupted the Internet in 1988 (Denning, 1989), with around 5 participating teams. As of 2024, over 700 incident response teams across 108 countries are members of FIRST (see Figure 1).

**Figure 1. Evolution of the number of incident response teams participating in FIRST**




Source: FIRST

**Membership in FIRST can be considered a relevant proxy indicator of a country's overall incident response capability,**[2] and developed countries typically have many teams participating in FIRST.

**In high-income countries, the incident response ecosystem is usually quite developed.** These countries usually have specialized CSIRTs for critical sectors as well as enterprise-level CSIRTs for some large organizations. In high-income contexts, national CSIRTs (nCSIRTs) often play the role of coordinator for the incident response ecosystem, and are also held in reserve as a CSIRT of "last resort" for major incident cases. In the United States, Spain, and Japan, 111, 57, and 44 teams participate in FIRST, respectively (FIRST, May 2024). On average, there are more than six CSIRTs in each

2 While some existing CSIRTs do not participate to FIRST, this note relies on FIRST membership as a proxy indicator to determine the effectiveness of a CSIRT and the overall incident response capability at the country level.

high-income country (see Table 1). Larger countries often have many more teams that are not members of FIRST (e.g., in Japan alone, the Nippon CSIRT Association (NCA) counts more than 500 members).

**In middle-income countries, a national or a government CSIRT is often operational,** in addition to one or a few sectoral CSIRTs (e.g., for the financial or telecoms sectors) in some cases. However, the maturity of the CSIRTs in middle-income countries is often more limited than in high-income countries. Costa Rica, Georgia, Ghana, and Egypt each have two CSIRTs participating in FIRST. On average, there is at least one CSIRT in each middle-income country (see Table 1).

**In low-income countries, incident response capabilities are typically more limited (see Table 1). Only six low-income countries** – Ethiopia, Malawi, Rwanda, Sudan, Togo, and Uganda – **have a CSIRT participating in FIRST and no low-income country has more than one.** In some low-income countries, there is a nascent incident response capability, although their effectiveness remains limited.

**Table 1. Incident response capacity by income group and World Bank region**

| Country group | Number of CSIRTs* | Average number of CSIRTs* |
|---|---|---|
| **High-income countries** | 547 | 6.6 |
| **Middle-income countries** | 164 | 1.5 |
| **Low-income countries** | 6 | 0.2 |
| **Eastern and Southern Africa (AFE)** | 15 | 0.6 |
| **Western and Central Africa (AFW)** | 6 | 0.3 |
| **East Asia and Pacific (EAP**)** | 19 | 0.8 |
| **Europe and Central Asia (ECA**)** | 32 | 1.6 |
| **Latin America and the Caribbean (LAC**)** | 82 | 3.4 |
| **Middle East and North Africa (MENA**)** | 10 | 0.8 |
| **South Asia Region (SAR)** | 6 | 0.7 |

*Defined as an incident response team with FIRST membership.

** Not including high-income countries located in the region

Source: FIRST, World Bank

**Establishing and enhancing CSIRTs in low- and middle-income countries has therefore become a key element of the digital development agenda.** In both low- and middle-income countries, the establishment and enhancement of CSIRTs is often supported by international development assistance financed through organizations such as the World Bank, International Telecommunication Union (ITU), Organization of American States (OAS) and the European Union (EU). For example, the World Bank has helped establish CSIRTs in many countries across regions, including Armenia, Bangladesh, Bhutan, Ghana, Kyrgyzstan, and Sierra Leone, among others.

**However, the role of CSIRTs in overall cyber resilience, and the key success factors that enable their operationalization, are still often unclear to policy makers.** Thus, this note aims to provide policy makers with a clear understanding of the role and importance of CSIRTs, while offering evidence-based policy advice on CSIRT establishment and enhancement in developing countries based on recognized best-practices and on-the-ground experience from World Bank projects. Towards this end, Table 2 debunks some common misconceptions that often cloud policy discussions on investments for CSIRTs in developing countries.

