KM 4: Cyber Incident Management

Content

Module objectives

Welcome to the knowledge module on **Cyber Incident Management** as part of the GFCE-Africa project.

The participants of this knowledge module will gain knowledge on policy and technical considerations for cybersecurity incident management through sharing of best practice, case studies, exercises, and reflection.

Upon finishing the module, you will be able to respond to, and find additional resources for the following focus areas:

- Types of cyber incident management teams,
- Establishment of a Computer Security Incident Response Team (CSIRT),
- Services that CSIRTs offer,
- Tools and skills required to run a CSIRT
- Regional and international CSIRT networks such as AfricaCERT, FIRST and OIC-CERT

1. Introduction

Africa has over 500 million internet users, which accounts for 38% of the continent's population. An Increase in the uptake and dependency of information and communication technologies in economic sectors, public institutions and the society is expected, which will require countries to build effective national cybersecurity capacity to protect and defend their citizens, information, and the infrastructure.

With persistent virtual realities accelerated by the COVID-19 pandemic, it is imperative that African countries build capacity and effectiveness in cybersecurity incident management.

> *Cybercriminals are developing and boosting their attacks at an alarming pace, exploiting the fear and uncertainty caused by the unstable social and economic situation created by COVID-19*."
>
> Jürgen Stock, INTERPOL Secretary General
> Source: African Cyberthreat Assessment Report, October 2021

Cybersecurity has been identified as one of the main Agenda 2063 flagship projects in energy and infrastructure development. The cybersecurity project is guided by the African Union Convention on Cyber Security and Personal Data Protection. The Convention's Chapter 3 provides for the promotion of cybersecurity through measures taken at a nation level. These measures include a national cybersecurity policy and strategy, legislative and regulatory measures, as well as national cybersecurity monitoring structures through the establishment of appropriate institutions such as Computer Emergency Response Team (CERT) or the Computer Security Incident Response Teams (CSIRTs).

2. Types of Cyber Incident Response Teams

With the significant increase in computer security incidents which have social, economic and political implications, most African countries are considering various mechanisms to minimise and mitigate the impact of incidents including the setting up or improvement of the coordination teams responsible for incident handling and response.

Case studies: *Cybersecurity Incidents in Africa during the COVID-19 Pandemic*

Interpol's African Cyberthreat Assessment Report, October 2021, identified that the most prominent threats in the region were online scams, digital extortion, business email compromise (BEC), ransomware, and botnets.

Experts in Kenya maintained that COVID-19 has triggered 'an epidemic of cybercrimes,' with a 37.3 per cent increase in cyberattacks in the period between April and June 2021, compared to January and March 2021.
The cyberattacks, including phishing, malware distribution, and attacks associated with remote working vulnerabilities have seen a substantial increase, as reported in the Africa Cybersecurity Report - Kenya, 2019/2020. These include remote access, risks associated with reduced monitoring, and exploitation of new teleworking infrastructure.

There are various types of teams that monitor, warn, coordinate response and recovery efforts, and facilitate collaboration between government entities, individual organisations, manufacturers, service and utility sectors, the academia and the international community on cybersecurity issues.

These teams are referred to by acronyms that include Computer Emergency Response Team (CERT), Computer Security Incident Response Team (CSIRT), Incident Response Team (IRT), Computer Incident Response Team (CIRT), Security Emergency Response Team (SERT), Security Operations Centre (SOC), National Computer Security Center (NCSC), Information Sharing and Analysis Center (ISAC) and more recently Cyber Defence Centres (CDC).

Subject to the mandate and the type of constituency, African stakeholders may use any of these terms to refer to the team managing cybersecurity incident management. National CSIRTs, for example, are often named using the CSIRT/CIRT/CERT abbreviation - CERT-MU, EG-CERT. Teams servicing a sector include a shortened form of the sector and the two-letter country code for example, EG-FinCIRT. The name of the company or organisation or a shortened version would be included if the team provides services to the company, for example Siemens CSIRT.

The term CSIRT is normally used to refer to a CIRT, CERT or SIRT. An organisation using this term must provide an incident handling (response) service. A SOC is used to refer to a team that monitors the operations for the security of networks and data centres. It is important to note that the CERT is a worldwide registered trademark of the CERT Coordination Center (CERT/CC), which falls under the Software Engineering Institute (SEI) of Carnegie Mellon University (CMU) in the USA. Organisations who wish to use "CERT" in their team name must contact SEI-CMU to request permission (this policy may be amended in the future).

Resources: *Definitions*

Request for Comments (RFC) 2350 defines a CSIRT as a team that coordinates and supports the response to security incidents that involve sites within a defined constituency. In order to be considered a CSIRT, a team must provide a (secure) channel for receiving reports about suspected incidents.

The Forum for Incident Response Teams (FIRST) definition for a Computer Security Incident Response Team (CSIRT) is an organisational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents, in accordance with its mission”. A specific set of individuals and/or organisations with common characteristics that a CSIRT provides services to is known as a constituency.

The International Telecommunications Union ITU-T Recommendation X.1060 defines cyber defence centre (CDC) as an entity within an organisation that offers security services to manage the cybersecurity risks of its business activities.

The SEI-CMU defines a Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Services are offered for defined constituency.

FIRST defines an Information Sharing and Analysis Center (ISAC) as a cooperation platform for security teams in the same sector or with a shared goal, which can offer many of the services a CSIRT can offer, but does not do incident handling.

A Security Operations Center (SOC) provides centralised real-time monitoring of an organisation's networks and systems, coordinated incident response and handling.

2.1. National Computer Security Incident Response Team

African countries can enhance cybersecurity capacities through various means including the establishment of national CSIRTs (Computer Security Incident Response Teams), which is a key element in the implementation of national cybersecurity strategies. With the operationalisation of a national CSIRT, a country can enhance its cybersecurity capacities including real-time monitoring, issuance of early warnings, incident response, quick recovery, and mitigation of consequences.

The GFCE Global Good Practices identifies specific characteristics and capabilities for N-CSIRTs;

- national scope and government recognition,
- being integral to the national crisis management structure,
- cooperating and collaborating with multistakeholders on countering cyber threats and incidents, nationally, bilaterally, and internationally, and
- collaborating with other national and/or regional CSIRTs, governmental CSIRT(s), product security teams of manufacturers/vendors (PSIRTs), and leading international communities to advance CSIRT governance, legal frameworks, and capacities

An N-CSIRT should at a minimum provide cyber-related incident management, outreach to and communication with its constituency and situational awareness services.

According to the International Telecommunications Union (ITU), as of March 2019, there were 118 National CSIRTs as shown in Figure 1 below.

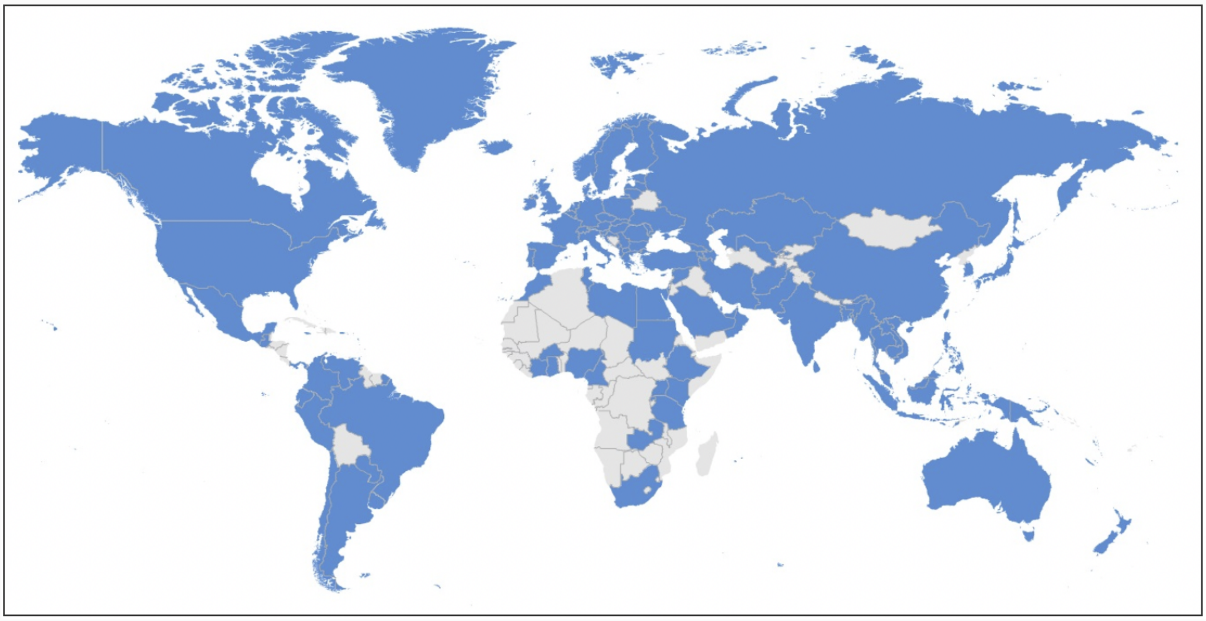


***Figure 1**: National CSIRTs Worldwide* Source: ITU

2.2. Product Security Incident Response Team

As more African countries engage in the manufacture and innovation, consideration should be given to security in the design, planning, development, testing and maintenance of products, solutions and services

According to FIRST, a Product Security Incident Response Team (PSIRT) is “an entity within an organization which, at its core, focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components, and/or services which an organization produces and/or sells.” The FIRST PSIRT Services Framework, provides guidance on the profile and capabilities of a team, created to manage vulnerabilities identified in products and offerings.

