The Commonwealth Computer Emergency Response Teams Toolkit for Africa

The Commonwealth

Foreign, Commonwealth
& Development Office

The Commonwealth Computer Emergency Response Teams Toolkit for Africa

The Commonwealth

Prepared by

The Commonwealth Africa Cyber Fellows

© Commonwealth Secretariat 2025

All rights reserved. This publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or otherwise provided it is used only for educational purposes and is not for resale, and provided full acknowledgement is given to the Commonwealth Secretariat as the original publisher.

Views and opinions expressed in this publication are the responsibility of the authors and should in no way be attributed to the institutions to which they are affiliated or to the Commonwealth Secretariat.

Wherever possible, the Commonwealth Secretariat uses paper sourced from responsible forests or from sources that minimise a destructive impact on the environment.

Published by the Commonwealth Secretariat.

Contents

List of Figures and Tables

Figures

Tables

Foreword

In an era of rapid digital transformation, the resilience of our cyber infrastructure is a necessity. Across the Commonwealth, as digital systems become the foundation for everything from public services to financial systems, we must act with urgency to protect the platforms and networks that underpin our economies, societies, and everyday lives.

I therefore commend to you the Commonwealth Africa Cyber Fellowship (CACF) *Computer Emergency Response Teams (CERTs) Toolkit*. This timely and practical resource, developed by the Commonwealth Africa Cyber Fellows, reflects the spirit of collaboration and innovation that defines our Commonwealth.

Designed specifically for Africa, this *Toolkit* provides a roadmap for establishing and strengthening CERTs — essential frontline institutions in our collective cyber defence. It offers hands-on guidance, operational tools, and policy templates that will help governments, institutions, and technical communities across the region prevent, detect, and respond to cyber threats with greater confidence and coordination.

The *Toolkit* delivers on the commitments made under the Commonwealth Cyber Declaration: to build inclusive, resilient, and secure digital societies. It acknowledges both the promise of digital opportunity and the perils of cyber insecurity. It equips stakeholders — especially those working in resource-constrained environments — with the means to take effective, locally relevant action.

I take this opportunity to thank the United Kingdom's Foreign, Commonwealth and Development Office (FCDO) for its financial support through the Commonwealth Cyber Capability Programme, which made this initiative possible.

We will continue to work together to ensure that digital progress across our Commonwealth is underpinned by robust security, trust, and shared responsibility.

I encourage all stakeholders to make full use of this *Toolkit* — and to continue to advance our shared effort to build a safer, stronger, and more resilient digital future.

Hon. Shirley Botchwey

Commonwealth Secretary-General

Acknowledgments

The Commonwealth Secretariat sincerely thanks the Commonwealth Africa Cyber Fellows (CACF) for developing the *Commonwealth Computer Emergency Response Teams (CERTs) Toolkit for Africa*.

This project was led by the Cyber Capability Programme within the Governance and Peace Division (GPD), which includes Dr Nkechi Amobi, Senior Research Officer; Emma Beckles, Programme Officer; and Shakirudeen Ade Alade, Programme Coordinator.

Special appreciation goes to Mr Kenneth Adu-Amanfoh (Chair of the CACF), Dr Aprielle Oichoe (Deputy Chair of the CACF), and Manish Lobin for their leadership and coordination of CACF members during the *Toolkit's* development.

We also appreciate the efforts of the following Fellows for their valuable input:

Donna Owiti, Dr Bright Mawudor, Jamila Akaaga Ade, Alex Williams, Geraldine Mugumya, Abbas Lawal, Mr Petrus Amuphadi, Jean Pierre Nzabahimana, Christpher Anthony, Paul Savy, Dr Lesedi Mashumba, Chewa Mutale, Richmond Redwood-Sawyerr, Johnson Tumusiime, Alick Mponela, Ntogwa Bundala, Professor Janvier Ngnoulaye, Richard Gyambiby, Eric Akumiah, and Jairus Kapenda.

Special thanks are given to Bello Hayatudeen, a founding member of CACF, for conceptualising this initiative.

Lastly, we recognise the valuable feedback from our internal reviewers, Anslem Charles, Adviser in the ICT Data and Analytics Section, and Clive Lawson, Publications Assistant in the Communications Division.

Acronyms and Abbreviations

APT	Advanced Persistent Threat
CACF	Commonwealth Africa Cyber Fellowship
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
FIRST	Forum of Incident Response and Security Teams
GDPR	European Union's General Data Protection Regulation
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IT	Information Technology
IR	Incident Response
IOC	Indicator of Compromise
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centre
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KE-CIRT/CC	Kenya Computer Incident Response Team Coordination Center
KPI	Key Performance Indicator
MISP	Malware Information Sharing Platform
nCSIRT	National Cybersecurity Incident Response Team
NIST	National Institute of Standards and Technology
OSINT	Open-Source Intelligence
PPP	Public–Private Partnership
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
TTP	Tactics, Techniques and Procedures

Executive Summary

The *Commonwealth Computer Emergency Response Teams (CERTs) Toolkit for Africa ('the CERTs Toolkit'*), developed by the Commonwealth Africa Cyber Fellowship (CACF), is a strategic and operational resource designed to enhance cybersecurity resilience across Commonwealth nations, with a focus on contextual challenges and opportunities within the Africa region. Developed by cyber experts under the Commonwealth Africa Cyber Fellowship, the *Toolkit* addresses the increasing complexity and scale of cyber threats impacting economies and societies across the Commonwealth.

As member nations continue to experience rapid digital transformation – driven by increased mobile connectivity, digital services and financial inclusion – cybersecurity risks have become more prevalent. The CACF *CERTs Toolkit* offers a practical, scalable and adaptable framework to support governments, organisations and cybersecurity practitioners in establishing, strengthening and sustaining CERTs.

The CACF *CERTs Toolkit*:

- supports the creation and operationalisation of CERTs, particularly in resource-constrained environments;
- offers policy templates, incident response frameworks, communication protocols, training modules and assessment tools tailored to the diverse contexts of Commonwealth nations;
- promotes cross-border collaboration, regional intelligence sharing and co-ordinated cyber incident response; and
- aligns with global cybersecurity best practices and Commonwealth priorities, including the Commonwealth Cyber Declaration.

Key objectives include.

1. Enhancing cyber resilience across national and sectoral levels.
2. Facilitating the structured establishment and capability development of CERTs.
3. Addressing the cybersecurity skills gap through capacity building and knowledge transfer.
4. Fostering intergovernmental and cross-sectoral co-operation; and
5. Supporting national cybersecurity policy development and sustainable planning.

While the CACF *CERTs Toolkit* provides a robust foundation, it acknowledges potential implementation challenges, including resource constraints, infrastructure gaps and the rapidly evolving threat landscape. Nonetheless, it remains a critical enabler of cybersecurity maturity for Commonwealth African countries, ensuring that nations are better equipped to defend against threats and safeguard their digital future.

1. Introduction

1.1. Africa's challenge

In an era where digital technologies drive economic growth and societal development, Africa's cybersecurity landscape presents both significant challenges and opportunities. Many African countries face technological infrastructure limitations, making it essential for critical systems to remain resilient during attacks and recover quickly to full capacity.

The continent is experiencing rapid digital adoption, driven by advancements in mobile technology, e-commerce and financial inclusion, among other factors. However, this transformation has also exposed Africa to increasingly sophisticated cybersecurity threats, including ransomware, phishing and state-sponsored cyberattacks. Computer Emergency Response Teams (CERTs) play a crucial role in national and organisational cybersecurity by mitigating cyber threats, responding to incidents and enhancing overall cyber resilience. As cyber threats grow in complexity and scale, the need for robust, co-ordinated and well-equipped CERTs has become more urgent than ever. Their importance stems from their ability to co-ordinate responses to cyber threats, protect critical infrastructure, and facilitate collaboration between governments, businesses and international organisations. However, many African nations face challenges in setting up and operationalising CERTs due to various issues, including insufficient infrastructure, limited funding, and a shortage of skills, policy frameworks, and unified laws and regulations.

1.2. Why a *CERTs Toolkit* for Africa?

Addressing this critical need, the Commonwealth Africa Cyber Fellowship (CACF) has developed the CACF *CERTs Toolkit* – a comprehensive resource designed to enhance cyber resilience across African nations. The CACF *CERTs Toolkit* is intended to support CERTs, policy-makers and cybersecurity practitioners in establishing and maintaining effective cybersecurity operations. By leveraging global best practices and contextualising them to Africa's unique challenges, the toolkit empowers stakeholders to:

- respond effectively to cyber incidents;
- strengthen national cybersecurity strategies;
- foster collaboration across sectors and borders; and
- minimise skills gaps through training and capacity building.