**Table 2. Common misconceptions about CSIRTs**

| Misconception | Reality | Insights for international development |
|---|---|---|
| **CSIRTs require extensive funding and advanced technology.** | Some CSIRTs can operate effectively with limited funding, particularly if they rely on small teams and use open-source tools.[3] Although some nCSIRTs have more than 50 staff members, other nCSIRTs have provided effective services with a team of just five people. | In some lower-income contexts, it is possible to establish effective CSIRTs with an initial funding envelope as low as $500,000 – for the first stages of operation. |
| **Establishing a CSIRT is a one-time effort.** | Building, maintaining, and enhancing an effective CSIRT is an ongoing process that requires continuous investments and improvements, e.g., through upskilling, outreach to constituents, and international cooperation. Cybersecurity risks are constantly evolving, and CSIRTs need to adapt to keep pace with these changes. | In lower-income contexts, stakeholders often focus on capital expenditure (capex) when establishing a CSIRT, while neglecting the operational expenditure (opex) necessary to make the CSIRT sustainable. This can lead to the decline of the CSIRT after a few years, when the initial funding mechanism (e.g., credits or grants) ends. |
| **CSIRTs can operate in isolation.** | Effective incident response requires cooperation and information sharing, including with international partners. Participation in global and regional networks facilitates this cooperation. | In lower-income contexts, participation in international networks is often deprioritized, which can significantly limit the overall effectiveness of CSIRTs. |
| **One can "copy-paste" a nCSIRT model from one country to another.** | There is no *one-size-fits-all* model for establishing and enhancing nCSIRTs. Some focus on government institutions, while others support private sector-owned Critical Infrastructure Protection (CIP). In higher-income contexts, the nCSIRT focuses on facilitating cooperation in the incident response ecosystem. | In lower-income contexts, it is key to "start small" by focusing on a few constituencies and services, while building trust with key stakeholders and securing funding to enable the sustainable development of the CSIRT. |
| **CSIRTs should focus exclusively on technical expertise.** | Attracting and retaining talent with technical expertise as well as upskilling staff are key components to successful CSIRT development. However, good governance, communication, outreach to stakeholders and capacity building are also essential. | A common pitfall in lower-income contexts is to focus solely on technical expertise while neglecting other key elements such as outreach to key stakeholders, communication with constituents, and capacity building. |

Source: World Bank.

3 See, for instance, resources available at https://opencsirt.org/ and open-source software such as The Hive, OpenCTI, IntelMQ, TaranisNG, RTIR, MISP and OpenVAS.

# 1. What are CSIRTs?

**CSIRT, CERT, and CIRT are all related terms that refer to the same concept of cybersecurity incident response team.** The term CERT™ was trademarked in the United States by Carnegie Mellon University in 1997, which encouraged the use of alternatives. The ITU often refers to "CIRTs" while FIRST and the OAS typically use the term "CSIRT".

The diversity of existing acronyms for the incident response function reflects the bottom-up approach that characterized the emergence of CSIRTs in the past 30 years. However, efforts have since been made to provide more standardization to the incident response function, as discussed in Box 1.

### Box 1. Towards standardization of the incident response function

Since its inception in the 1990s, the community of incident response practitioners has developed many tools that provide comparability and guidance for the establishment and enhancement of CSIRTs.

For instance, the Security Incident Management Maturity Model (SIM3) provides a framework to assess the maturity of CSIRTs. SIM3 is made of 45 measurable parameters (e.g., "mandate," "constituency," and "code of conduct") that are divided into four key areas ("Organizational," "Human," "Tools," and "Processes"). The maturity of a CSIRT can be analysed for each parameter through five maturity levels. Self-evaluation through SIM3 is a pre-requisite for CSIRTs to become members of FIRST.

Importantly, as the mandate, constituency, and service offering of CSIRTs can vary significantly, they usually only implement a subset of these requirements. In other words, a CSIRT can be fully operational and provide value to their constituents without achieving high maturity in each of the 45 SIM3 parameters.

More recently, other standards relevant to the incident response function have emerged, including the FIRST CSIRT Services Framework, ITU CIRT Framework, NIST 800-61, ITU-T X.1060 and ISO/IEC 27035.

Source: World Bank, Open CSIRT Foundation

**To understand the role of CSIRTs in overall cyber resilience, it is helpful to consider the NIST Cybersecurity Framework (CSF),** which conceptualizes cybersecurity risk management around six key functions: govern, identify, protect, detect, respond, and recover (see Figure 1).

**Figure 1. Risk management functions in the NIST Cybersecurity Framework**


Source: (NIST, 2024, p. 6).

**CSIRTs can be defined as organizations or units that specialize in the "respond"[4] function, as the core characteristic of CSIRTs is to provide incident handling capabilities.** Incident response is the primary mandate of CSIRTs, even though in many countries they also provide "incident detection" services and perform other roles, such as facilitating broader cooperation for cybersecurity risk management through trainings, awareness-raising, promoting cyber hygiene, and threat information sharing.

CSIRTs should be distinguished from the following entities:

- **Security Operations Centers (SOCs)**, i.e., organizations or units that focus on the "detect" function through network monitoring. SOCs can be incorporated within CSIRTs, typically in a physical area or separate room dedicated to centralized, real-time monitoring and incident handling allocation. SOCs can also exist independently of CSIRTs, enabling organizations to monitor their own networks.
- **Information Sharing and Analysis Centers (ISACs)**, i.e., organizations or platforms that focus on enabling cooperation for cybersecurity teams within the same sector or for organizations sharing a common interest. ISACs primarily enable information sharing but usually do not provide an incident handling function.
- **Cybersecurity Agencies or Authorities** (e.g., The National Information Systems Security Agency (ANSSI) in France or Cybersecurity and Infrastructure Security Agency (CISA) in the United States), which are governmental bodies defining and implementing cybersecurity policies. CSIRTs typically focus on technical aspects and do not engage in public policy development – even though nCSIRTs are sometimes established or later integrated within such agencies.
- **Law enforcement agencies**, which perform criminal investigations. CSIRTs do not engage in such activities, as their role is rather to provide technical expertise to a defined community of constituents.