Examples of a PSIRT include Siemens ProductCERT, which is part of Siemens cyber incident handling and vulnerability handling (IHVH) portfolio and Kaspersky’s Product Security Team (PST). The Microsoft Security Development Lifecycle (SDL) consists of a set of practises that support security assurance and compliance, including the establishment of a standard incident response process.

Resource: ***Presentation***: Product CSIRTSs (PSIRTs) Special Interest Group (SIG)

The presentation made at the FIRST & AfricaCERT Virtual Symposium for Africa and Arab Regions December 7-9, 2021 By PSIRT SIG Co-Chairs Pete Allor, Red Hat and Josh Dembling, Intel covers the following areas:

- PSIRT training videos and maturity guide 2018

- PSIRT Services Framework V.1.1.2019
- PSIRT Services Framework V.1.X. (Q2 2022)
- Determining mission, Goals and Deliverables

2.3. Sector CSIRTs

According to the Carnegie Mellon University SEI: CSIRT Sector Framework, ''Sector CSIRTs are responsible for facilitating incident response and management for a particular sector or subset of a country or economy (e.g. financial, energy, or government)

Also referred to as sectoral CSIRTs, sector-based Cybersecurity Centers, Sector CERTs or Information Sharing and Analysis Centers (ISACs), they are uniquely adapted, specialised incident response teams..that have the advantage of bridging the gap between public and private sectors, and providing a mechanism or platform for cooperation, information sharing, and trust building''.

Case Studies: Sector CSIRTs in Africa

Tunisia: The Financial CERT offers security services to the Tunisian financial sector. These services include: monitoring, incident management, threat intelligence, and sensitisation. The Financial CERT is a member of FIRST.

Egypt: EG-FinCIRT set up by the Central Bank of Egypt inline with the bank's strategy to move towards a less-cash economy, support fintech applications and financial inclusion. According to the Central Bank of Egypt, Economic Review Vol. 60 No. 4 2019/2020, EG-FinCIRT provides incident response, proactive monitoring, and analysis of information security incidents to the financial sector with significant human capital investment made to support these functions.

Ghana: The NCA-CERT was established by the National Communications Authority, the regulator for the communications industry, to respond to incidents within the communications Sector.

The primary constituency of NCA-CERT are licensed operators within the communications sector and their subscribers. It provides a platform for information sharing and coordinates incidents within the communications sector

The CERT works with its constituents to infuse cyber security best practises into its regulatory and licensing regimes, while providing services including Incident Management, Analysis, Information Assurance, Situational Awareness, Communications and Outreach, Capability Development, Research and Development.

2.4. Security Operation Centre

There is no set definition of what a Security Operation Centre (SOC) is. A SOC or internal CSIRT monitors, protects, defends, or basically manages cybersecurity risks to an organisation's business activities. A SOC typically provides routine services including analysis of incident detection, and monitoring and maintenance of security response systems. The centre is managed by a chief security officer (CSO) or a chief information security officer (CISO).

In building a SOC, an organisation should start small and slowly build in a controlled manner to create a fully fledged SOC. At the beginning, the emphasis should be on gaining experience in monitoring log data from a select number of infrastructure or middleware components, registering incidents using the right tools, generating periodic reports and recording lessons learned. Staff should participate in relevant meetings within the organisation. An information security policy that has been approved by the management is essential for the operation of a SOC.

Compliance or certification to ISO/IEC 27001 standard demonstrates the quality and effectiveness of the organisation's information security policies, procedures and controls. This standard can be used to support the functioning of the SOC.

2.5. Commercial CSIRT

A commercial CSIRT offers managed security services to paying customers or organisations. These organisations, in most cases, have limited resources in terms of funding and skilled personnel (expertise) to provide the full range of services required for a CSIRT or an SOC.

To create consumer confidence in the services that a commercial CSIRTs provides, it is recommended that these entities are regulated and certified based on international standards.

Resource:

The French Network and Information Security Agency, Agence nationale de la sécurité des systèmes d'information (ANSSI), recognised that it could not by itself support operators of critical infrastructure and, therefore, the established evaluation process allowing it to qualify private cybersecurity "Trust Service Providers'' and products in the fields of:

- cybersecurity audit service providers (PASSI)
- incident detection service providers (PDIS)
- integration response services providers (PRIS)
- integration/architecture service providers (planned)

***Case Studies**: The space for Commercial CSIRTS or Managed Security Service*

Serianu's Cyber Incident Response Team (CIRT) provides incident response and investigation, Remediation and technology support, managed threat detection and monitoring, security assessment and assurance, cyber risk quantification, training and awareness for African organisations. Serianu has a presence in Kenya, Uganda, Tanzania, Ethiopia, Nigeria, Ghana, Botswana and Lesotho

CSIRT.TN

3. What needs to be considered when establishing a National CSIRT?

There are various guides and best practises that African countries could reference in the foundation and the establishment of a CSIRT. These frameworks recommend the use of a phased approach for the establishment of a National CSIRT include the:

- ITU Cybersecurity Programme: CIRT Framework
- ITU-T Recommendation X.1060: Framework for the creation and operation of a cyber defence centre
- European Union Agency for Cybersecurity (ENISA): How to set up a CSIRT and SOC
- GFCE Global Good Practice: National Computer Security Incident Response Teams (CSIRTs)
- GFCE Cyber Incident Management in Low-Income Countries - Part 1- A Holistic View on CSIRT Development and Part 2- A Guideline for Development

3.1. CIRT framework

ITU has employed the CIRT Framework to African countries including Botswana, Burundi, Gambia, Ghana, Kenya, Malawi, Tanzania, Uganda, and Zambia in setting up national teams. This framework consists of four (4) phases: assessment, design, establishment and enhancement.

Phase 1: Assessment This phase involves evaluation of the country's cybersecurity posture through onsite assessment and stakeholder engagement in a series of workshops to clarify the value and justification of establishing a CSIRT and obtaining support for resourcing and financing mechanisms. The outcome of this phase is an assessment report, prepared by ITU experts, that contains key issues, findings and analyses, recommendations, and a phased implementation plan for setting up the national CIRT.

Phase 2: Design The outcome of this phase is detailed Design Document and involves a review of the mandate and positioning of the CSIRT, the definition of services model according to the FIRST CSIRT Services Framework, list of workflows, policies and procedures, a processes map, constituency engagement plan and communication strategy, networks design, list of hardware and software equipment and tools, selection of premises and personnel.

Phase 3: Establishment This phase involves capabilities (process, policies, procedures, technology and human resource) development, capabilities deployment and testing, customization, fine-tuning and training, operations, handover and closure. The outcomes of this phase reports, documentation and operational acceptance of the CIRT by the beneficiary country.

Phase 4: Enhancement This phase establishes new services (situation awareness and digital forensics) based on the FIRST CSIRT Services Framework (see section 5.2), custom-built services and better automation of existing services.

3.2. How to set up CSIRT and SOC

ENISA provides guidelines for setting up CSIRT and SOC that are organised in five (5) phases: assessment for readiness, design, implementation, operations and improvement.

Phase 1: Assessment for readiness – At this phase, the preliminary mandate of authority, the governance structure defining the responsibilities of stakeholders of a national CSIRT and the identification of the CSIRT hosting organization is determined. These elements are usually expressed through a law, a cybersecurity strategy, or a cybersecurity plan.

Good Practice: Well thought of organisational positioning

The national CSIRT should be positioned to take advantage of the nation's organisational structure, i.e. established in law, connected to the national crisis management structure, and available as an international point of contact for cybersecurity incidents.

This phase includes the consideration and approval of a high-level roadmap and budget that includes the expected timeline for the CSIRT establishment phases and the detailed requirements for the design stage

Good Practises: Establish the right mandate and ensure top-down embedding:

According to the GFCE Global Good Practice - National Computer Security Incident Response Teams (CSIRTs), the effectiveness of a CSIRT is determined by a mandate laid down in the national cybersecurity strategy, regulation, or law.

The national strategy should define the CSIRT's mandate, mission, authority and responsibilities towards its constituency, stakeholders, and governance model. It is critical that there is a legal obligation to report cybersecurity incidents.

To ensure top-down embedding, a national CSIRT should have political and governmental endorsement with well established governance and accountability structures, as well as connection to the national crisis management structure. The CSIRT's connection to regional and international CSIRTs supports the mandatory coordination mechanisms between neighbouring countries as required by international protocols including the African Union Convention on Cybersecurity and Personal Data Protection.