This toolkit embodies the Commonwealth Africa Cyber Fellowship's commitment to enhancing Africa's cybersecurity capacity through leadership, training and collaboration. It provides practical guidelines, templates and resources that address the operational, technical and strategic aspects of CERT development and management. The CACF *CERTs Toolkit* actualises the objective of the Commonwealth Cyber Declaration 2018, reiterating the Commonwealth's shared interest in protecting the security of its networks, data, the people who use them and the services that run on them.

The CACF *CERTs Toolkit* also aligns with the Commonwealth's values of co-operation and mutual support to provide a guide to setting up and maintaining CERTs, cognisant of the challenges faced by Africa as a continent. This ensures that African nations can have a reference in their bid to protect their digital economies, through the establishment of functional CERTs, and ultimately build a safer digital future for Africa.

1.3. Purpose of the CACF *CERTs Toolkit*

The CACF *CERTs Toolkit* aims to bridge the cybersecurity knowledge gap, foster regional co-operation and ultimately build a safer digital future for Africa. This document serves as a step-by-step guide for establishing CERTs, strengthening CERT capabilities and empowering nations to defend against emerging threats while leveraging the vast potential of the digital age.

This toolkit serves not only as a technical guide but also as a strategic resource, aimed at fostering collaboration, innovation and resilience. Developed by the Commonwealth Africa Cyber Fellowship, it incorporates insights from cyber experts across the Commonwealth and beyond. The goal is to empower African nations to protect their digital futures and ensure that they are prepared to meet the challenges of the digital age. The toolkit provides a comprehensive set of templates and guidelines tailored to address the region's unique cybersecurity challenges.

1.4. Objectives of the of the CACF *CERTs Toolkit*

i. **Strengthening cyber resilience**

- Enable African nations to proactively identify, respond to and mitigate cyber threats, minimising disruptions to critical infrastructure, businesses and services.
- Provide standardised frameworks and tools to ensure consistent and efficient cybersecurity operations.

ii. **Supporting the establishment of CERTs**

- Offer a step-by-step guide for nations or organisations looking to set up new CERTs, even in resource-constrained environments.
- Provide templates for organisational structure, operational workflows and budget planning to streamline the establishment process.

iii. **Enhancing operational capabilities of existing CERTs**

- Assist existing CERTs in scaling their operations to handle emerging threats such as ransomware, phishing and advanced persistent threats (APTs).
- Introduce best practices for incident management, threat intelligence sharing and stakeholder co-ordination.

iv. **Promoting regional collaboration and knowledge sharing**

- Encourage cross-border intelligence sharing to combat transnational cyber threats and strengthen regional cyber defences.
- Facilitate partnerships among African nations through shared resources, training programmes and collaborative initiatives.

v. **Building human and institutional capacity**

- Provide training materials, skill development programmes and leadership resources to enhance the technical and operational expertise of CERT personnel.
- Strengthen institutional capacity by aligning CERT activities with national cybersecurity strategies and global standards.

vi. **Supporting policy development and advocacy**

- Guide policy-makers in creating sustainable and effective cybersecurity policies that integrate CERTs as central elements of national cyber defence.
- Advocate for public–private collaboration to address the growing cyber risks facing businesses and individuals.

vii. **Promoting sustainability and long-term planning**

- Help CERTs develop funding strategies, recruit skilled personnel and acquire necessary infrastructure for long-term sustainability.
- Provide resources for continuous improvement through regular assessments and updates to the toolkit.

viii. **Aligning with global cybersecurity goals**

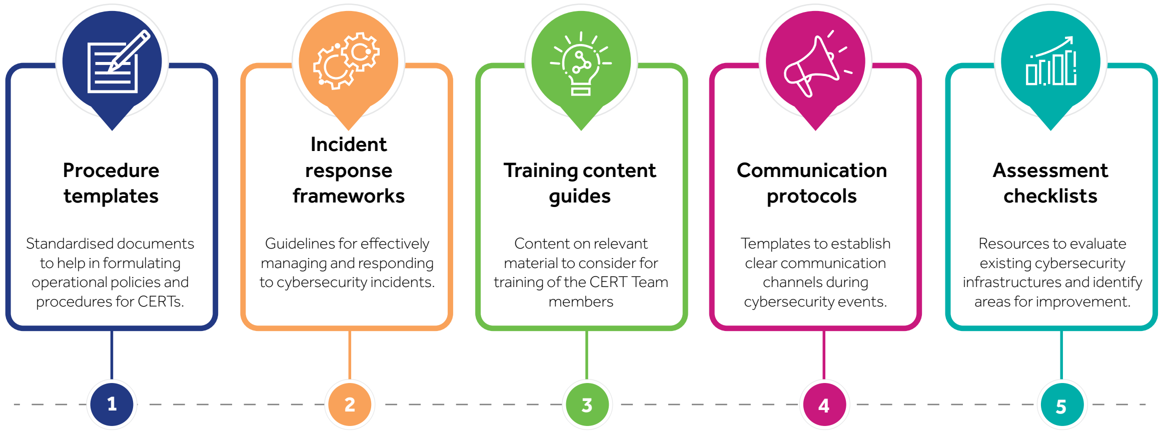
- Support African nations in aligning with international cybersecurity frameworks such as the United Nations Convention on Cybercrime, the Commonwealth Cyber Declaration and the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention').

1.5. Key Components of the CACF *CERTs Toolkit*

The key components of the toolkit are depicted and detailed below:

1. **Policy and procedure templates**: Standardised documents to help in formulating operational policies and procedures for CERTs.
2. **Incident response frameworks:** Guidelines for effectively managing and responding to cybersecurity incidents.
3. **Communication protocols:** Templates to establish clear communication channels during cybersecurity events.

Figure 1.1 Key components of the CACF CERTs Toolkit.



Procedure templates

Standardised documents to help in formulating operational policies and procedures for CERTs.

Incident response frameworks

Guidelines for effectively managing and responding to cybersecurity incidents.

Training content guides

Content on relevant material to consider for training of the CERT Team members

Communication protocols

Templates to establish clear communication channels during cybersecurity events.

Assessment checklists

Resources to evaluate existing cybersecurity infrastructures and identify areas for improvement.

4. **Training modules:** Educational materials aimed at building the capacity of CERT personnel.

5. **Assessment tools:** Resources to evaluate existing cybersecurity infrastructures and identify areas for improvement.

These resources are instrumental in strengthening national cybersecurity postures and fostering collaboration across the continent.

1.6. Scope

While the toolkit is a comprehensive resource, it operates within specific boundaries to ensure practical and achievable outcomes. Below is a detailed overview of its scope and limitations.

Geographic focus

- The toolkit is designed specifically for the African context, addressing the unique cybersecurity challenges faced by countries in the region.
- It is applicable to individual nations, regional blocs (for example, the Economic Community of West African States [ECOWAS], the Southern African Development Community [SADC]) and sector-specific CERTs.

Target users

- The toolkit targets governments and policy-makers aiming to establish or enhance national CERTs.
- It is also aimed at industry-specific organisations, such as those in the financial services, telecommunications, health and energy sectors, that require sectoral CERTs.
- It also targets regional cybersecurity initiatives to foster collaboration and intelligence sharing.

1.7. Key functional areas of the CACF *CERTs Toolkit*

The functional key areas addressed by this CACF *CERTs Toolkit* are depicted in Figure 1.2.

1.8. Limitations

Resource constraints

- Infrastructure requirements: The toolkit assumes access to certain levels of infrastructure (for example, secure communication tools, reliable internet), which may not be available in all regions.
- Human capital: Successful implementation requires skilled personnel, which some nations may lack initially.

Customisation needs

- While the toolkit is adaptable, countries with highly unique political, cultural or legal environments may require additional customisation beyond what the toolkit provides.