4 Or as "a capability set up for the purpose of assisting in responding to computer security-related incidents" (NIST, 2021)

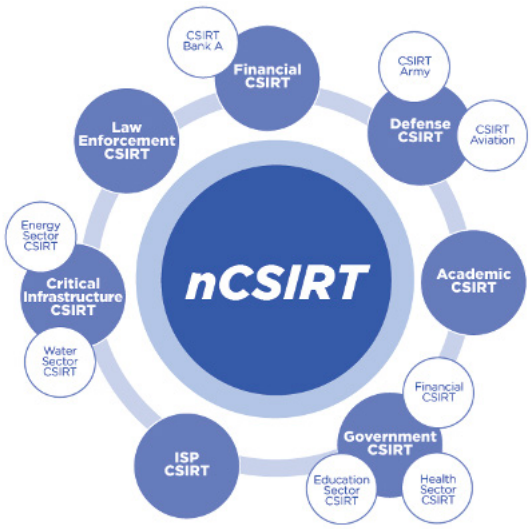
# 2. Key features of CSIRTs

Constituency, service offering, and governance are three features fundamental to defining the role of a given CSIRT. They determine the appropriate funding and staffing levels necessary to CSIRT operationalization. For the national incident response function, these features should be clearly defined within a mandate given by the government or by law to the nCSIRT and its host institution.

## Constituency

**Constituencies are the customer base or recipients of the services provided by the CSIRT.** The constituency should be clearly defined early in the CSIRT mandate. CSIRTs are typically categorized as national (nCSIRT), governmental, sectoral (e.g., financial, health, energy, telecoms, etc.), or focusing on certain products (PSIRT) or organizations. In developed countries, the role of the nCSIRT is typically to coordinate the overall incident response ecosystem, while specialized CSIRTs can be considered their key constituents (see Figure 2).

**Figure 2. CSIRT constituencies in a developed incident response ecosystem**




Source: OAS (2023)

However, in lower-income countries, the incident response ecosystem is less developed, and nCSIRT constituencies typically focus either on:

- The government, i.e., ministries and central government agencies. **In Bangladesh**,[5] the e-Government Computer Incident Response Team (BGD e-Gov CSIRT), whose operationalization was financed by the World Bank from 2016-2020, focuses solely on governmental entities.
- Operators of certain critical infrastructures (e.g., energy, water, transport, banking, etc.), based on the national CIP policy.

**The national context is key to defining the right constituency for the nCSIRT.** If a government CSIRT already exists, the nCSIRT can focus on private sector-owned critical infrastructure. In contrast, if the incident response capabilities do not yet exist, the nCSIRT can focus exclusively on governmental entities.

5 BGD e-GOV CSIRT, 2024, https://www.CSIRT.gov.bd/

**CSIRT constituencies can evolve over time as the national incident response ecosystem develops.** If new sectoral CSIRTs are established, the nCSIRT can progressively delegate incident handling in these sectors while focusing on overall coordination at the national level.

**From 2014-2017, the World Bank helped the government of Ghana establish its nCSIRT,** which is now hosted within Ghana's Cyber Security Authority (World Bank, 2023). Other CSIRTs have since been established in the country, focusing on specific critical sectors. With the technical assistance and financing provided by the World Bank, Ghana made remarkable progress towards cyber resilience, becoming the top-performing country for cybersecurity capacity in Western and Central Africa in 2021 (ITU, 2021). The setup of a robust incident response ecosystem has been instrumental to Ghana's achievements – as of 2024, Ghana is the only country in Western and Central Africa with more than one incident response team registered with FIRST.

**In lower-income contexts, a common pitfall for newly formed nCSIRTs is to be overly ambitious when identifying constituents.** For instance, a mandate considering that "all users of the national cyberspace" or "all operators of critical infrastructures" will be served by a newly created nCSIRT is likely to lead to underwhelming results, as the nCSIRT can lack the human and financial resources necessary to effectively implement such mandate. The lack of effective communication and outreach to constituents is another risk that can hinder the effectiveness of CSIRTs.

**Newly established CSIRTs should therefore "start small" and focus on fewer constituents** (e.g., one or two critical sectors), while investing in key functions such as technical expertise, trainings, outreach, and communication.

## Services

**The second key feature of CSIRTs is the service offering they provide to their constituents.** The extent of these services will determine the budget and staff needed for the effective functioning of the CSIRT.