Phase 2: Design The recommendations of this phase are aligned with Security Incident Management Maturity Model (SIM3) in the organisation, human, tools and processes areas referenced in the model. The outcome of this phase included the approved detailed mandate, and plans covering the CSIRT services, processes, workflows organisation, skills and training structure, facilities, technologies and processes automation, cooperation, IT and information security management and detailed requirements for the implementation stage. It is good practice to publish the resulting design structure in the format provided in Request for Comments (RFC) 2350: Expectations for Computer Security Incident Response.

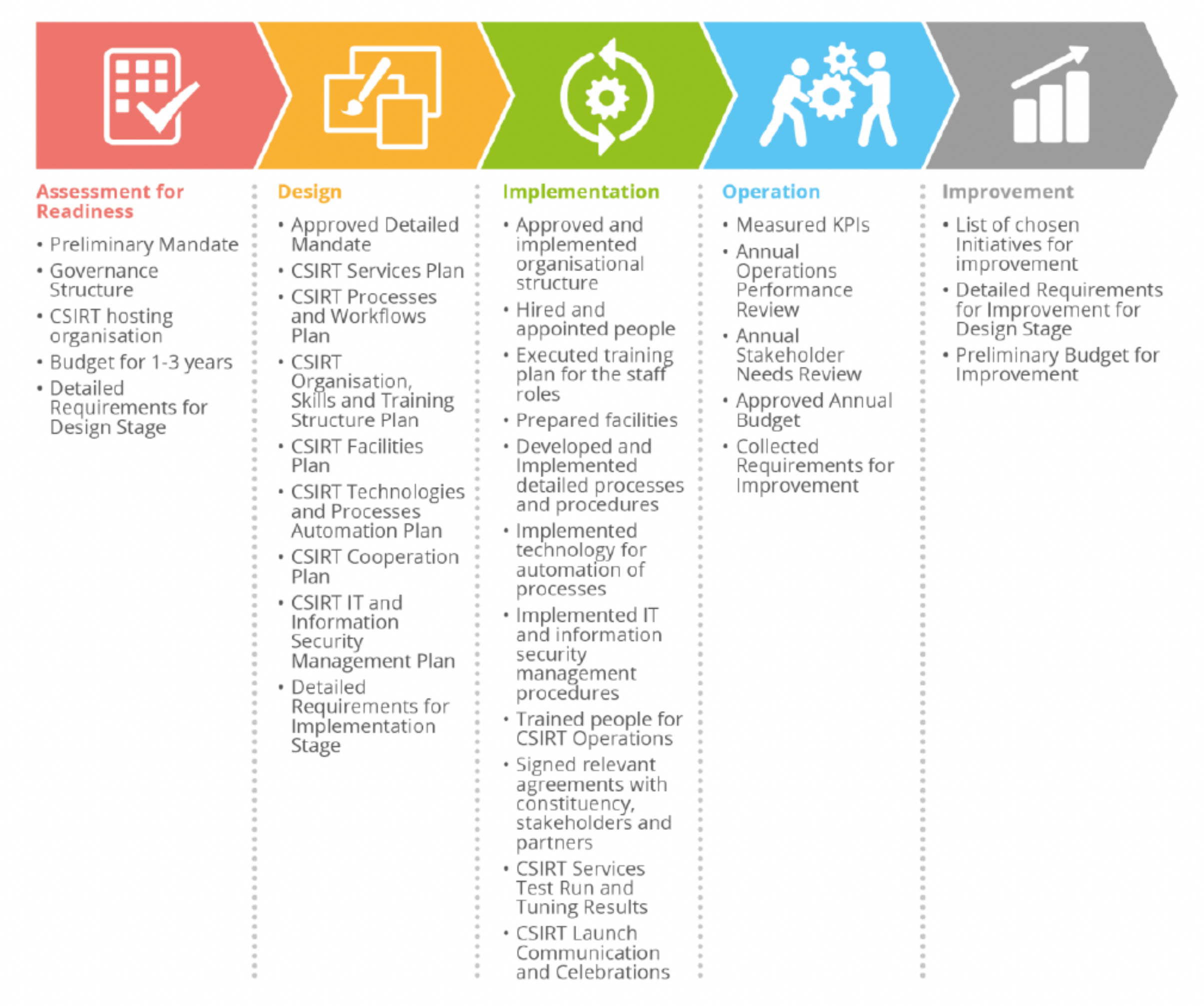
Phase 3: Implementation The outcomes of this phase include an approved and implemented organizational structure, hiring and training of staff, implementation of process and procedures, signed agreements with the constituency, stakeholders and partners and the CSIRT launch communication and celebrations. It is expected that at end of the implementation phase, the CSIRT is ready to deliver services to its constituency and start the operations phase.

Phase 4: Operation– At this phase, a CSIRT delivers the CSIRT services in accordance with its mandate on a daily basis. The outcomes of this phase are measured Key Performance Indicators (KPIs) for management and governance purposes and quality monitoring, annual operations performance review, annual stakeholder needs review, approval annual budget and collection of requirements for improvement.

Good Practice: Annual CSIRT stakeholder workshop or meeting

An annual workshop or meeting with CSIRT stakeholders where the performance of the CSIRT and stakeholders' priorities for and expectations of the CSIRT are presented is identified as a good practice.

Phase 5: Improvement – The outcomes of this phase include a list of improvement initiatives, the associated requirements and preliminary budget. The improvement initiatives may arise from the operations phase; a high-level roadmap; from stakeholders; or from the management's demand to improve the maturity and capability of the CSIRT based on frameworks such as the Security Incident Management Maturity Model (SIM3) and the Security Operation Centre Capability and Maturity Model (SOC-CMM).



Assessment for Readiness

- Preliminary Mandate
- Governance Structure
- CSIRT hosting organisation
- Budget for 1-3 years
- Detailed Requirements for Design Stage

Design

- Approved Detailed Mandate
- CSIRT Services Plan
- CSIRT Processes and Workflows Plan
- CSIRT Organisation, Skills and Training Structure Plan
- CSIRT Facilities Plan
- CSIRT Technologies and Processes Automation Plan
- CSIRT Cooperation Plan
- CSIRT IT and Information Security Management Plan
- Detailed Requirements for Implementation Stage

Implementation

- Approved and implemented organisational structure
- Hired and appointed people
- Executed training plan for the staff roles
- Prepared facilities
- Developed and Implemented detailed processes and procedures
- Implemented technology for automation of processes
- Implemented IT and information security management procedures
- Trained people for CSIRT Operations
- Signed relevant agreements with constituency, stakeholders and partners
- CSIRT Services Test Run and Tuning Results
- CSIRT Launch Communication and Celebrations

Operation

- Measured KPIs
- Annual Operations Performance Review
- Annual Stakeholder Needs Review
- Approved Annual Budget
- Collected Requirements for Improvement

Improvement

- List of chosen Initiatives for improvement
- Detailed Requirements for Improvement for Design Stage
- Preliminary Budget for Improvement

Figure 2: *Summary of CSIRT establishment outcomes Source:*ENISA

There are training designed for managers and project leaders who have been tasked with implementing a computer security incident response team (CSIRT) i s available. This includes the CMU-SEI Creating a Computer Security Incident Response Team and the Managing Computer Security Incident Response Teams support managers in improving the effectiveness of the team.

***Case study**: Establishing a CSIRT in Togo*

Input from ACE Community - Video Interview with: CERT Togo's Palakiyem Assih

CERT.tg is operated by Cyber Defense Africa S.A.S. (CDA), as a service delegated by the National Cybersecurity Agency (ANCy).

Resource: *Establishing CSIRTs*

Establishing A CSIRT: This handbook describes the process and requirements for establishing a CSIRT, along with the relevant examples.

Handbook for Computer Security Incident Response Teams (CSIRTs) provides a description of different organisational models for implementing incident handling capabilities.

4. How to assess cyber incident maturity

Identification of needs/gaps in various aspects of cybersecurity capability of a country or a team can be determined utilising various tools and maturity models.

These include the Security Incident Management Maturity Model (SIM3), the Security Operation Centre Capability and Maturity Model (SOC-CMM), and the CSIRT Maturity - Self-assessment Tool.

Good Practice: Measuring and Improving Maturity

Using the SIM3, the CSIRTs carry out a self-assessment based on 44 maturity parameters in the fields of organisation, human aspects, tools, and processes. Emerging and existing CSIRTs can use the Maturity Kit to improve their maturity level. By defining a maturity growth path based on SIM3, a CSIRT improve their maturity level from basic'' maturity level, via intermediate'', to certifiable'' based on a combination of self-assessments and peer reviews.

4.1. Security Incident Management Maturity Model (SIM3)

Security Incident Management Maturity Model (SIM3) supports the measurement of maturity of an incident response or a security team based on four areas: organisation, human issues, tools, and processes. SIM3 is freely available from the not-for-profit Open CSIRT Foundation (OCF). The model is used for self-assessment of teams and supports the TI Certification scheme under the TF-CSIRT and is considered by FIRST for membership.

4.2. Security Operation Centre Capability and Maturity Model (SOC-CMM)

The Security Operation Centre Capability and Maturity Model (SOC-CMM) consists of 5 domains and 25 aspects. The domains include business, people, process, technology, and service.