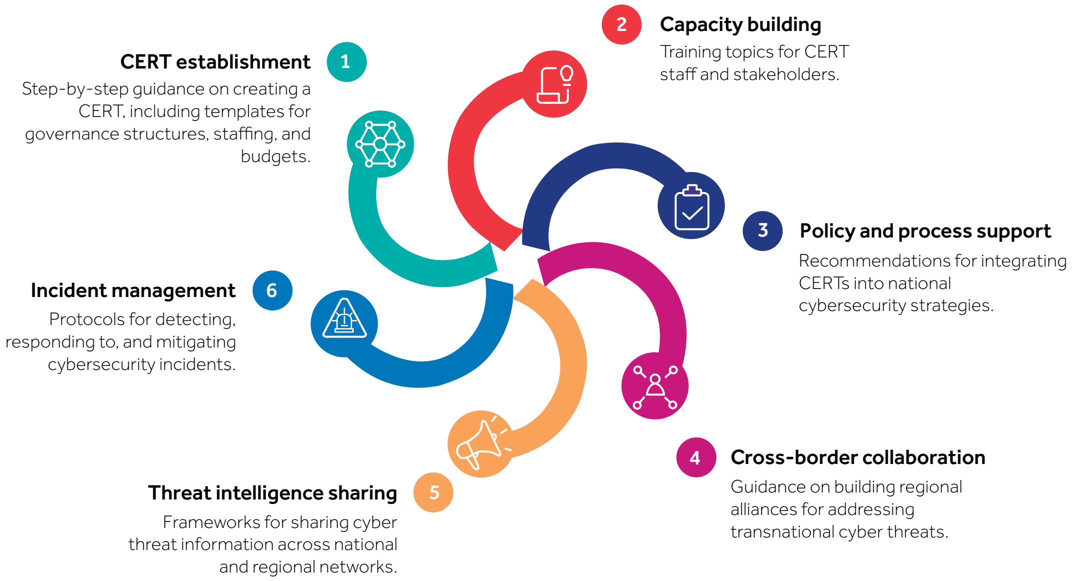
Financial challenges

- Implementation and operation of CERTs require funding, which may be a challenge for resource-constrained nations. The toolkit provides guidance but does not directly address funding gaps.

Technological dependencies

- The toolkit focuses on existing technologies and methodologies. Nations facing rapid

Figure 1.2 Key functional areas of the CACF CERTs Toolkit.



1 **CERT establishment**
Step-by-step guidance on creating a CERT, including templates for governance structures, staffing, and budgets.

2 **Capacity building**
Training topics for CERT staff and stakeholders.

3 **Policy and process support**
Recommendations for integrating CERTs into national cybersecurity strategies.

4 **Cross-border collaboration**
Guidance on building regional alliances for addressing transnational cyber threats.

5 **Threat intelligence sharing**
Frameworks for sharing cyber threat information across national and regional networks.

6 **Incident management**
Protocols for detecting, responding to, and mitigating cybersecurity incidents.

technological advancements or emerging threats may need to supplement the toolkit with cutting-edge solutions.

Limited focus on specialised threats

- Although comprehensive, the toolkit may not cover niche or highly specialised threats (for example, quantum computing risks, advanced persistent threats targeting specific sectors).

Reliance on regional co-operation

- The success of certain elements, such as intelligence sharing, depends on active participation and trust among regional partners. Political or logistical barriers can limit collaboration.

No direct implementation role

- The toolkit is a guide and does not provide direct technical support or personnel for CERT establishment. Nations will need to rely on their own resources or external partnerships for implementation.

Rapidly evolving threat landscape

- Cybersecurity threats evolve rapidly, and the toolkit may require regular updates to stay relevant. Users must complement it with ongoing research and global best practices.

1.9. Tools and resources provided

- Templates for operational procedures, reporting and risk assessments.
- Best practices and case studies from African and global contexts.
- Strategies for securing funding and long-term sustainability.

2. The Computer Emergency Response Team (CERT)

CERT stands for 'Computer Emergency Response Team'. A CERT is a group of experts organised to handle and respond to cybersecurity incidents, threats and vulnerabilities. These teams work to improve the security and resilience of computer systems and networks.

2.1. Definition

A CERT is a specialised team of professionals responsible for identifying, managing and mitigating cyber risks, responding to incidents, and preventing future attacks. They often operate within organisations, governments or national security frameworks.

2.2. Purpose of a CERT

- *Incident response:* A CERT provides rapid and effective solutions to mitigate the impact of cybersecurity incidents such as malware outbreaks, data breaches or DDoS (distributed denial-of-service) attacks.
- *Threat analysis:* It analyses and assesses potential threats and vulnerabilities to anticipate and prevent cyberattacks.
- *Co-ordination:* It acts as a central point for co-ordinating efforts between different stakeholders, such as organisations, law enforcement or other CERTs.
- *Education and awareness:* It promotes cybersecurity awareness and provides training or best practices to minimise vulnerabilities.
- *Resilience building:* It enhances the overall security posture of systems by recommending and implementing protective measures.

2.3. CERT classifications

i. **National CERTs**

National CERTs operate on a country-wide level (for example, US-CERT, CERT-EU, CERT-In, JP-CERT). Examples of national CERTs in Africa are shown in Table 2.1.

Table 2.1 Examples of national CERTs.

Country	National CERT
Ghana	The National CERT of Ghana
Kenya	Kenyan National Computer Security Incident Response Team
Mauritius	Mauritian National Computer Security Incident Response Centre
Nigeria	Nigeria Computer Emergency Response Team (ngCERT)
South Africa	South African Computer Security Incident Response Team
Tunisia	Tunisia Computer Emergency Response Team

ii. **Sectoral CERTs**

A sector-specific CERT focuses on sectors such finance, healthcare, telecommunications etc. A typical example is the NCA-CERT of Ghana.

The telecommunication sectoral CERT of Ghana was set up by the Ghana National Communications Authority (NCA), the communications industry regulator, to respond to incidents within the sector and provide a platform for information sharing to enhance the safety of the communications industry. The NCA-CERT has as its primary constituency, licensed operators within the communications sector and their subscribers.

NCA-CERT works with the national CERT to co-ordinate incidents within the communications sector. The authority is expected to work with its constituents to infuse cybersecurity best practices into its regulatory and licencing regimes.

Another example is Nigeria's CERT structure, which includes:

- NCC-CSIRT (Computer Security Incident Response Team) – The sectoral CERT for the telecommunications sector, established by the Nigerian Communications Commission (NCC).

- NITDA-CERRT – The government sector CERT, set up by the National Information Technology Development Agency (NITDA).
- NFI-CERT/CBN-SOC – The financial sector CERT, responsible for co-ordinating incident response within Nigeria's financial sector.

These are just a few examples. Each of these sectoral CERTs collaborates with the national CERT (ngCERT) to ensure co-ordinated cybersecurity response, information sharing and sector-specific threat mitigation.

iii. **Organisational CERTs**

These are CERTs that are built to serve specific companies or institutions.

Table 2.2 shows the key functions of CERTs.

Table 2.2 Key functions of CERTs.

Function	Responsibilities
Incident response and mitigation	Detect, analyse and respond to cyber incidents such as malware outbreaks, data breaches and denial-of-service attacks. Minimise damage and downtime for affected organisations. Provide forensic analysis and post-incident reports.
Threat intelligence and early warning	Monitor cyber threats and provide real-time alerts on emerging vulnerabilities, exploits and attacks. Share intelligence with stakeholders (government agencies, businesses and international CERTs) to improve collective security. Maintain a national or sectoral cyber threat database.
Vulnerability-management	Identify and track vulnerabilities in critical systems and infrastructure. Issue security advisories and guidance for patching known vulnerabilities. Conduct risk assessments to prevent exploitation by malicious actors.
Cybersecurity awareness and training	Provide cybersecurity education, best practices and training programmes for businesses and the public. Develop guidelines on secure configurations, phishing awareness and cyber hygiene. Organise cybersecurity drills and exercises to improve preparedness.
Policy development and compliance	Assist in shaping national cybersecurity policies, laws and regulations. Ensure compliance with international security frameworks (for example, NIST [the National Institute of Standards and Technology], ISO [International Organization of Standardization] 27001, GDPR [the European Union's General Data Protection Regulation]). Act as an advisory body for government and private sector security strategies.
Co-ordination and collaboration	Act as a bridge between the public and private sectors for cybersecurity co-ordination. Work with law enforcement agencies to investigate cybercrimes. Participate in international cybersecurity forums and partnerships (the Forum of Incident Response and Security Teams [FIRST], the International Telecommunication Union [ITU], regional CERT networks).

Table 2.3 Key personnel roles in a CERT.