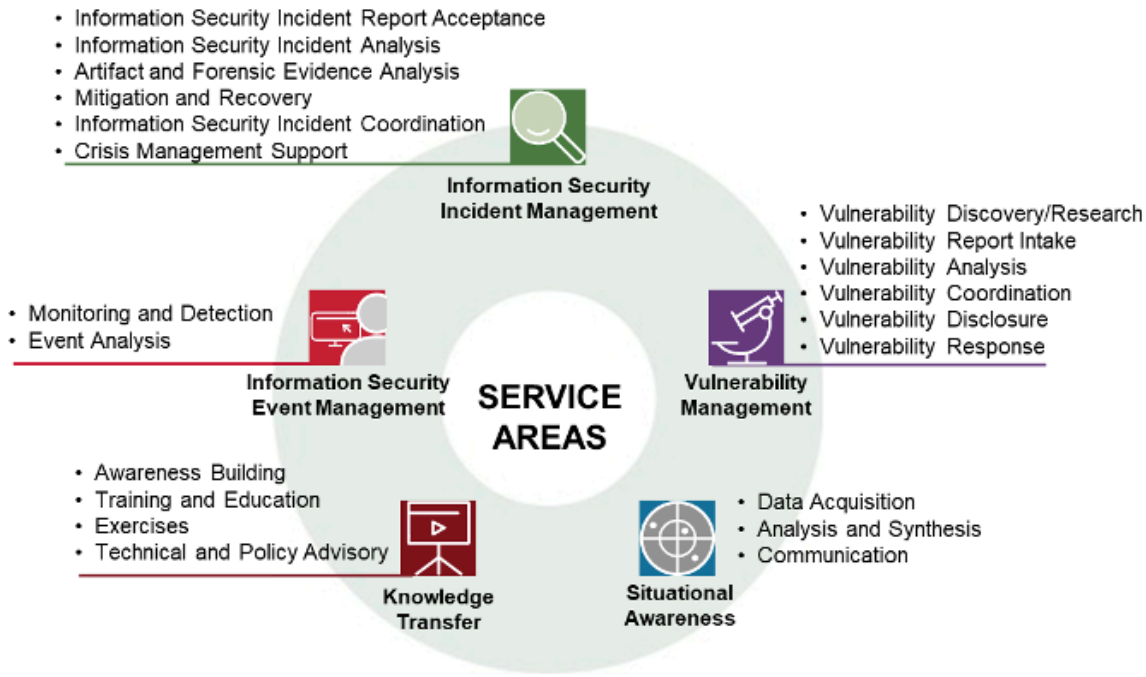
**Historically, the main service provided by CSIRTs has been the handling of incidents,** which requires the establishment of Standard Operating Procedures (SOPs) or policies that enable CSIRT staff to evaluate the severity of each event and allocate resources accordingly (see Figure 3).

**Figure 3. Cybersecurity incident handling example pathway**


Source: (European Union Agency For Cybersecurity (ENISA), 2020, p. 23)

**Over the years, the role of CSIRTs has evolved** from providing limited incident handling services to coordinating and communicating with different stakeholders, as well as sharing threat information and providing technical training to their constituents. Just like firefighters, CSIRTs increasingly do more than just respond to emergencies – they also raise awareness, provide trainings, and build relationships with their community of stakeholders and constituents. The CSIRT Services Framework,[6] developed by FIRST, outlines five main service areas for CSIRT activities, as shown in Figure 4.

**Figure 4. Service Areas for CSIRTs**




Source: (FIRST)

**In lower-income contexts, CSIRTs should "start small" and limit their service offering to the core needs of their constituents.** For instance, in its first two years, a newly established nCSIRT or sectoral CSIRT can focus on incident analysis, forensics, vulnerability coordination, and awareness building. In years three and four, if the CSIRT managed to build solid relationships with its constituents and grow its team, it can extend its service offering towards situational awareness, table-top exercises, and crisis management support, among others. Importantly, different services can be offered to different constituents. For instance, a nCSIRT could provide incident handling services to governmental entities, while only engaging in awareness raising and promoting cyber hygiene to citizens at large.

6 FIRST, 2020, https://www.first.org/standards/frameworks/CSIRTs/CSIRT_services_framework_v2.1

## Governance

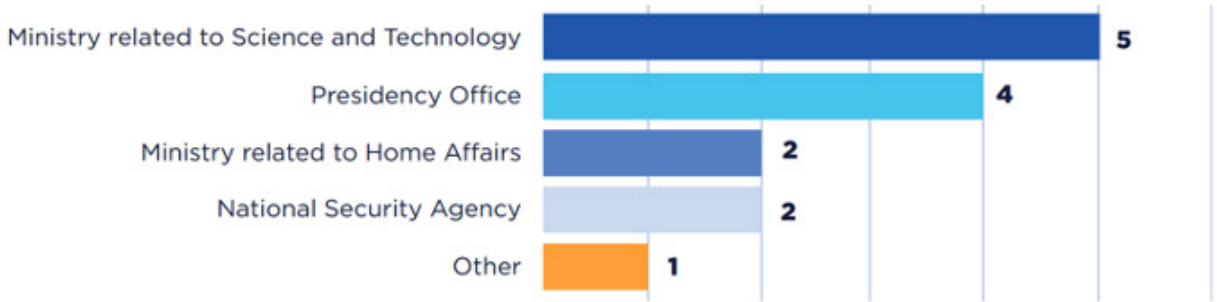
The last key feature of a CSIRT is its governance model, which can greatly vary across countries and sectors. The governance of the CSIRT depends primarily on:

- **The host or parent organization.**
  - A government or nCSIRT can be hosted in a government organization, such as the National Cybersecurity Agency, the telecom regulator, or the Ministry of Digital. In other cases, nCSIRTs are hosted within independent multi-stakeholder associations.
  - A sectoral CSIRT can be hosted within a public body (e.g., a Central Bank for the financial sector or the Ministry of Health for the health sector), or within an ad-hoc structure led by the private sector or civil society (e.g., a university or a trade association).
- **The business model** that enables the CSIRT to secure enough funding to provide services to its constituents (see Table 3).
  - If the CSIRT is hosted within the government, a stable funding allocation should be earmarked for incident response in the government budget.
  - If the CSIRT supports constituents in the private sector, membership fees may help secure the funding. However, a bottom-up, voluntary approach is typically key to build trust with the constituents – imposing fees through a top-down approach from the outset could result in chilling effects and limit effective cooperation.