4.3. CSIRT Maturity - Self-assessment Tool

CSIRT Maturity - Self-assessment Tool helps CSIRTs to self-assess their team's maturity in terms of 44 parameters of the SIM3 model in 4 broad areas: organisation, human, tools, and process.

Reflection point

Carry out a self-assessment of your country or a N-CSIRT using any one of the above tools or maturity models.

5. Which services do the CSIRTs offer?

The integral and minimum services a CSIRT should offer to its constituents are cyber-related incident management, outreach to and communication with its constituency, and cyber security risk awareness creation. However, entities in the CSIRT community can develop their own service lists reference to the FIRST CSIRT Services Framework or International Telecommunications Union Standardization Sector (ITU-T) Recommendation X.1060.

Good Practice: Decide on the set and scope of national CSIRT services

The GFCE Global Good Practice - National Computer Security Incident Response Teams (CSIRTs) identifies the determination of the services and service areas from the onset as a good practice.

Both the GFCE and the ITU recommend the use of the CSIRT Services Framework, which includes incident management, analysis, information assurance, situational awareness, outreach/communications, capability development, and Research & Development.

5.1. FIRST CSIRT services framework

The FIRST CSIRT Services Framework categorises CSIRT services into five service areas, each area having several services. Most CSIRTs offer incident response service. The CSIRT cases can be classified based on the category, criticality level, and sensitivity level. The five service areas are:

- Information Security Event Management (ISEM)
- Information Security Incident Management (ISIM)
- Vulnerability Management (VM)
- Situational Awareness (SA)
- Knowledge Transfer (KT)

5.1.1. Information Security Event Management (ISEM)

This service area identifies information security incidents based on the correlation and analysis of security events from a wide variety of event and contextual data sources''. ISEM service offerings include monitoring and detection, along with event analysis. Using automated, continuous processing tools, the CSIRT extracts data from a wide variety of information security event sources and contextual data, in order to identify potential information security incidents. Event analysis involves grouping and correlating events to qualify them as potential information security incidents for escalation to the Information Security Incident Management service area, or as a false alarm.

Based on the National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity, the CSIRT should have competencies in data management, infrastructure design, network management, and operating systems to deliver the monitoring and detection service. Skills required to deliver the event analysis service are incident management, data analysis, threat analysis, computer forensics, and cyber threat monitoring. Training and certification in those areas is provided by SANS, Udemy, EC-Council, IBM, AfricaCERT, ENISA, FIRST, CIRCL, CERT-Tools Community, ICANN, and CREST.

5.1.2. Information Security Incident Management (ISIM)

This is the main service that a CSIRT provides to its constituents. The team collects, evaluates, and analyses information security incident reports. The results of the analysis are used in recommendations given to constituents for the mitigation of, and the recovery from the incidents. This service requires the CSIRT coordinate with other CSIRTs, or security experts to ensure that all aspects of the incident are addressed and to help reduce similar future attacks.

Various frameworks and guidelines provide guidance on CSIRT services including the Computer Security Incident Handling Guide. This guide provides guidelines on the creation of an incident response policy and plan, developing procedures for performing incident handling and reporting, setting communication guidelines, selecting a team structure and staffing model, establishing relationships and lines of communication between both internal and external parties, and determining which services the incident response team should provide. Others include the Carnegie Mellon University Engineering Institute (CMU-SEI) Handbook for Computer Security Incident Response Teams (CSIRTs) and RFC-2350.

The core competencies required in the ISIM area include: computer forensics, data analysis, incident management, threat analysis, vulnerability assessment, information systems/network security, system testing, evaluation and administration, encryption and soft skills including critical thinking, written and oral communication, client relationship management, conflict and knowledge management. The team requires competencies in law, regulations, policies, and ethics.

Training identified for this service area includes, but is not limited, to those offered by SANS - Hacker Tools, Techniques, and Incident Handling, CMU-SEI- CERT Incident Response Process Professional Certificate, EC-Council - Certified Incident Handler Program, Udemy - Cyber Security Incident Handling and Response, Cyber Security Incident Response and Mile2- C)IHE Certified Incident Handling Engineer course.

5.1.3. Vulnerability Management (VM)

The Vulnerability Management Service Area includes services related to the discovery/research, analysis, and handling of new or reported security vulnerabilities including coordination, disclosure, and response. In this service area, CSIRTs offer services that establish a continuous process of identifying, analysing, disseminating, and remediating vulnerabilities in information systems.

Guidelines for the provision of this service are contained in ISO/IEC 29147:2018 Information Technology - Security Techniquest - Vulnerability disclosure, ISO/IEC 30111:2019 Information technology - Security techniques - Vulnerability handling, the FIRST Product Security Incident Response Team (PSIRT) Services Framework and the Dutch National Cybersecurity Center Coordinated Vulnerability Disclosure: the Guideline.

To offer this service, a team requires competencies in vulnerability assessment, threat analysis, computer languages, operating systems, web technology, network management, system administration, software testing and evaluation, data privacy and protection, encryption, information assurance, identity management, asset/inventory management, database administration including soft skills such as critical thinking, conflict management, oral and written communication, as well as knowledge and client relationship management.

Training and certification in this areas include, but are not limited to SANS, CREST, Offensive Security, EC-Council, CompTIA, MILE2, and Udemy.

Case Study: Log4shell or Log4j vulnerability

Log4shell is a critical vulnerability in the widely-used logging tool Log4j. The UK National Cybersecurity Centre published information on “Log4j vulnerability - what everyone needs to know " including tips of organisations which had been affected.

On 13 December 2021, the EU CSIRTs Network escalated to Alert Cooperation Mode’’ on the Log4j. The CSIRT’s Network Members exchanged information, contributed to updating the list of vulnerable software, published relevant advisories for the benefit of their constituencies, and met to discuss the results of two reporting surveys and national situations from 10 to 12 December 2021.

On 12 January 2022, based on the data collected, the national reporting, along with the absence of large-scale or cross-border incidents, the EU CSIRTs Network decided to move back to default cooperation mode, in relation to the log4j/log4shell vulnerability.

5.1.4. Situational Awareness (SA)

Situational Awareness comprises the ability to identify, process, comprehend, and communicate current state and anticipated potential changes in a CSIRT’s area of jurisdiction. This service requires the team to gather, integrate, and disseminate information to its constituents to enable them to make informed decisions. The information is made available for the delivery of other services including Security Event Management, Incident Management, and Knowledge Transfer.

The service offerings in this area include data acquisition, analysis and synthesis and communication. In order to deliver this service to its constituencies, the CSIRT requires competencies in asset/inventory management, enterprise architecture, systems integration, threat analysis, vulnerability assessment, data analysis and management, modelling and simulation, data and privacy protection, information assurance, identity management, encryption and soft skills in oral and written communication, knowledge and client relationship management, organisational and technology awareness.

5.1.5. Knowledge Transfer (KT)

Given the unique position of the CSIRT’s service, the team collects, analyses, identifies security threats, trends, and risks, and develops operational practises to assist its organisations in detecting, preventing and responding to incidents. The transfer of this knowledge through awareness building, training and education, exercises, technical and policy advisory services to the constituents, is crucial to improving overall cybersecurity.

The competencies required for this service are oral and written communication, interpersonal skills, knowledge management, presenting effectively, workforce management, strategic management, teaching others, client relationship management, business continuity, conflict and risk management.

Training in this area is available from CREST, MITRE, SANS- Security Strategic Planning, Policy, and Leadership, A Practical Introduction to Cyber Security Risk Management, NIST- links are for free and low-cost online educational content, ESET, NINJIO - Cybersecurity Awareness Training, KnowBe4 - Security Awareness, and CybSafe - security awareness training