Role category	Position	Responsibilities
Executive leadership and management	CERT director / CISO	Provides strategic leadership, defines policies and engages with stakeholders.
	CERT operations manager	Oversees day-to-day operations, allocates resources and ensures operational readiness.
Incident response and threat management	Incident response team lead	Manages cyber incident response, containment and mitigation.
	Incident handle/ responder	Investigates security incidents, performs analysis and escalates cases as needed.
	Threat intelligence analyst	Monitors emerging threats, analyses hacker activities and shares intelligence.
Forensics and malware analysis	Digital forensics analyst	Conducts forensic investigations, collects digital evidence and supports legal inquiries.
	Malware analyst	Examines malware behaviour, identifies threats and develops countermeasures.
Security operations and monitoring	SOC analyst	Monitors security logs, analyses alerts, and detects potential cyber threats.
	Penetration tester (ethical hacker)	Simulates cyberattacks to identify vulnerabilities and recommend security improvements.
Risk and compliance	Cyber risk analyst	Assesses cyber risks, develops mitigation strategies and ensures security compliance.
	Policy and compliance officer	Ensures adherence to cybersecurity laws and regulatory frameworks.
Communications and public relations	Public relations/communications officer	Manages media relations, public advisories and government communications.
	Security awareness and training specialist	Develops training programmes and awareness campaigns to educate employees and stakeholders.
IT (information technology) and infrastructure support	Network security engineer	Secures network infrastructure, implements firewalls and mitigates threats.
	Systems administrator (security focused)	Manages IT systems, ensures patching and works with incident responders.
Research and development	Cybersecurity researcher	Conducts research on new threats, develops security tools and collaborates with academia.

2.4. Key personnel roles in a CERT

The key personnel roles in a CERT are shown in Table 2.3.

Other personnel include:

- Incident handlers
- Forensic analysts
- Cyber threat intelligence specialists
- Vulnerability management experts
- Security policy developers

2.5. Steps to developing a national CERT

A well-functioning CERT is a cornerstone of national and organisational cybersecurity strategy. However, establishing a national CERT or Computer Incident Response Team (CIRT) is a complex process that requires careful planning, collaboration and sustained commitment. To create an effective national CERT, technical and legal expertise – as well as national, organisational and diplomatic efforts – are required. Setting up a functional national CERT/ CIRT involves several critical steps. Table 2.4

Table 2.4 Steps to developing a national CERT.

Step	Key actions	Details
1. Planning and stakeholder engagement	Define objectives and scope	• Determine the primary objectives, such as incident detection, co-ordination and response. • Decide whether the CERT will serve government entities, the private sector or both. • Define the types of incidents the CERT will handle.
	Identify key stakeholders	• Government agencies (ministries of information and communication technology [ICT], defence, law enforcement, regulatory bodies). • Private sector (banks, telecom providers, utilities, healthcare, etc.). • International partners (FIRST, ITU, regional CERTs, cybersecurity alliances).
	Secure government support	• It is important to obtain endorsement and funding from national government bodies to ensure legitimacy and resource allocation.
	Legal and regulatory framework	• Develop policies that define the CERT's authority, responsibilities and operational boundaries. • Ensure compliance with national laws and international agreements.
2. Organisational and technical setup	Establish governance and funding	• Define governance structure, secure sustainable funding.
	Infrastructure and technology	• Set up secure facilities, deploy cybersecurity tools (SIEM [security information and event management], forensics, threat intelligence).
	Staffing and capacity building	• Hire cybersecurity experts, train staff, establish workforce development programmes.
3. Incident and threat management framework	Develop incident response procedures	• Establish standardised response processes (preparation, detection, containment, etc.).
	Threat intelligence and information sharing	• Partner with information sharing and analysis centres (ISACs), CERT networks and intelligence platforms for data sharing.
	Cybersecurity monitoring and early warning	• Implement national monitoring systems, conduct vulnerability assessments.
4. Public engagement and-collaboration	National cybersecurity awareness	• Educate the public and businesses on cybersecurity threats and best practices.
	Establish reporting and communication	• Set up hotlines, online reporting portals and public alerts.
	International co-operation	• Join global cybersecurity alliances, participate in cyber drills.
5. Testing, continuous improvement and sustainability	Conduct cyber drills and simulations	• Test response capabilities through national exercises.
	Performance metrics and reporting	• Define key performance indicators (KPIs), publish cybersecurity reports.
	Policy and framework updates	• Regularly update laws, policies and frameworks to adapt to new threats.

Table 2.5 Technical tools required by a CERT.

Category	Tools	Description	Examples
Incident detection	Intrusion detection systems (IDS)	Detect unauthorised access or malicious activities on networks.	Snort, Suricata
	Intrusion prevention systems (IPS)	Proactively block or mitigates threats detected by IDS.	Cisco Firepower, Suricata
	Network traffic analysis tools	Monitor and analyse network traffic for unusual patterns.	Zeek, Wireshark, ntopng
	Endpoint detection and response (EDR)	Provides continuous monitoring of endpoints to detect suspicious behaviour.	CrowdStrike, Carbon Black, SentinelOne
	Security information and event management (SIEM)	Centralised logging and real-time analysis of security events.	Splunk, IBM QRadar, LogRhythm
Threat intelligence	Threat intelligence platforms (TIPs)	Aggregate and correlate threat data from multiple sources.	ThreatConnect, Anomali, MISP, OpenCTI
	Malware analysis tools	Analyse malicious files and identify their functionality.	Cuckoo Sandbox, REMnux, VirusTotal
	Open-source intelligence tools (OSINT)	Gather publicly available information to track threats.	Maltego, Shodan, Recon-ng
Incident-analysis and response	Digital forensics tools	Investigate incidents, retrieve evidence and analyse compromised systems.	FTK Imager, EnCase, Autopsy
	Network forensics tools	Analyse captured network traffic to identify malicious behaviour.	Xplico, NetworkMiner
	Automated incident response tools	Automate tasks such as blocking internet protocols (IPs), quarantining files.	TheHive, Cortex, Demisto
	Case management systems	Track and manage ongoing cybersecurity incidents.	Jira (with plugins), Remedy, ServiceNow
Communication	Collaboration platforms	Real-time messaging platforms for incident co-ordination.	Slack, Microsoft Teams, Mattermost
	Secure communication tools	Ensure encrypted communication during incidents.	Signal, Wickr, PGP encryption
	Public notification systems	Issue alerts and advisories about cybersecurity threats.	Twitter, CERT websites, mailing lists
Vulnerability management	Vulnerability scanning tools	Identify security weaknesses in systems.	Nessus, OpenVAS, Qualys
	Patch management tools	Automate the process of patching vulnerabilities.	WSUS, SolarWinds Patch Manager, Ivanti
Data analysis and visualisation	Data analysis tools	Analyse security event data for insights.	Elasticsearch, Kibana, Splunk, Tableau,
	Visualisation tools	Visualise attack trends and anomalies.	Grafana, Gephi, Cyber Analyst

(*Continued*)

Table 2.5 Technical tools required by a CERT.

Category	Tools	Description	Examples
Automation and orchestration	SOAR platforms	Automate workflows for handling incidents.	Palo Alto Cortex XSOAR, Swimlane, Splunk Phantom
	Runbook automation tools	Automate incident response procedures.	StackStorm, Runbook Automation (BMC)
Backup and recovery	Backup solutions	Ensure recovery of data after an incident.	Veeam, Acronis,-BackupExec
	Disaster recovery tools	Restore affected systems and data post-attack.	Zerto, Arcserve, Datto
Threat hunting	Threat hunting platforms	Search logs and data for potential cyberattacks.	Elasticsearch, MITRE ATT&CK, THF
	Behavioural analytics tools	Analyse system behaviour to detect anomalies.	Sumo Logic, Exabeam, Gurucul
Reporting and Documentation	Report generation tools	Create standardised reports for incidents.	Sumo Logic, IRRS
	Documentation management systems	Maintain incident records and resolutions.	Confluence,-SharePoint, Google Drive (secured)

provides a structured roadmap for establishing a national CERT.

Developing a national CERT involves a multistep process including planning, stakeholder coordination, legal empowerment, infrastructure deployment, and capacity building. These steps are emphasized in both ITU guidelines and the African Union's continental cybersecurity frameworks (ITU, 2021; African Union, 2014).

2.6. Case study

Development of Kenya's national KE-CIRT/CC

Mandate and establishment

The Kenya Information and Communications Act mandates the development of a national cybersecurity management framework. In alignment with this, the national Kenya Computer Incident Response Team Coordination Center (KE-CIRT/CC) was established as a multi-agency collaboration framework responsible for co-ordinating cybersecurity efforts nationwide.