**In lower-income contexts, CSIRTs often face two key challenges when choosing a business model:** i) building trust and proving value to their constituents, and ii) securing long-term funding.

**The ability to build trust with their constituents is a key success factor for CSIRTs.** If the host organization lies within the defense, intelligence, or law enforcement community, for instance, it may be more difficult for CSIRTs to build trust with external constituents. The World Bank usually recommends governmental or nCSIRTs to be hosted within civilian institutions, such as Ministries or independent agencies. In Latin America and the Caribbean, most nCSIRTs are hosted within civilian bodies, such as ministries related to Science or Technology or the Presidency Office (see Figure 5).

**Figure 5. National CSIRT placement within the Americas**




Source: OAS, 2023.

**Table 3. Examples of potential funding models for CSIRTs**

| Funding mechanism | Benefits | Risks | Key factors | Example |
|---|---|---|---|---|
| **Earmarked government budget** | Can be more stable and enable long-term planning, if government support is guaranteed.<br><br>Can be necessary in the first stages of CSIRT establishment when the value proposition still needs to be demonstrated. | Can provide less incentives for the CSIRT to evolve and effectively respond to a wider membership base.<br><br>In some cases, can be more dependent on changes in political leadership or governmental restructuration. | This model requires long-term governmental support and is likely to be successful in politically stable countries where cybersecurity is recognized as a policy priority (e.g., through a dedicated cybersecurity agency) | In Ghana, the national CSIRT is hosted within the national Cyber Security Authority and benefits from an earmarked |
| **Membership fees** | Can provide more incentives to closely align CSIRT service offering and activities with the needs of the membership base.<br><br>Can be more flexible and allow for progressive growth in case members decide to allocate more resources to the CSIRT. | Can be more difficult to implement in the first stages of CSIRT establishment, as the value proposition may still be unclear to potential members.<br><br>Can be less stable and limit long-term financial planning, particularly if funding is dependent upon one or two key members. | This model requires strong engagement from the private sector and is likely to be successful where co-operation mechanisms (including between competitors within a sector) are already in place. | The Nordic Financial CERT brings together financial institutions from five Nordic countries in Europe. |
| **Hybrid or blended** | Can provide more flexibility for budget allocation and growth.<br><br>Can limit dependency on members and political leadership. | Can lead to conflicts of interests or confusion among stakeholders.<br><br>In some cases, can compete with services that could be offered by the private sector. | This model requires a clear delineation of services offered freely and services offered for a fee (e.g., SOC services). | |
| **Public-Private Partnerships (PPPs)** | Can facilitate and accelerate knowledge transfer and skills development.<br><br>Can reduce the need for initial public funding.<br><br>Can enable the implementation of private sector good practices. | Can lead to conflicts of interests or confusion among stakeholders.<br><br>Can result in difficult situations if sensitive, national security information is involved.<br><br>Can result in partner lock-in or be subject to geopolitical constraints if the PPP involves a foreign company. | TTo be successful, PPPs for CSIRTs require well-designed articles of incorporation and / or Service Level Agreements (SLAs). Establishing trust between the retained company and the stakeholders is also key. | The national CSIRT of Togo (see Box 2). |

Source: World Bank

**The ability to secure funding to finance their service offering is also a key success factor for CSIRTs.** While international development assistance can, in some cases, finance the initial capex as well as the opex for the first two to three years of CSIRT operation, CSIRTs should build a solid financial model in parallel to support long-term development. For instance, the host organization could earmark a budget dedicated to the functioning of the CSIRT. Beyond central government budget and membership fees, innovative hybrid models provide some services for free and others for a fee. PPPs could reduce the financial burden for the public sector and facilitate knowledge transfer (see Box 2).

### Box 2. Establishing the national CSIRT as a PPP – the case of Togo

Located on the west coast of Africa, Togo is a small, low-income country of approximately 8.7 million people. In 2021, the government of **Togo** established the national CSIRT as a PPP. The nCSIRT is operated by Cyber Defense Africa (CDA), a joint venture between the Togolese government and a Polish IT company, Asseco. It enabled Togo to jumpstart its incident response function by:

- **Reducing initial investment costs:** the capex for establishing the Togolese CSIRT required a much lower public investment, as CDA invested in the joint venture together with the government.
- **Adopting an innovative financial model:** the opex of the Togolese CSIRT is also financed by the joint venture, as CDA provides CSIRT services to Togolese organizations for free, but also offers SOC services (e.g., incident detection tools) to organizations in the region for a fee. This model has enabled the government of Togo to significantly reduce the public investments needed for opex as well.
- **Facilitating access to cutting-edge skills and technology:** access to skills was a key obstacle for establishing the national CSIRT, as the Togolese workforce had very few cybersecurity professionals experienced in the operation and management of a CSIRT. The partnership with Asseco enabled CDA to accelerate cybersecurity skills development through knowledge transfer – experts from Asseco headquarters provided a robust training program to the staff of CDA (the technical team being composed almost exclusively of Togolese nationals).