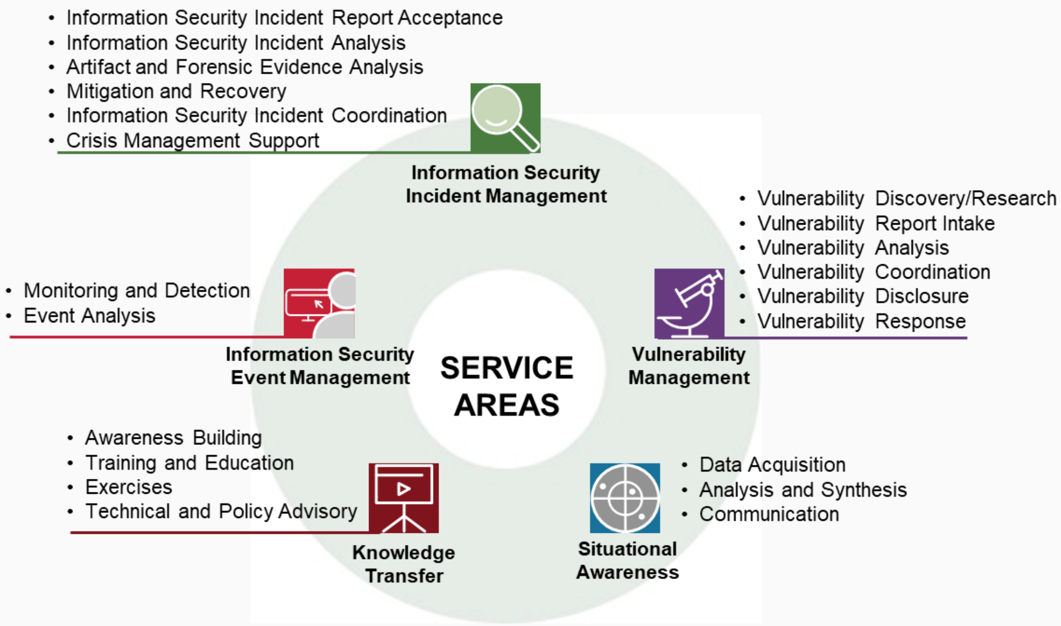

Information Security Incident Report Acceptance
Information Security Incident Analysis
Artifact and Forensic Evidence Analysis
Mitigation and Recovery
Information Security Incident Coordination
Crisis Management Support
Information Security Incident Management
Vulnerability Discovery/Research
Vulnerability Report Intake
Vulnerability Analysis
Vulnerability Coordination
Vulnerability Disclosure
Vulnerability Response
Monitoring and Detection
Event Analysis
Information Security Event Management
SERVICE AREAS
Vulnerability Management
Awareness Building
Training and Education
Exercises
Technical and Policy Advisory
Data Acquisition
Analysis and Synthesis
Communication
Knowledge Transfer
Situational Awareness

Figure 3: *CSIRT Services Framework Service Areas and Service* Source: FIRST

5.2. ITU-T Recommendation X.1060 service categories

The International Telecommunications Union Standardardization Sector (ITU-T) Recommendation X.1060 establishes a framework for organisations to build and manage a cyber defence centre which may be a CSIRT or SOC. Through three (3) processes – building, management, and evaluation – a CSIRT determines which security services should be included in its service catalogue, profile, and portfolio.

ITU-T Recommendation X.1060 identifies nine (9) service categories. Based on basic, standard, and advanced recommendation levels, a CDC can extract a service catalogue from this service list. Furthermore, by determining the service assignment as insourced, outsourced or unassigned, the CDC can develop a service profile and finally a service portfolio by measuring the current service score (As-is) or medium-long term target service score (To-be):

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.

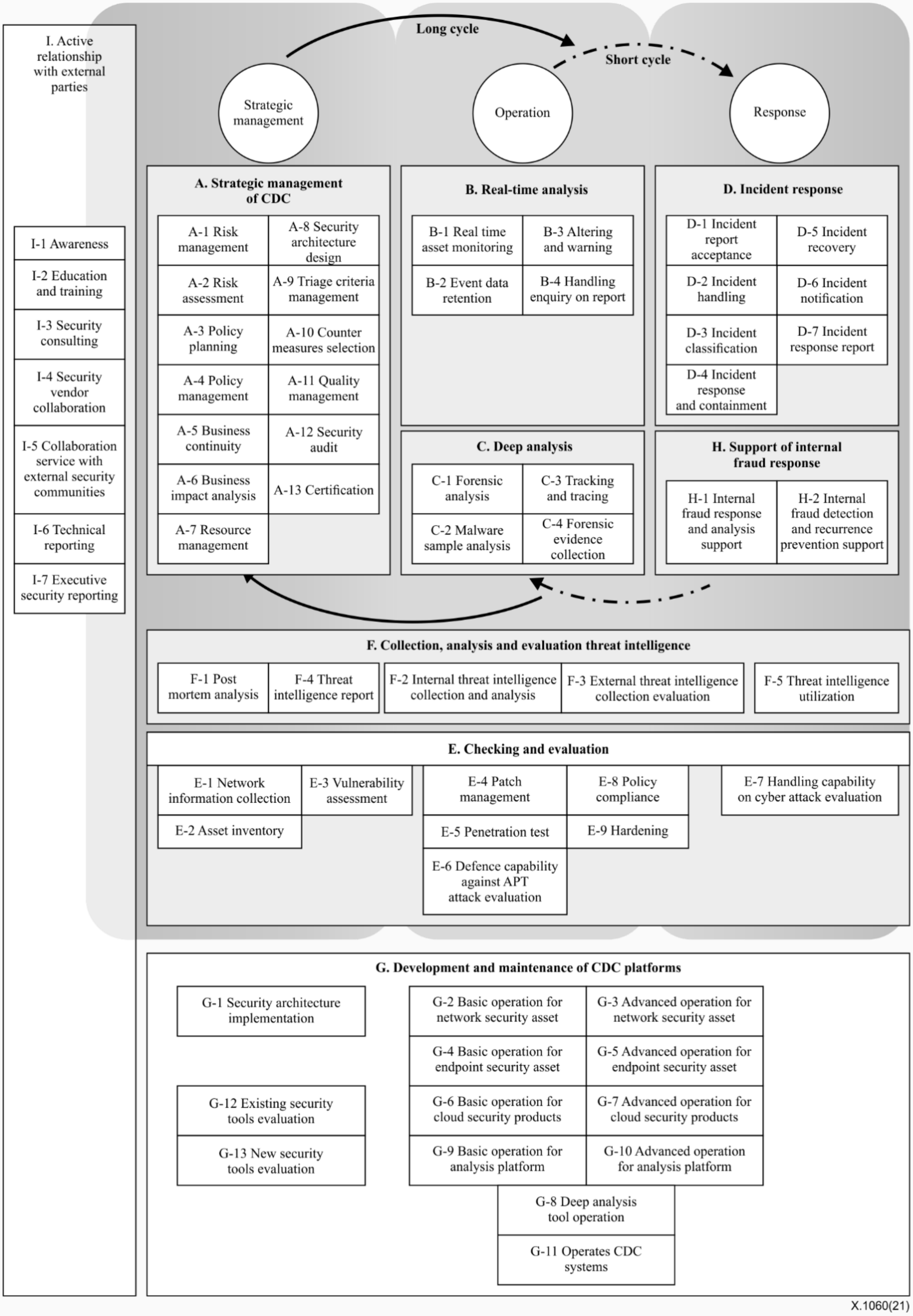

I. Active relationship with external parties
I-1 Awareness
I-2 Education and training
I-3 Security consulting
I-4 Security vendor collaboration
I-5 Collaboration service with external security communities
I-6 Technical reporting
I-7 Executive security reporting
Long cycle
Short cycle
Strategic management
Operation
Response
A. Strategic management of CDC
A-1 Risk management
A-8 Security architecture design
A-2 Risk assessment
A-9 Triage criteria management
A-3 Policy planning
A-10 Counter measures selection
A-4 Policy management
A-11 Quality management
A-5 Business continuity
A-12 Security audit
A-6 Business impact analysis
A-13 Certification
A-7 Resource management
B. Real-time analysis
B-1 Real time asset monitoring
B-3 Altering and warning
B-2 Event data retention
B-4 Handling enquiry on report
D. Incident response
D-1 Incident report acceptance
D-5 Incident recovery
D-2 Incident handling
D-6 Incident notification
D-3 Incident classification
D-7 Incident response report
D-4 Incident response and containment
C. Deep analysis
C-1 Forensic analysis
C-3 Tracking and tracing
C-2 Malware sample analysis
C-4 Forensic evidence collection
H. Support of internal fraud response
H-1 Internal fraud response and analysis support
H-2 Internal fraud detection and recurrence prevention support
F. Collection, analysis and evaluation threat intelligence
F-1 Post mortem analysis
F-4 Threat intelligence report
F-2 Internal threat intelligence collection and analysis
F-3 External threat intelligence collection evaluation
F-5 Threat intelligence utilization
E. Checking and evaluation
E-1 Network information collection
E-3 Vulnerability assessment
E-4 Patch management
E-8 Policy compliance
E-7 Handling capability on cyber attack evaluation
E-2 Asset inventory
E-5 Penetration test
E-9 Hardening
E-6 Defence capability against APT attack evaluation
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-12 Existing security tools evaluation
G-6 Basic operation for cloud security products
G-7 Advanced operation for cloud security products
G-13 New security tools evaluation
G-9 Basic operation for analysis platform
G-10 Advanced operation for analysis platform
G-8 Deep analysis tool operation
G-11 Operates CDC systems
X.1060(21)

Figure 4: *Cyber Defence Centre Services* Source: ITU-T Recommendation X.1060

Reflection Point:

- What services does the national CSIRT in your country offer?
- Which services do you feel should be added to the CSIRT service portfolio and why?

6. Who does the CSIRT serve?

A multistakeholder approach within a country and organisation is critical for the effective management of incidents. The GFCE identifies the building of communities as a good practice that facilitates trusted information sharing and exchange of experience and knowledge.

Good practice: Build communities

A national CSIRT should invest time and continuous effort to build and maintain trust with its constituency and other stakeholders, both nationally and internationally. This can be achieved through constituency relationship management, targeted workshops, and joint exercises.

With cooperation and (relative) transparency, the CSIRT should strive to be a trustworthy, politically neutral, unbiased, and professional/technical partner in the national and international communities.

Reflection point

Using the ENISA Interactive Cybersecurity Institutional Map find out how actors in Europe are involved in functions within a community.