Key activities and initiatives

- *Incident resolution:* KE-CIRT/CC supports technical teams in resolving cyber incidents, follows up with local security teams and collects national statistics on cyber incidents.
- *Capacity building:* KE-CIRT/CC organises regular preparation exercises to build readiness and resilience against a wide range of cyber threats.
- *Collaboration:* KE-CIRT/CC engages with both international and local entities through threat intelligence sharing, exchange programmes and training to strengthen its incident response capabilities.

Resource requirements

- *Human resources:* KE-CIRT/CC established a team of cybersecurity experts, which includes roles such as incident responders, analysts and forensic specialists.
- *Technological infrastructure:* For instance, KE-CIRT/CC modernised its web portal, communication platforms and incident co-ordination tools to enhance its operations.
- *Training and development:* Continuous training programmes are vital to keep the team updated on emerging cyber threats and response techniques.

Process and steps involved

- *Assessment and planning:* Develop a plan outlining the objectives, scope and resources required for the CERT establishment.

Table 2.6 Key legal and policy elements.

Framework	Role	Example
National cybersecurity strategy:	Integrate CERT roles and responsibilities into a national strategy.	South Africa's National Cybersecurity Policy Framework. Ghana's National Cybersecurity Policy and Strategy.
Legal mandate:	Grant CERTs authority through legislation or executive orders.	Kenya's KE-CIRT/CC by Act of Parliament Ghana's NITA-CERT by Electronic Communications Act, 2008 Mauritius CERT-MU by ICTA Act Tunisia's TunCERT by Ministerial Decision

- *Legal and regulatory framework:* In Kenya's case, the formation of KE-CIRT/CC was facilitated through the Kenya Information and Communications Act, CAP 411A, as amended by the Kenya Information and Communication (Amendment) Act, 2014.
- *Infrastructure development:* Kenya set up the necessary technological infrastructure, including secure communication channels, incident tracking systems and data analysis tools.
- *Team formation:* KE-CIRT/CC recruited and trained personnel with expertise in various aspects of cybersecurity, including incident detection, analysis and response.
- *Stakeholder engagement:* KE-CIRT/CC has established collaboration mechanisms with international and local entities through threat intelligence sharing, exchange programmes and training to strengthen the incident response function.
- *Continuous improvement:* KE-CIRT/CC carries out regular assessments to refine processes, update training programmes and adapt to evolving cyber threats.

2.7. Technical tools required for a national CERT operations centre

To establish a fully functional CERT (Computer Emergency Response Team) or CIRT (Computer Security Incident Response Team), a robust technical infrastructure is essential. CERTs need a range of tools to support their operations, including detection, analysis, response and communication.

National cybersecurity strategies and legal mandates are essential for formalising CERT roles and responsibilities, ensuring they are integrated into national frameworks and empowered through appropriate legislation (ITU, 2021). Integrating CERTs into national cybersecurity strategies and granting them legal mandates are crucial steps many African countries have taken to institutionalise their cybersecurity response structures (ITU, 2021; Republic of Kenya, 2010; Government of Ghana, 2008).

Table 2.5 outlines the essential technical tools required for a fully functional CERT, categorised based on their purpose in cybersecurity operations.

2.8. Legal and regulatory requirements

Establishing a strong legal and regulatory foundation is critical for a CERT's success, particularly in the African context where cybersecurity threats are growing, but regulatory frameworks often lag. Below are sample policies and legal frameworks tailored to the needs of African nations or organisations seeking to establish or strengthen their CERTs.

2.8.1. Legal and policy foundations

A CERT requires a clear mandate, authority and responsibilities enshrined in national policies or organisational frameworks (Table 2.6).

2.8.2. Sample policy objectives

- Protect critical infrastructure: Legal frameworks should prioritise securing essential services (for example, energy, banking, healthcare).
- Incident reporting obligations: Organisations should be mandated to report cybersecurity incidents to the CERT.

Table 2.7 Policy components.

Description	Examples	Key elements	Recommendations
Confidentiality and anonymity	Protect reporting- entities' identity and data	Specify penalties for unauthorised disclosure	Confidentiality- agreements
Collaboration- incentives	Encourage voluntary reporting	Include non-punitive- policies for private- organisations	Safe harbour provi sions
Data protection and privacy laws	Align with national and regional data protection laws	African Union Convention on Cybersecurity and- Personal Data Protection	Define data collection policies, ensure privacy compliance
Cybercrime legislation	Mauritius Cybercrime Act (2021), Nigeria Cybercrimes Act (2015)	Define cybercrime offenses and penalties	Include hacking, iden tity theft, support law enforcement
Critical infrastruc ture protection	South Africa's Protection of Critical Infrastructure Act (2019)	Implement sector-specific standards and risk- assessments	Require regular risk assessments
Public–private- collaboration	Facilitate information sharing and joint- exercises	Enable two-way threat intelligence sharing,- protect proprietary- information	Limit liability for shared information
Cybersecurity- standards and- compliance	Adopt international standards like ISO/IEC 27001	Require compliance with standards as part of regulations	Use CERTs for guid ance and- assessment
Enforcement and penalties	Impose penalties for non-compliance	Specify fines or operational restrictions for- failure to report incidents	Criminalise interference with CERT operation

- International co-operation: Provisions should be included for cross-border collaboration in combating cyber threats.

2.8.3. Incident reporting and information sharing policies

Every CERT should create a structured policy for how incidents are reported, documented and acted upon.

Policy components

Table 2.7 highlights the incident reporting policy components that should be considered.

Sample legal clauses

Incident reporting clause:

'All organizations operating critical infrastructure must report cybersecurity incidents to the National CERT within 24 hours of detection. Failure to comply will result in penalties of up to $10,000.'

Data protection clause:

'The CERT shall ensure all collected data are encrypted, anonymised where applicable, and only used for purposes outlined in this policy.'

Collaboration clause:

'Private sector entities are encouraged to share threat intelligence with the CERT. Data shared under this clause will be protected under confidentiality agreements.'

3. Key CERT Functions

3.1. Incident management

Cyberattacks are increasingly becoming a significant concern across Africa, with both their frequency and complexity on the rise. These attacks are inflicting greater damage and disrupting essential systems. Cybersecurity incidents targeting critical national infrastructure, such as power grids, healthcare and financial services, can have far-reaching effects on the delivery of government services, particularly in developing regions. A swift and effective response to such incidents is crucial to maintaining the stability and continuity of government operations. Establishing a robust incident response framework is vital to detecting and addressing incidents quickly, minimising damage, addressing vulnerabilities exploited by attackers, and restoring normal services.

In many African nations, where technological infrastructure is still evolving, critical systems must be resilient enough to operate during an attack and recover rapidly to full functionality. This section outlines the responsibilities and actions of various stakeholders to ensure a co-ordinated, timely and effective response to cybersecurity threats with national consequences.

3.1.1. Roles and responsibilities of stakeholders in incident management

Key players

This section details the roles and responsibilities of stakeholders in managing and co-ordinating cybersecurity incidents.

The stakeholders include representatives from various public and private sector entities, including the critical sectors, all of whom are essential for a co-ordinated and effective response to cyber threats and incidents.

Cybersecurity committee

In the event of a national cyber crisis, the cybersecurity committee will be chaired by '*as per applicability in each country*' and shall consist of permanent and extended members. The composition of the committee shall be as follows:

The key responsibilities of the national cybersecurity committee include oversight and evaluating the effectiveness of CERT performance.

3.1.2. National Cybersecurity Incident Response Team (nCSIRT)

The National Cybersecurity Incident Response Team (nCSIRT) plays a critical role in managing and responding to cybersecurity incidents that threaten national security, public safety or the economy. Its responsibilities are vital for ensuring a co-ordinated, timely and effective reaction to cyber threats. The key functions of a nCSIRT may include the following, in accordance with the FIRST Service Framework:

1. ***Incident detection and monitoring:*** The nCSIRT is responsible for monitoring national networks and systems to detect potential cybersecurity incidents. This includes gathering and analysing data on threats and vulnerabilities to ensure early identification of incidents.
2. ***Incident assessment and prioritisation:*** Once a cyber incident is detected, the team assesses its severity, scope and potential impact. The nCSIRT prioritises incidents based on their potential to affect national security, critical infrastructure and public safety.
3. ***Co-ordinated incident response:*** The nCSIRT co-ordinates response efforts across government agencies, critical sectors, law enforcement and private sector organisations. This ensures that responses are aligned, resources are efficiently utilised and there is a unified approach to mitigating the incident.
4. ***Incident mitigation and containment:*** The team works to contain the spread of the cyber incident, prevent further damage and neutralise the threat. This includes shutting down affected systems, isolating compromised networks, and applying patches or other countermeasures.
5. ***Investigation and analysis:*** The nCSIRT investigates the cause and impact of cybersecurity incidents. This includes determining how the attack occurred, which

vulnerabilities were exploited and identifying the perpetrators when possible. The team gathers evidence for potential legal or law enforcement action.