In a few months, the expertise of the staff grew significantly, which enabled the Togolese CSIRT to join FIRST. Togo hence became the first - and so far, the only - low-income country in Western and Central Africa represented by an incident response team in FIRST.

Source: World Bank, cert.tg.

# 3. How much does a CSIRT cost?

**CSIRTs typically incur two types of costs: capex and opex.** The capex includes the initial investments needed to establish the CSIRT such as pre-assessment, acquisition of software and hardware (e.g., servers, switches, firewalls, laptops, printer, backups, etc.), recruitment of consultants to train and upskill the staff, and financing of fixed assets such as the purchase of an office. Opex covers the day-to-day expenses of the CSIRT such as staff salary, software licences, trainings, membership fees, office maintenance, communications, and events.

**Figure 6 provides rough estimates for the establishment of a national CSIRT at three different levels of service offerings.** However, the actual costs of establishing and operating a CSIRT are heavily context-dependent, and are impacted by the country's income level in particular (e.g., the staff salary levels and costs of renting an office will vary significantly between a high-income country and a low-income one) and size (operating a national CSIRT in a small island developing state is likely to be less costly than operating a national CSIRT in a larger country with more than 50 million inhabitants). The cost ranges outlined below are reflective of a very lean operating model and can easily go higher depending on the design, context, and functions of the CSIRT.

**Figure 6. Illustrative structures and estimated costs for national CSIRTs at different maturity levels**

| | Minimal service offering[7] | Average service offering | Key factors |
|---|---|---|---|
| **Staff** | 5-6 | 12-20 | 30-50 |
| **Structure** | • 1 x Manager<br>• 2-3 x Incident Handlers<br>• 1-2 x Multifunctional Roles (Communications; IT support; Project Management, Policy Analysis) | • 1 x Manager<br>• 1 x Deputy Manager<br>• 8 x Incident Handlers<br>• 1-3 x Analysts<br>• 1-3 x IT support<br>• 1-3 x Communications & Liaison | • 1 x Director<br>• 1 x Deputy Director<br>• 3-4 x Unit Managers<br>• 12-14 x Incident Handlers<br>• 3-6 x Analysts<br>• 3-6 x IT support<br>• 3-6 x Communications & Liaison<br>• 3-6 x Admin & Support |
| **Initial investments (capex)** | $500,000 – 700,000 + | $700,000 – 1.5 million + | $1.5 - 3 million + |
| **Annual operating costs (opex)** | Up to $500,000 | $500,000 – 1 million + | $1 - 2 million + |

Source: World Bank

**Trainings and participation in international incident response networks are essential to the successful development of CSIRTs.** CSIRT financial plans should therefore earmark budget[8] for such activities, typically by sending at least two staff members to participate in these events. To limit travel costs, trainings for larger teams can be done on-site, by bringing in specialized trainers within the country to provide one- or two-week training sessions.

7 See Figure 4 for a mapping of the different services that CSIRTs can provide.
8 While membership fees for international incident response networks are relatively low (usually below $5,000), travel costs, such as plane tickets and hotels, also need to be factored in.

**In lower-income contexts, a common pitfall is to focus solely on capex,** while neglecting the need to finance opex, particularly once the initial funding from international development assistance ends. It is therefore essential for CSIRTs to adopt a clear operating model at inception, with defined constituencies, service offering, governance structure, and long-term financial planning. If the design phase of a CSIRT does not include reasonable financial projections, particularly in terms of funding and opex, it can lead to negative outcomes. For instance, a CSIRT in a low-income context might be unable to perform key functions a few years after its establishment if it was "oversized" at inception. The following recommendations can help to keep overall CSIRT opex relatively low:

- **Systematically assess the necessity of expenses and consider alternative solutions.** This would include dropping expenses that are not directly contributing to the key service offering of the CSIRT and considering less expensive products or services.
- **Adapt the service offering to the budgetary constraints.** For instance, 24/7 shift work can become very expensive, as six teams are required to cover the 8-hour shifts, including holidays. CSIRTs could instead decide to operate only during business hours. Alternative options are to have an out of hours duty officer on call; or outsourcing to another 24/7 operations center for the initial triage of reported incidents at night and over the weekend. (ENISA, 2020, p. 17).
- **Maximize the use of cloud services,** such as Infrastructure as a service (Iaas) or Software as a service (Saas), to "outsource" part of the IT investments and maintenance costs (ENISA, 2020, p. 18).
- **Take advantage of existing open source tools,** particularly for specialized software (e.g., ticket management tool, intelligence sharing platforms, etc.) (OAS, 2023, pp. 39, 42).
- **Leverage existing resources,** particularly at the regional or national level (for instance, a newly established nCSIRT can seek cooperation and peer learning from neighboring countries, while a newly established sectoral CSIRT can rely on the nCSIRT for some key functions).