Attempt to develop a similar map for Africa.

The constituent(s) of a CSIRT is the recipient or customer base of the CSIRT services. The team must, in its charters, mission statements, concept of operations documents, or similar documents, clearly define its constituency. The team should understand its constituency so as to determine their needs, the assets they need to be protected, and what the interactions with the CSIRT would be.

Good Practice: Establish the national CSIRT's constituency, authority, and responsibility

The constituencies are the entities and communities for whom the CSIRT provides service and support. The extent of the authority and responsibility of the CSIRT should be predetermined in its role and mandate.

There are different types of CSIRTs depending on the constituency served as indicated in Table 1 below:

Sector	**Focus**	**Typical Constituents**
Academic Sector CSIRT	Academic and educational institutions,such as universities or research facilities, and the campus Internet environments.	University staff and students.
Commercial CSIRT	Commercial services. This can be an independent organisation, an ISP, or managed services provider.	Paying customers
CIP/CIIP Sector CSIRT	Critical Information Protection and/or Critical Information and Infrastructure Protection. This covers the IT of all critical sectors in a country.	Government, critical sectors and citizens.
Governmental Sector CSIRT	The government itself.	Government agencies.
Internal CSIRT/Security Operation Centre (SOC)	The hosting organisation itself.	Internal staff and IT department.
Military Sector CSIRT	Military organizations with responsibilities in IT infrastructure.	Staff of military institutions and closely related entities such as the Ministry

National CSIRT	National focus, considered as the central security point of contact.	No direct constituents, although a National CERT is sometimes combined with a Governmental CERT
Small & Medium Enterprises (SME) Sector CSIRT	This is a self-organised CSIRT to provide services to its own business branch or similar user group.	The SMEs and their staff
Vendor CSIRT/PSIRT	Vendor-specific products, usually to address vulnerabilities or advise on specific attack mitigations. A common acronym is PSIRT, or Product Security Incident Response Team	Product owners

Table 1*: Types of CSIRTs and Constituents* Source: ENISA A step-by-step approach on how to set up a CSIRT

7. Which Tools does a CSIRT need?

There are various tools available that enable a CSIRT to carry out its functions, many of them being open source and therefore free to use.

The GFCE has identified various open source and commercial tools to enable CSIRTs provide services in the five service areas given in the FIRST CSIRT Services Framework of Information Security Event Management (ISEM), Information Security, Incident Management (ISIM), Vulnerability Management (VM), Situational Awareness (SA), and Knowledge Transfer (KT).

FIRST provides a list of security tools (Appendix C) for domain and IP address query, network monitoring, network auditing, vulnerability assessment, intrusion detection, malware analysis, and WiFi tools

8. Policies, frameworks, and guidelines

Policies, frameworks, and guidelines are critical for the support of the incident management, incident handling, information handling, and exchange process and procedures of a CSIRT.

In developing these policies, frameworks and guidelines to provide services in the 5 areas of the FIRST CSIRT Services Framework, the GFCE guideline for development of cyber incident management in low income countries recommends that a team make reference to the international standards such as the ISO/IEC 27035-1:2016, Recommendation ITU-T X.1500, and frameworks such as the the MITRE ATT&CK framework, the SANS framework, the CMU SEI guidance documents.

9. Resourcing and funding a CSIRT

Establishing a successful incident response capability requires substantial planning and resources.

There are several types of funding models that can be used when establishing and operating a CSIRT:

- a cost centre within an organisation, or
- full or partial grants, detailing the grant including issuer and source, purpose, amount and duration of the grant should it be determined.
- selling services either internally or externally
- funded through a consortium of organisations such as universities in a research network.
- or a combination of any of those listed above

The funding should cover:

- Capital Expenditure (CAPEX): to cover initial cost related to the acquisition of hardware and software, equipment and tools, and premises
- Operating Cost (OPEX): to cover recurring operational costs for engagement with the constituency, personnel, facilities and software licences, delivery, maintenance and maintenance of services, technology, processes, and organisational capabilities.

9.1. What does a CSIRT Budget look like?

An initial budget of the CSIRT is drawn up in the initial phase of the CSIRT establishment. The ENISA guide on How to set up CSIRT and SOC recommends that the budget for the initial year should cover at least:

- Initial staff salaries,
- Facility establishment costs,
- Salaries or consultancy service fees for creating the design stage results,
- CSIRT skills acquisition recruitment and training, and

- Preliminary technology and licences.

Resource: Indicative costs for setting up a CSIRT for 2020

Budget Item	**Average cost per year**
CSIRT staff member (including managers)	EUR 40 000–60 000
Minimum three staff members Depending on the constituency size and mandate, CSIRTs typically employ the following numbers of staff: small – 3–7, medium – 10–15, large – 30–60.	EUR 120 000–180 000
12 additional employees (six teams of two staff members to cover 24/7, with each shift covering 8 hours) if required to provide operations 24/7 for 365 days a year	EUR 480 000
Office rental per staff member per year	EUR 3 000–4 000
Staff training and conference attendance per person per year	EUR 3 000–10 000
Depending on the scope, consultancy services for the establishment of a CSIRT (design and implementation)	EUR 75 000 -1 000 000 (over a 1- 3-years)
Hardware, networking and specialised equipment for performing specific CSIRT operations (use of cloud services reduce initial investments in hardware)	EUR 100 000–300 000
Software and software services (open-source solutions may reduce costs)	EUR 50 000

Note: Cost estimates are done for illustrative purposes only and does not depict any particular country.

Source: How to set up CSIRT and SOC, ENISA

Reflection point

The ENISA guide: How to set up CSIRT and SOC states that "*The discrepancy between the detailed mandate and the budget is a common reason why CSIRTs do not fulfil their mandate*."
Where does the national CSIRT derive its mandate?
What are the sources of funding for the national CSIRT in your country?
Which funding model is used in your country?
What are the initial and operating budget considerations?

Leave your comment below.

10. CSIRT capabilities

10.1. Training and certification

The role of a CSIRT is to manage the operational response to incidents, regardless of the type of incident, both out-of-band and day-to-day incidents. To perform such tasks, a CSIRT needs to be efficient and professional, with experts qualified in the IT security field.

Resource: Video: Cybersecurity Professional Profile

The making of Cybersecurity Professional: Listen in as bikozulu catches up with cyber security guru, Dr. Bright Gameli

Training in technical and soft skills, malware analysis, industrial control systems/SCADA, cyber threat monitoring and analysis, oral/written communication, relationship management at international and national levels, coping with stress and problem solving, were, in particular, identified as important in improving the functionality of the CSIRTs in GFCE survey of low income countries. The challenges associated with the acquisition of these skills with limited budgets, the lack of competent trainers, and heavy workloads may be overcome through regional and international collaboration in capacity building.

Good Practises: Seek support from others for national CSIRT capacity building

Reference to the GFCE Global Good Practice - National Computer Security Incident Response Teams (CSIRTs) sharing information as well as seeking knowledge and expertise for practical and applicable solutions from global and regional communities is critical for the foundation of a national CSIRT. Capacity building through communities such as Forum for Incident Response Teams (FIRST), AfriCERT, OIC-CERT, Meridian process buddy initiative.

To build the critical mass of cybersecurity experts required to protect the Continent, it is proposed that countries consider introducing cyber-related training to children at an early age. Taking advantage of increased access to broadband, this training could be delivered online.

Resource:

An objective of the Digital Transformation Strategy for Africa (2020-2030) is to "*offer a massive online e-skills development program to provide basic knowledge and skills in security and privacy in the digital environment to 100 million Africans a year by 2021 and 300million per year by 2025.*"

Based on the classification of services in the FIRST CSIRT Services Framework (*see section 5.2*), the GFCE has developed an N-CSIRT service roadmap which proposes the resources requirements, knowledge, skills, competencies, policies, guidelines, frameworks, tools, and trainings necessary to manage each service.

Training tailored for CSIRT teams is offered by Udemy, SANS National Initiative for Cybersecurity Education (NICE), EC Council, ISACA, IBM, ISC2, eLearningSecurity, Cyber4Dev, CREST and global CSIRT collaborations including AfricaCERT, ENISA, CIRCL, CERT-Tools Community, ICANN. Make reference to Section 4.

Reflection point

An self-assessment of the N-CSIRT capability using the above tools and maturity models can help in the identification of resources and training required to improve the services of the team to its constituents.

Based on the existing and planned services of your N-CSIRT what training does the team require?

Identify the training providers.

Case Study: EG-CERT Experience in Capacity Building

Egyptian national Computer Emergency Readiness Team (EG-CERT), affiliated with the Egyptian National Telecom Regulatory Authority (NTRA) was launched in April 2009. EG-CERT offers both reactive and proactive services to its constituents who are in the ICT, financial, and government sectors.

The EG-CERT employs over 60 professionals (more than 45 of them are full-time cybersecurity professionals). Recognising the need to empower and enhance the skills of those responsible for CIIP in the critical sectors, the NTRA organised and sponsored a pilot national cybersecurity training program between 2009–2010. The program trained 220 professionals in 38 organisations within the governmental/public sector, banking sector, education sector, as well as from ICT private sector companies. Outcomes from the program included 179 international certificates from SANS and creation of awareness, enhanced readiness, and the establishment of a network of trust and enhanced cooperation spirit among participating entities and professionals.