6. ***Recovery and restoration:*** After a cyber incident, the nCSIRT supports efforts to restore systems, services and operations as quickly as possible. This involves ensuring that affected critical infrastructure and services are fully operational again, while minimising downtime and further disruptions.
7. ***Public communication and information sharing:*** The nCSIRT is responsible for communicating with the public, stakeholders and relevant organisations about ongoing incidents. It also ensures that critical cybersecurity information, including threat intelligence, is shared between relevant parties for better national defence.
8. ***Reporting and documentation:*** After an incident is handled, the nCSIRT prepares detailed reports outlining the incident's timeline, impact, response actions and lessons learned. These reports are used for improving future responses and shaping national cybersecurity policies.
9. ***Collaboration with international partners:*** Given the global nature of cyber threats, the nCSIRT often collaborates with international cybersecurity teams, agencies and organisations. This collaboration involves sharing intelligence, resources and best practices to combat cybercrime and cyber threats more effectively.

It is recommended that a National Cybersecurity Incident Response Team (nCSIRT) clearly define the services it would offers to its constituents and formally document them in a publicly available RFC 2350 profile. The National Cybersecurity Incident Response Team is the central body responsible for managing and co-ordinating responses to major cybersecurity incidents, ensuring the protection of critical national infrastructure, the recovery of services and the overall security of the nation's digital landscape.

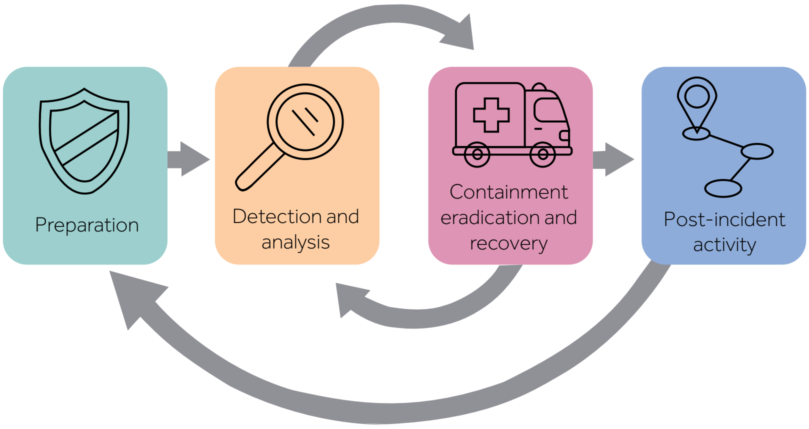
3.1.3. Cyber incident response life cycle

Preparation

Preparation in the incident response (IR) phase refers to the actions taken before an actual security incident occurs, ensuring an organisation is ready to respond effectively when one does. This phase involves:

1. ***Developing an incident response plan:*** Creating a documented strategy for handling various types of security incidents.
2. ***Establishing an incident response team (IRT):*** Assigning roles and responsibilities to team members with expertise in different areas (for example, security, IT, legal).

Figure 3.1 Cyber Incident Response Life Cycle [1].



[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3. ***Training and awareness:*** Conducting regular training and simulations for staff to recognise and properly report potential incidents.
4. ***Tool and resource setup:*** Ensuring necessary tools, technologies and resources (for example, logging systems, forensic tools) are in place and accessible.
5. ***Defining communication channels:*** Establishing clear communication protocols within the organisation and with external stakeholders (for example, vendors, law enforcement).

Preparation helps ensure the organisation can quickly identify, contain and recover from security incidents with minimal impact.

Detection and analysis

Detection and analysis in the incident response (IR) phase involves identifying and evaluating potential security incidents to determine their scope, impact and severity. This phase includes:

1. ***Detection:*** Continuously monitoring systems, networks and security logs to identify unusual activities or potential threats using tools like intrusion detection systems (IDS) or security information and event management (SIEM) systems.
2. ***Incident triage:*** Prioritising incidents based on their severity and potential impact, distinguishing between false positives and real threats.
3. ***Analysis:*** Investigating the incident to understand its nature, cause and potential consequences. This involves gathering evidence, preserving logs and conducting forensic analysis to assess the full scope of the incident.

The goal of this phase is to quickly confirm an incident, accurately assess its impact and initiate appropriate responses.

Incident classification

Table 3.1 shows the ENISA (European Union Agency for Cybersecurity) Incident Classification[2] Taxonomy, which could be used as reference for ease of identification and handling. Each incident category may require different mechanisms to handle and contain.

Incident prioritisation

Apart from incident classification, it is also important to determine the impact and urgency of a security incident. This helps an organisation to prioritise its response efforts, allocate resources efficiently and manage the potential risks associated with different types of incidents. In this regard, severity levels are typically assigned to the incidents based on factors like the potential damage to systems, data, operations or reputation, as well as the urgency with which the incident needs to be addressed. Table 3.2 presents an example of the different severity levels that can be assigned to an incident.

Containment, eradication and recovery

Containment, eradication and recovery in the incident response (IR) phase focuses on managing and mitigating the impact of an incident after detection and analysis. These steps include:

1. ***Containment:*** Taking immediate actions to limit the spread and impact of the incident, such as isolating affected systems, blocking malicious network traffic or shutting down compromised services. Containment can be short term (quick fixes to stop immediate damage) and long term (sustained actions to ensure the threat doesn't recur).
2. ***Eradication:*** Removing the root cause of the incident, such as deleting malware, closing vulnerabilities, and eliminating any backdoors or compromised accounts to prevent the attacker from regaining access.
3. ***Recovery:*** Restoring affected systems and services to normal operations, ensuring that no traces of the incident remain. This involves recovering data from backups, patching systems and carefully monitoring for signs of reinfection.

The goal of this phase is to stop the incident's progression, eliminate threats, and restore systems to a secure and functional state.

Post-incident activity

Post-incident activity in the incident response (IR) phase focuses on learning from the incident to improve future responses and strengthen security.

[2] https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf

Table 3.1 Incident classification.

Incident classification	Incident examples	Description
Abusive Content	Spam	or "Unsolicated Bulk Email", this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content
	Harmful Speech	Discreditation or discrimination of somebody (e.g. cyber stalking, racism and threats against one or more individuals)
	Child/Sexual/Violence/...	Child pornography, glorification of violence, ...
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialler	
	Rootkit	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also Some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social engineering	Gathering infomation from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerablllties wlth a standardised identifier such as CVE name (e.g. buffer overflow, backdoor, cross site scripting, etc.).
	Login attempts	Multiple login attempts (Guessing/ cracking of passwords, brute force).
	New attack signature	An attempt usinp an unknown exploit.

(Continued)

Table 3.1 Incident classification (*Continued*).

Incident classification	Incident examples	Description
Intrusions	Privileged account compromlse	A successful compromise of a system or appllcatlon (service). This can have been caused remotely by a known or new vulnerability, but also by an unauthorized local access. Also includes being part of a botnet.
	Unprivileged account compromise	
	Application compromise	
	Bot	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. DoS examples are ICMP and SYN floods, Teardrop attacks and mail-bombing. DDoS often is based on DoS attacks originating from botnets, but also other scenarios exist like DNS Amplification attacks. However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.) — or by Act of God, spontaneous failures or human error, without malice or gross neglect being involved.
	DDoS	
	Sabotage	
	Outage (no malice)	
Information Content-Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthemore, attacks are possible that intercept and access information during transmission (wiretapping, spoofing or hijacking). Human/configuration/software error can also be the cause.
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Offering or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
	Phishing	Masquerading as another entity in order to persuade the user to reveal a private credential.
Vulnerable	Open for abuse	Open revolvers, world readable printers, vulnerability apparent from Nessus etc scans, virus signatures not up-to-date, etc
Other	All incidents which do not fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
Test	Meant of testing	Meant of testing

Table 3.2 Incident prioritisation.