# 4. Establishing and enhancing CSIRTs

Many guides and resources are available to assist with the establishment and enhancement of CSIRTs. Several are listed in section 6.

**The CSIRT establishment process rarely starts from a blank slate, even in lower-income countries.** There are often relevant existing capabilities in place, even though their maturity and standardization may be limited. In the Republic of Congo, for instance, while there is no operational CSIRT, an online platform[9] with similar features was put in place in an IT academic institution associated with the defense ministry.

**Assessing existing capabilities is therefore a key first step in the process of establishing an operational CSIRT.** SIM3 (see Box 1) is a recognized best-practice to perform such assessment, usually requiring a few months to complete. Online self-assessments based on SIM3 are also available.[10] Once the initial assessment is complete, the CSIRT design, implementation, and operation phases can be launched in sequence. Figure 7 provides an example of the five-step process to establish, operate, and improve a CSIRT.

**Figure 7. Process for establishing, operating, and improving a CSIRT**


Source: (ENISA, 2020, p. 14)

**World Bank-financed projects often utilize a "design - build - transfer" model when financing new CSIRTs in developing countries.** The design and build phases involve the recruitment of international experts to support the early stages of the CSIRT, including developing a CSIRT implementation plan, providing training to local CSIRT staff to build capacity, and transferring all operational functions to the upskilled staff once they reach a sufficient level of expertise. Organizations such as ITU and FIRST also offer trainings for CSIRT staff and CSIRT managers.[11]

9 See http://pssn.cg/declaration
10 See https://sim3-check.opencsirt.org/
11 For instance, see https://academy.itu.int/training-courses/

**Measuring progress is key to building an effective incident response function** – e.g., by regularly identifying gaps and adjusting plans accordingly. If a CSIRT maturity framework was used in the assessment phase, as recommended above, then a re-evaluation against it will allow progress to be objectively measured and tracked. The World Bank typically includes quantitative data in the frameworks used to measure success for CSIRT development (see Box 3).

### Box 3. Measuring success for CSIRTs

A key aspect of establishing and enhancing CSIRTs is selecting metrics to measure success at various stages of the implementation process. The following data are usually collected and used for this purpose:

- Event and incident management:
  - Number of incidents detected.
  - Number of successfully handled incidents (by type, source, automation, etc.).
- Vulnerability management:
  - Number of vulnerability scans performed (or supported).
  - Number of critical vulnerability cases handled.
- Situational awareness:
  - Number of Cyber Threat Intelligence (CTI) artifacts documented and available for analysis and sharing.
  - Number of CTI sources matching constituent assets for incident registration.
  - Number of resources shared for situational awareness (reports, alerts, etc.).
- International cooperation and knowledge transfer:
  - Number of active memberships in international and regional CSIRT networks.
  - Number of constituents actively engaged.
  - Number of trainings and awareness-raising events delivered.

Source: NRD, World Bank.

**Many "low-hanging fruits" are available for newly established CSIRTs and can help them effectively jumpstart their organization.** Peer learning and study tours have proved particularly useful for CSIRTs, especially within a specific region where challenges and opportunities are often similar across countries. Recognizing that teams from lower-income contexts face specific challenges, the CSIRT community has designed programs dedicated to helping teams from underserved regions. For instance, in 2023, the Suguru Yamaguchi fellowship helped more than 20 teams participate in FIRST events across regions (e.g., Tonga, Vietnam, Gambia, Cameroon, Uzbekistan, and Albania). Overall, securing "quick wins" is essential to put new CSIRTs on the right development track (see Figure 8).

**Figure 8. Quick wins "cheat sheet" for newly established CSIRTs**

| Strategic level | Technical level |
|---|---|
| • **Use freely available resources** developed by the community of practitioners.<br>• **Reach out to constituents** to build trust and strengthen the CSIRT value proposition.<br>• **Manage relationships with key stakeholders** (e.g., Ministry) to secure funding and high-level support.<br>• **Earmark budget for staff training** and participation in international networks.<br>• **Apply to CSIRT fellowships such as the Suguru Yamaguchi Program in FIRST.** | • **Subscribe to community-driven cybersecurity feeds** (e.g., Shadowserver Foundation and PhishTank).<br>• **Organize or participate in regular events with constituents and key stakeholders** to build the "CSIRT brand."<br>• **Invest in peer learning from other CSIRTs in the region**, including site visits and joint drills, to forge strong relationships with at least two peer CSIRTs.<br>• **Register with FIRST and regional incident response networks,** and participate in at least two meetings every year. |

Source: World Bank.[12]

12 See, for instance, resources shared by FIRST and the Open CSIRT Foundation.

# 5. Conclusion

**CSIRTs are key to the foundation of the cybersecurity ecosystem in developing countries.** There is a strong correlation between a country's robust incident response function and its overall cybersecurity capacity. In Western and Central Africa, for instance, the four countries whose ITU GCI score[13] is above the global median are also the four[14] countries that registered an incident response team with FIRST: Ghana, Nigeria, Ivory Coast, and Benin. This finding indicates that the robustness of the national incident response ecosystem is at least indicative of a stronger cybersecurity capacity, if not outright conducive to it.