The financial sponsorship from the NTRA was an indication of commitment, partnership, and support from the public sector, and inspired other programs and gained the recognition of International Telecommunications Union (ITU) in the Global Cybersecurity Index, published in 2015 and subsequent years.

EG-CERT participates in national cybersecurity matters including the development and implementation of the Egyptian National Cybersecurity Strategy, first published in 2017 and in the Egyptian Supreme Cybersecurity Council (ESCC) established in 2014. At the regional and international level, EG-CERT participates in collaboration events including annual international cyber drills with Asia Pacific – APCERT annual cyber drill, Organization of Islamic Countries – OIC-CERT annual cyber drills and the ITU Arab region cyber drill. EG-CERT is a member of the international Forum of Incident Response and Security Teams (FIRST), and a founding member of the Organization of Islamic Countries CERT (OIC-CERT) and AfricaCERT.

Source:
Cyber Incident Management in Low-Income Countries - 1: PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT

10.2. Auditing

Cybersecurity audits are a primary element of cybersecurity strategy and legislation. However, skills and funds to carry these audits out are limited.

Analysis of cybersecurity incidents would assist in building capabilities and in research and development (R&D), while the exploration of a Cybersecurity Incident Report and Analysis System for the African continent would be useful.

10.3. Cyber drills

The capabilities of a CSIRT are significantly improved through cyber drills through using scenarios to test preparedness, communication, and response capabilities.

Resource: Improving capabilities with cyber drills

AfricaCERT

AfricaCERT organised its first Cyber Drill: “Testing the Waters’’, in 2021. The drill aimed to test the response capability of participating teams facing the following scenarios: phishing, defacement, REM, and ransomware investigation. These exercises were designed to put participants into live conditions and test their communication and technical capabilities. 32 Computer Security Incident Response Teams from 24 countries, including APCERT and OIC-CERT economies teams, participated in the Drill.

APCERT

APCERT organises a cyber drill for APCERT Region and partners. The theme of the 2021 APCERT drill was ’’Supply Chain Attack through Spear-Phishing – Beware of Working from Home’. The exercise reflected real incidents while issues reflected the collaboration amongst the economies in mitigating cyber threats and validated the enhanced communication protocols, technical capabilities, and quality of incident responses that APCERT fosters in assuring Internet security and safety. Twenty five CSIRTs from nineteen economies of APCERT and two of the OIC-CERT and AfricaCERT participated.

ITU

The ITU organises annual Cyber Drills designed with a dual purpose: as a platform for cooperation, information sharing, and discussions on current cybersecurity issues, as well as to provide hands-on exercise for national Computer Incident Response Teams (CIRTs) / Computer Security Incident Response Teams (CSIRTs).

OAS

OAS (Organization of American States) and INCIBE (Spanish National Cybersecurity Institute) annually organise the International CyberEx that seeks to strengthen the ability to respond to cyber incidents and improve collaboration and cooperation. International CyberEx 2020 had 80 teams and 320 team members representing 39 countries.

OIC-CERT

The Organization of the Islamic Cooperation - Computer Emergency Response

Teams (OIC-CERT) organises an annual Cyber Drill with objectives to:
• Test the communication capabilities of the members' points of contact.
• Check the processes and procedures in managing contingencies.
• Test the technical competencies of participating teams.
• Simulate cross-border cooperation in mitigating information security incidents.

Capture-The-Flag (CTF)
This is a competitive computer security event where participants compete in security-themed challenges for the purpose of obtaining the highest score

Source:
Cyber Incident Management in Low-Income Countries - 1: PART 1: A HOLISTIC VIEW ON CSIRT DEVELOPMENT

11. Regional and global coordination and cooperation

As cyberspace is transboundary, trusted cooperation with global alliances and networks of CSIRTs, such as the global Forum for Incident Response and Security Teams (FIRST), African Forum of Computer Incident Response Teams (AfricaCERT), Team Cymru CSIRT Assistance Program, TF-CSIRT, and Operations Security Trust (Ops-T) forum, Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT), is of the essence.

These networks provide a forum for cooperation, exchange of information, and building trust and enhance members' capabilities in handling cross-border incidents and coordinated incident responses. Membership to these networks requires teams to meet a minimum requirements including payment of annual membership fees. Recognition of the CSIRT's maturity level determines membership status.

Resources: Trusted Introducer

Trust is a critical element in cybersecurity coordination and cooperation. The Trusted Introducer Service (TI) provides a robust membership criteria and includes demonstrated and checked levels of maturity for evaluation. The TI has established a trust-building clearing house for its CSIRT community. The Trusted Introducer Service (TI) differentiate between four categories:

- teams are
    - listed, which provides basic information about the team itself as well as shows endorsement of the team by the TI community, Morocco's maCERT, Mozambique's MoRENet CSIRT, South Africa's SA NREN CSIRT, Togo's CERT.tg are listed;
    - accredited, which ensures a defined level of best practises and acceptance of the established TI policies for such teams. South Africa's SA NREN CSIRT is accredited;

    - certified, if they have been accredited before and prove a confirmed level of maturity as defined by the TI SIM framework.
- security experts can participate as TI Associates.

Reasons why CSIRTs in Africa should consider becoming a Trusted Introducer (TI) listed team are to:

- express an interest in cybersecurity on an international stage
- provide proof to stakeholders of a commitment to follow contemporary security challenges and adhere to community-agreed best practices and standards
- provide an opportunity to be involved in different security projects, where their success is largely based on the contributions of CSIRTs from different sectors and constituencies
- learn from the successes and failures of other teams from personal face-to-face meetings and subject-matter presentations or briefings
- meet other security teams three times a year in different European locations by being invited by volunteering teams or national communities willing to support the TF-CSIRT objectives
- become a member of very open, friendly and not-competitive environment that cultivates a sensitive discussion and consensus building which is outside of the usual pressures of the daily business
- After getting familiar with the community and adopted practices, you can take the appropriate steps towards accreditation and certification

11.1. Forum of Incident Response and Security Teams (FIRST)

The Forum of Incident Response and Security Teams (FIRST) has a CSIRT membership model based on the conformance to evaluation criteria and site visit (now virtual, beginning April 2020 due to COVID-19 restrictions).

There are two types of membership:

- **Full Members** represent security incident response teams who assist an information technology community or other defined constituency in preventing and handling security-related incidents. After membership is confirmed, a team must pay an initial one-time application fee of US$800 for full membership and annual fee is US$ 2000;
- **Liaison Members** are individuals or representatives of organisations other than incident response or security teams that have a legitimate interest in and value to FIRST. The initial application fee is not applicable to liaison members, who pay an annual fee of US$100.

FIRST membership benefits include access to a forum for trusted interactions, sharing of information at annual conferences and technical colloquia, technical tools and collaboration channels, and expertise.

11.2. AfricaCERT

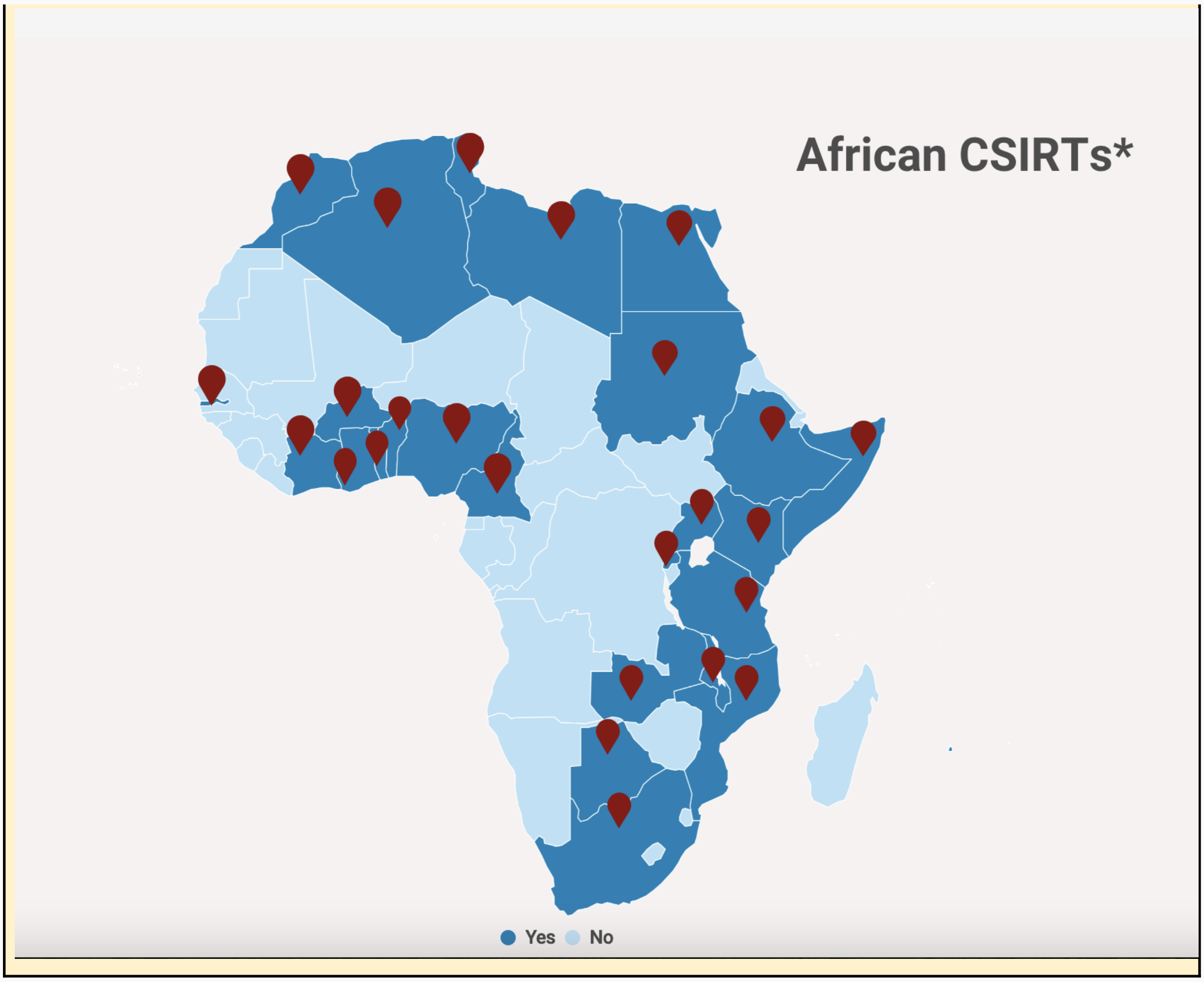
The African Forum of Computer Incident Response Teams (AfricaCERT) objectives include facilitating:

- regional and international coordination and cooperation
- assistance in establishing CSIRTS
- education and outreach programs
- Information, good practises and experience sharing
- improved cyber readiness and resilience
- collaborative research, development, and innovation

Membership to AfricaCERT is by way of application supported by a sponsor. The application form submitted by email is reviewed and evaluated by the members of the AfricaCERT Board of Directors. There are 3 membership categories:

- Operational Member must be located in Africa and is expected to be an active participant in AfricaCERT affairs
- Supporting Member is an entity from any region with activities related to cyber security and includes the NGOs or academia
- Individual Member: individuals can apply for membership sponsored by two AfricaCERT operational members. Individuals pay a membership fee of US$25.

Resources: *Interactive Map of AfricaCERT members* Source: DiploFoundation



11.3. Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT)

The purpose of the Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) is to support the collaboration and cooperation of CERTs in OIC member countries. OIC-CERT objectives include:

- strengthening relationships amongst CERTs in the OIC member countries and stakeholders
- encouraging experience and information sharing
- preventing and reducing cybercrimes, harmonise cyber security policies, laws, and regulations
- building cybersecurity capabilities and awareness
- promoting collaborative cybersecurity research, development, and innovation
- promoting international cooperation
- assisting in the establishment and development of national CERTs.

OIC-CERT has 6 membership categories:

- Full Member
- General Member
- Professional Member
- Affiliate Member
- Commercial Member
- Fellows Member
- Honorary Member

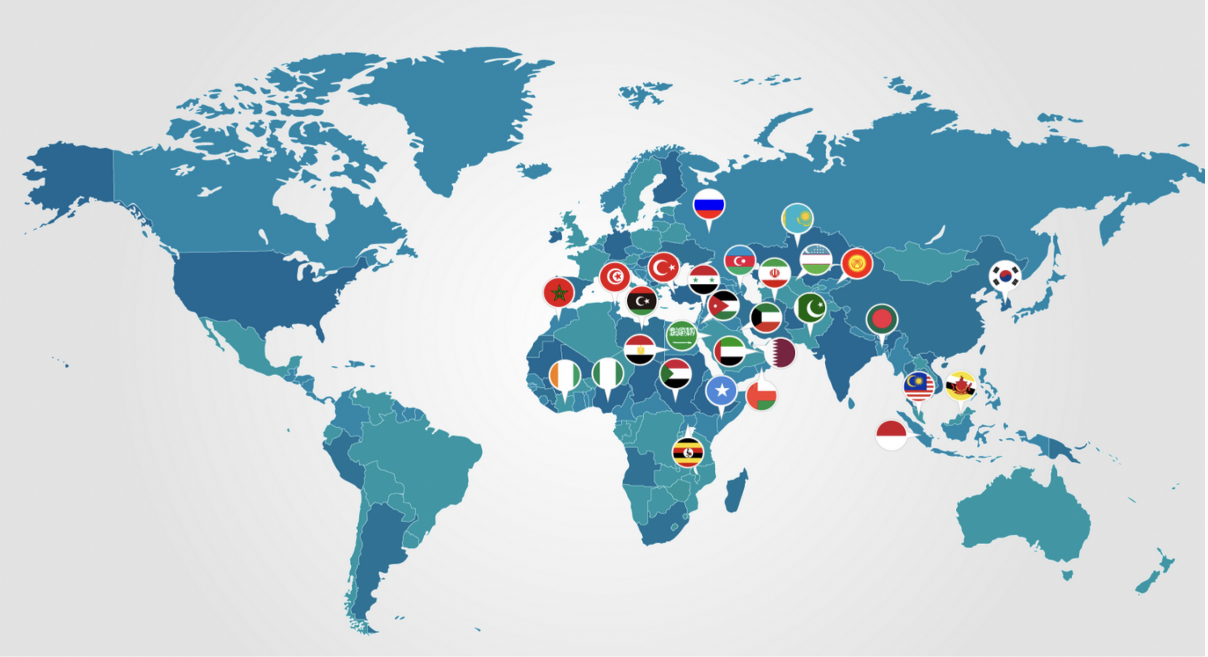


***Figure 5**: OIC-CERT members* Source: OIC-CERT

11.4. Meridian Process Buddy initiative

Countries can establish bilateral and multilateral collaboration. The GFCE-Meridian 'Buddy Initiative' is mentioned as a good practice, in addition to other good practices in Networking and information sharing.

Good Practice: Buddying system

A buddy nation (or a guide nation) may formally or informally share, in a confidential
environment, valuable organisational or process-wise approaches and lessons learned with a nation with less developed policies, limited resources, and knowledge.

Cyber security strategy development arrangements in the African Union (AU) can be used as a budding system.

12. Women in Cybersecurity

On a global scale, women are under-represented in the cybersecurity workforce and paid less than their male counterparts. Various institutions are seeking to train, recruit, and retain women within the cybersecurity field, as well as support women to take up leadership and managerial positions.

The GFCE Gender and Cybersecurity: creating a more inclusive digital world project aims to explore the possible reasons for and solutions to address this gender gap in the cybersecurity field. Few women in Africa, and 10 percent globally, are represented in the cybersecurity profession, because young girls in the education system are not aware of the field as a career option. In addition, there is a need to build confidence in women to take up leadership and strategic positions, and provide mentorship. The GFCE Women in Cyber Capacity Building Network aims to enhance cooperation and knowledge sharing, identify cyber capacity needs on a regional level, and support the growth of a trusted community of cyber experts.

Resource: *Podcast Bridging the Gender Gap in Cybersecurity with Louise Marie Hurel and Angela Matlapeng*

Women are under-represented in the field of cybersecurity.

ITU's Women in Cyber mentorship programme, organised jointly by the EQUALS Global Partnership and the Forum for Incident Response Teams (FIRST), aims to help bridge the gap. The programme is an outcome of the CyberDrill 2020 Empowering Women in Cybersecurity Webinar, where the need for role models and mentorship was identified as pivotal for increasing the number of women leaders in cybersecurity.

In this episode of the UNconnected, Doreen Bogdan-Martin, Director of the ITU Telecommunication Development Bureau, speaks with Louise Marie Hurel and Angela Matlapeng, who, as a mentor and mentee respectively, participated in the programme. They discuss the challenges and opportunities for women in cyber, and the way forward for women to co-create and lead solutions in this field.

Women in Cyber Mentorship Programme
Become a changemaker in cybersecurity
http://itu.int/go/WiCmp
Partners
FIRST
EQUALS GLOBAL PARTNERSHIP
ITU

13. Conclusion

Congratulations, you have reached the end of the module. In the concluding part, we will reflect on the key takeaways from this module, leaving some additional space for you to write down the points which seem important to you and are not included above.

With the use of resources, examples, reflections and exercises, we have addressed the importance of cyber incident management and the building of cybersecurity capacities through the establishment of a Computer Security Incident Response Team (CSIRT). We have familiarized ourselves with services that CSIRTs offer as well as identified the tools and skills required to run a CSIRT. Finally, we have discussed the importance of regional and international cooperation and identified the requirements for membership in regional and international CSIRT networks such as AfricaCERT, FIRST and OIC-CERT.

Reflection: Important Points

Write down 5 important points that are important to you and are not included in this module.

Next steps

Take the Forum for Incident Response Teams (FIRST): Incident Response for Policy makers