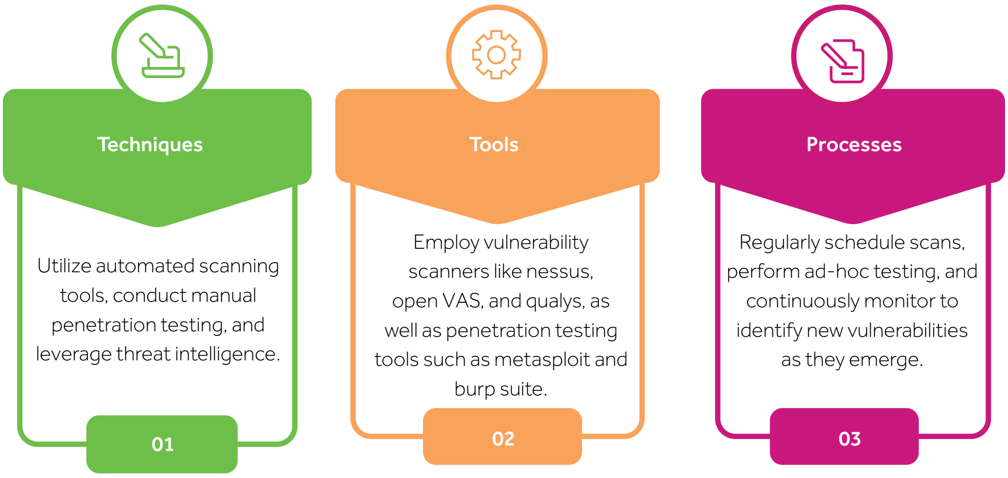
Severity level	Description	Impact	Response time	Example
Severity 1 (Critical)	High-impact incident with immediate and severe consequences, requiring urgent response.	Major operational disruption, data breach or critical systems compromised. Could affect business continuity or cause legal/regulatory-consequences.	Immediate (response within minutes to hours).	Ransomware attack encrypting critical business data; major breach of customer data.
Severity 2 (High)	Significant incident with moderate impact, causing some disruption but not critical to operations.	Significant service degradation, partial system failure or unauthorised access with potential for escalation.	Response within hours to a few hours.	Major vulnerability exploitation leading to partial system compromise; DoS attack affecting a key service.
Severity 3 (Medium)	Moderate impact incident that may cause some inconvenience but does not pose an immediate risk to critical systems or data.	Limited system compromise, service degradation or unauthorised access that does not result in substantial damage.	Response within hours to 1–2 days.	Phishing attack with successful credential capture; malware detection on non-critical systems.
Severity 4 (Low)	Minor incident with minimal impact on business operations, requiring routine monitoring or administrative actions.	Low risk to system integrity or data, with no significant threat to operations or confidentiality.	Response within 1–2 days.	Low-level malware detection; minor unauthorised access attempt; configuration errors.
Severity 5 (Informational)	Non-critical incidents that do not pose a risk to security but are worth tracking for future improvements.	No immediate impact on operations or security. Incident is informational, providing insight into system performance or potential vulnerabilities.	No immediate response required.	False positive alerts; audit trail analysis; routine patch updates.

Incident classification is a critical function of CERTs, enabling the categorization of threats such as malware, social engineering, and unauthorized access based on standardised frameworks (ENISA, 2020; FIRST, 2018).

Incident prioritisation helps CERTs allocate response resources based on the severity, impact, and urgency of incidents, ranging from critical ransomware attacks to low-risk configuration errors (NIST, 2012). This phase includes:

1. ***Root cause analysis:*** Conducting a thorough investigation to understand how the incident occurred, the vulnerabilities exploited and why existing defences failed.
2. ***Reporting and documentation:*** Documenting the incident's details, including actions taken, decisions made and lessons learned, to create a comprehensive incident report.
3. ***Review and improvement:*** Analysing the response process to identify areas for improvement, such as gaps in the incident response plan, team performance or tools. This may lead to updates in policies, procedures and training.

Figure 3.2 Discovery and identification – steps[3].



Techniques

Utilize automated scanning tools, conduct manual penetration testing, and leverage threat intelligence.

01

Tools

Employ vulnerability scanners like nessus, open VAS, and qualys, as well as penetration testing tools such as metasploit and burp suite.

02

Processes

Regularly schedule scans, perform ad-hoc testing, and continuously monitor to identify new vulnerabilities as they emerge.

03

4. ***Communication:*** Sharing findings with stakeholders, including internal teams, regulatory bodies and external partners, as required, while ensuring compliance with legal and regulatory reporting obligations.

The goal of this phase is to improve preparedness, prevent similar incidents in the future and ensure continuous improvement in the organisation's security posture.

3.2. Vulnerability management

Vulnerability management is a systematic approach to identifying, assessing, prioritising and mitigating security weaknesses within an organisation's IT infrastructure. This guideline provides a comprehensive framework for managing vulnerabilities effectively, ensuring a robust security posture and minimising the risk of cyber threats.

3.2.1. Vulnerability lifecycle

The vulnerability life cycle outlines the stages a vulnerability goes through from discovery to remediation. The key stages include:

- **Discovery:** Identifying new vulnerabilities through various methods such as automated scanning and manual testing.
- **Assessment:** Evaluating the potential impact and exploitability of the discovered vulnerabilities.
- **Prioritisation:** Ranking vulnerabilities based on risk factors, including severity, asset value and threat landscape.
- **Remediation:** Implementing measures to fix or mitigate the vulnerabilities, such as applying patches or configuration changes.
- **Verification:** Ensuring that the remediation efforts have successfully addressed the vulnerabilities.

Vulnerability discovery and identification

Effective discovery and identification involve the steps shown in Figure 3.2.

Vulnerability classification and prioritisation

Classifying and prioritising vulnerabilities is crucial for effective management, with steps as follows:

- **Classification:** Categorise vulnerabilities based on factors such as severity, exploitability and potential impact.
- **Frameworks:** Use the Common Vulnerability Scoring System (CVSS) to standardise the assessment of vulnerabilities.
- **Prioritisation:** Adopt a risk-based approach that considers the value of affected assets, the likelihood of exploitation and the potential impact on the organisation.

Patch management and remediation

Patch management and remediation are essential for addressing vulnerabilities:

[3] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

- **Patch management:** Manage the process of applying software updates to fix vulnerabilities. This includes identifying available patches, testing them in a controlled environment and deploying them across the organisation.
- **Remediation:** Implement patches, configuration changes or other mitigations to resolve vulnerabilities. This may also involve temporary workarounds or compensating controls if immediate patching is not possible.

Continuous monitoring

Continuous monitoring ensures ongoing detection and management of vulnerabilities by maintaining vigilance to detect new vulnerabilities and changes in the threat landscape. This proactive approach helps organisations stay ahead of potential threats and respond quickly to emerging vulnerabilities. Methods for continuous monitoring include conducting regular scans, real-time monitoring and integrating threat intelligence feeds. This comprehensive visibility is achieved by using security information and event management (SIEM) systems, intrusion detection systems (IDS) and other monitoring tools, which collectively provide a robust security posture for the organisation.

3.3. Threat intelligence for a national CERT

'Threat intelligence' refers to the process of collecting, analysing and disseminating information about potential or actual cyber threats to enhance situational awareness and enable proactive defences. For a national CERT, threat intelligence plays a pivotal role in identifying, mitigating and preventing cybersecurity threats at the national, sectoral and organisational levels.

3.3.1. Objectives of threat intelligence

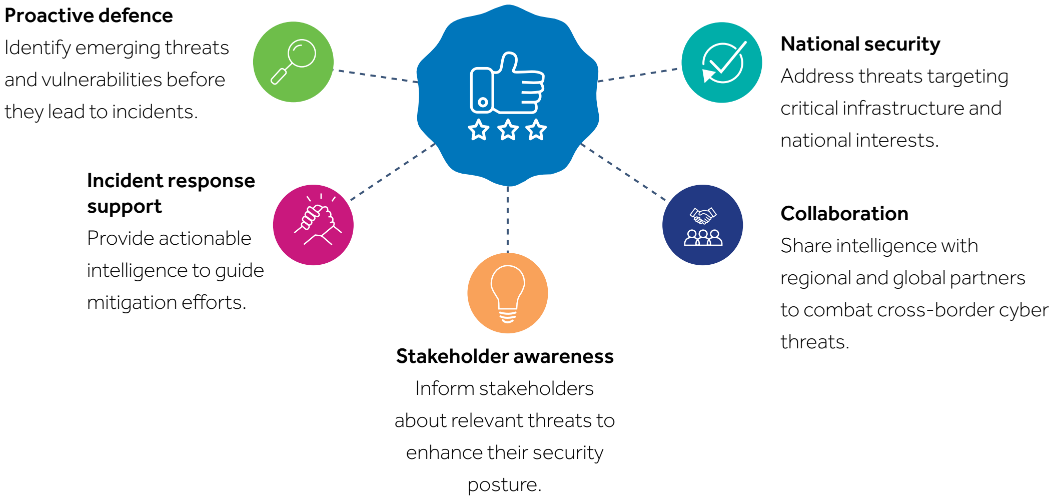
The objectives of threat intelligence are shown in Figure 3.3.