**The establishment and enhancement of a strong incident response function should therefore be further prioritized in developing countries.** In low-income countries, investments can focus on building and strengthening the national CSIRT, whose existence or effective operationalization is often lacking. NCSIRTs are an essential building block of a country's cybersecurity ecosystem – when major cybersecurity incidents occur, nCSIRTs serve as a single point of contact for the international community. In middle-income countries, the development of a robust incident response ecosystem can be prioritized, including the establishment of sectoral CSIRTs for critical infrastructures such as energy, healthcare, and transport.

**Compared with the estimated costs of cybersecurity incidents (up to 3 percent of GDP), the initial investment to setup a CSIRT stands out as financially sound, with potential to yield remarkable economic returns overall.** However, stakeholders should also ensure the financial sustainability of CSIRTs after the initial funding ends – operational expenditures, such as salaries, trainings, and participation in international networks are of the utmost importance for CSIRT development.

**Cooperation with international partners and communities of practitioners can help accelerate capacity building in lower-income contexts.** Many free resources are now available to incident response practitioners, thanks to the dedication of a community of practice within organizations such as FIRST, the Shadowserver Foundation, and the Open CSIRT Foundation.

**Finally, regional cooperation is increasingly recognized as a key driver for the development of the incident response function in lower-income contexts.** Regional cooperation can lower overall costs for the operation of CSIRTs by mutualizing certain key functions, facilitating information sharing, and accelerating skills development through peer learning and joint exercises. Such regional cooperation can take different forms, for instance, through the establishment of a regional CSIRT or ISAC that can serve as an information sharing platform for national CSIRTs in the region. Another common form of regional cooperation is the establishment of regional networks of CSIRTs through the organization of regular trainings and drills dedicated to national CSIRTs of the region.

13 ITU's GCI is a composite index measuring countries' commitment to cybersecurity. The latest GCI was published in 2021.
14 Togo being an exception, as its nCSIRT was established in 2021, i.e., after data collection for ITU GCI was complete.

# 6. Practitioner resources

| Publication date | Resource | Organization / Authors |
|---|---|---|
| 2023 | A Practical Guide for CSIRTs (vol 2) A sustainable business model | **OAS** |
| 2022 | 11 Strategies of a World-Class Cybersecurity Operations Center | **MITRE** |
| 2022 | Cyber Incident Management in Low-Income Countries - Part 1<br>Cyber Incident Management in Low-Income Countries - Part 2 | **AfricaCERT and GFCE** |
| 2021 | Getting Started With A National CSIRT | **TNO and GFCE** |
| 2021 | Commonwealth nCSIRT Capacity Building Programme Self-help Guide | **UK Foreign Commonwealth and Development Office** |
| 2020 | How to set up CSIRT and SOC | **ENISA** |
| 2019 | CSIRT Service Framework | **FIRST** |
| 2017 | GFCE Global Good Practices National Computer Security Incident Response Teams (CSIRTs) | **TNO and GFCE** |
| 2016 | Best practices for establishing a national CSIRT | **OAS** |
| 1998 | RFC2350 | **Internet Engineering Task Force (IETF)** |

# References


Denning. (1989). Retrieved from https://www.jstor.org/stable/27855650

FIRST. (n.d.). CSIRT service framework. Retrieved from https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

FIRST. (May 2024). Retrieved from https://www.first.org/members/map

ITU. (2021). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

World Bank. (2023). Retrieved from https://projects.worldbank.org/en/projects-operations/project-detail/P177077

World Bank. (2023). Ghana: A Case Study in Strengthening Cyber Resilience. Retrieved from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099111623162584046/p17785201f69be0150909902c3a7202107e

World Bank. (2024 (forthcoming)). The economics of cybersecurity.

Elis, N. (2015) 'Cyber Chief: 8% of ministry budgets should go to cyber security', The Jerusalem Post | JPost.com, 25 March. Available at: https://www.jpost.com/israel-news/new-tech/cyber-chief-8-percent-of-ministry-budgets-should-go-to-cyber-security-395101 (Accessed: 10 October 2023).

ENISA (2020) How to set up CSIRT and SOC, ENISA. Available at: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc (Accessed: 12 October 2023).

Mishra, A. (2017) 'MeitY Asks Ministries To Spend 10% Budget On Cyber Security', Inc42 Media, 2 September. Available at: https://inc42.com/buzz/meity-cyber-security/ (Accessed: 10 October 2023).

NIST (2021) Computer Security Incident Response Team (CSIRT) - Glossary | CSRC, NIST Computer Security Resource Center. Available at: https://csrc.nist.gov/glossary/term/computer_security_incident_response_team (Accessed: 10 October 2023).

NIST (2023) The NIST Cybersecurity Framework 2.0. NIST CSWP 29 ipd. Gaithersburg, MD: National Institute of Standards and Technology, p. NIST CSWP 29 ipd. Available at: https://doi.org/10.6028/NIST.CSWP.29.ipd.

Organization of American States (OAS) (2023) A Practical Guide for CSIRTs (vol 2) A sustainable business model. Organization of American States. Available at: https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/Guia-CSIRT%202023%20Digital%20ENG.pdf (Accessed: 19 September 2023).