3.3.2. Types of threat intelligence

i. ***Strategic threat intelligence***

- **Definition:** High-level insights designed for executives and decision-makers to understand cybersecurity risks from a business and national security perspective.
- **Focus:** Trends, long-term risks and geopolitical threats.
- **Examples:**
  - cybercrime trends (for example, increase in ransomware-as-a-service);
  - nation-state actors' cyber strategies; and
  - reports on emerging threats to critical infrastructure.

Figure 3.3 Objectives of threat intelligence.



Proactive defence
Identify emerging threats and vulnerabilities before they lead to incidents.

National security
Address threats targeting critical infrastructure and national interests.

Incident response support
Provide actionable intelligence to guide mitigation efforts.

Collaboration
Share intelligence with regional and global partners to combat cross-border cyber threats.

Stakeholder awareness
Inform stakeholders about relevant threats to enhance their security posture.

ii. ***Tactical threat intelligence***

- **Definition:** Technical details about threats that help security teams defend against known attacks.
- **Focus:** Indicators of compromise (IOCs) that allow security teams to detect and block threats.
- **Examples:**
    - malware hashes (unique identifiers for malicious files);
    - IP addresses associated with cyberattacks;
    - phishing URLs used in recent attacks; and
    - domain names linked to malicious activities.

iii. ***Operational threat intelligence***

- **Definition:** Information about specific ongoing attacks, campaigns, or threat actors targeting an organisation or sector.
- **Focus:** Real-time intelligence used to respond to active threats.
- **Examples:**
    - details of a live distributed denial-of-service (DDoS) attack.
    - information on ransomware campaigns targeting a particular industry; and
    - reports on a hacking group's latest phishing techniques.

iv. ***Technical threat intelligence***

- **Definition:** Deep technical analysis of the tactics, techniques and procedures (TTPs) used by cybercriminals.
- **Focus:** Understanding how attackers operate to develop defences.
- **Examples:**
    - exploit kits that hackers use to target vulnerabilities.
    - malware behaviour analysis (for example, how a Trojan communicates with a command-and-control server); and
    - details on zero-day vulnerabilities.

3.3.3. The threat intelligence life cycle

The threat intelligence life cycle is a systematic process followed by a CERT to ensure relevant and actionable intelligence.

Direction

- Define intelligence requirements based on national priorities, critical infrastructure and stakeholder needs.
- Example: Focus on ransomware targeting healthcare systems.

Collection

Gather data from various sources, including:

- ***Internal sources:*** Incident reports, logs and forensic analysis.
- ***External sources:*** Open-source intelligence (OSINT), commercial feeds and intelligence-sharing platforms.
- ***Collaboration:*** Data from regional CERTs, law enforcement and international organisations.

Processing

- Organise raw data into usable formats (for example, parsing logs, filtering relevant data).

Analysis

- Assess the credibility, relevance and potential impact of threats.
- Use frameworks like the MITRE ATT&CK framework for mapping threat actor behaviour.

Dissemination

Share actionable intelligence with stakeholders through:

- threat reports, advisories and situational awareness bulletins; and
- real-time alerts and dashboards.

Feedback

- Collect feedback from stakeholders to refine intelligence requirements and processes.

3.3.4. Tools and platforms for threat intelligence

Threat intelligence platforms (TIPs)

- Examples: MISP (Malware Information Sharing Platform), ThreatConnect.

Open-source tools

- OSINT tools: Shodan, Maltego and theHarvester.
- IOC tools: VirusTotal, AbuseIPDB.

Threat feeds and frameworks

- Commercial feeds: Recorded Future, FireEye Threat Intelligence.
- Frameworks: MITRE ATT&CK, Diamond Model of Intrusion Analysis.

Automated systems

- Security information and event management (SIEM) systems for real-time threat correlation.
- Example: Splunk, QRadar.

3.3.5 Threat intelligence sharing

Effective sharing of threat intelligence ensures collective defence across sectors and borders.

Information sharing frameworks

- Establish a national threat intelligence exchange for trusted sharing among stakeholders.
- Utilise standardised formats like STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated Exchange of Indicator Information).

Various threat information sharing communities exists, such as:

- Forum of Incident Response Security Team MISP
- Africa CSIRT MISP
- ECOWAS ISAC

The core objectives of threat intelligence include proactive defense, incident response support, national security protection, cross-border collaboration, and raising stakeholder awareness, principles supported by leading frameworks from SANS, ENISA, MITRE, and Gartner (SANS Institute, 2020; ENISA, 2021; MITRE, 2023; Gartner, 2021).

It is recommended that nCSIRTs collaborate to share information across the different countries.

Stakeholder engagement

- Government: Share intelligence on threats to national security.
- Private sector: Provide tactical and operational intelligence to protect business operations.
- Regional/international partners: Collaborate through platforms like AfricaCERT and FIRST (the Forum of Incident Response and Security Teams).

Confidentiality and data protection

- Use non-disclosure agreements (NDAs) and classification levels to protect sensitive intelligence.

3.3.6. Threat Intelligence Use Cases

1. ***Proactive threat hunting:***

   Example: Using IOCs to detect advanced persistent threats (APTs) in critical infrastructure networks.

2. ***Vulnerability management:***

   Example: Advisories on zero-day vulnerabilities to guide patch management.

3. ***Incident analysis and response:***

   Example: Analysing ransomware behaviour to identify decryption keys.

Table 3.3 Challenges in threat intelligence.

Challenge	Mitigation strategy
Incomplete or low-quality data	Use multiple data sources and validate intelligence.
Lack of skilled analysts	Invest in capacity-building and training programmes.
Limited sharing due to trust issues	Implement strong confidentiality agreements and secure platforms.
High cost of commercial tools	Leverage open-source tools and international collaborations
Data privacy concerns	Anonymise data and comply with national data protection laws.

Figure 3.4 Threat intelligence effectiveness metrics.

Timeliness	Accuracy	Stakeholder engagement	Incident mitigation success	Collaboration metrics
How quickly is intelligence disseminated after detection?	Percentage of actionable intelligence without false positives.	Number of stakeholders utilising shared intelligence.	Reduction in incident impact due to early intelligence.	Frequency of intelligence-sharing with regional and global partners.

4. ***Security awareness training:***

   Example: Educating stakeholders on phishing campaigns targeting specific industries.

The challenges to threat intelligence are shown in Table 3.3.

3.3.7. Metrics for evaluating threat intelligence effectiveness

Measuring the effectiveness of threat intelligence is essential for ensuring that security teams get value from their intelligence efforts. Some of the key metrics that can be used to evaluate the impact and efficiency of a threat intelligence programme are illustrated in Figure 3.4. Additional metrics can be found in Appendix D.

3.3.8. Sample threat intelligence report template

See Appendix A for a CERT threat intelligence report template designed for CERT use. It includes all essential sections to ensure clarity, usability and actionability.

3.4. Training and exercises

In line with the objective of building Africa's cybersecurity resilience through capacity building, the *CERTs Toolkit* framework includes provisions for training and exercises aimed at building, maintaining and evaluating the capabilities of national and regional CERTs. A vibrant cyberspace, together with a skilled workforce, is a major catalyst to the digital economy, which in the long run leads to the development of a country's gross domestic product (GDP), national security and cyber resilience.

This section is designed to help CERT personnel develop the skills and preparedness necessary to effectively manage cybersecurity incidents. It focuses on improving knowledge, developing the requisite effective incident response skills, enhancing team co-ordination, reducing the response time in the event of incidents, and helping to meet compliance requirements.

3.4.1. training

CERTs should incorporate the use of modules which, among other things, have the benefit of flexibility, personalisation, reusability, scalability and standardisation, resulting in effective, efficient and engaging learning experiences.

Training modules

i. **Cybersecurity fundamentals**

   This module provides a comprehensive introduction to cybersecurity, covering the following key areas.

   - CERT mandate and national policies: An overview of the Computer Emergency Response Team (CERT) responsibilities and alignment with national cybersecurity strategies.
   - Core cybersecurity concepts: Introduction to the CIA triad (confidentiality, integrity, availability) as the foundation of cybersecurity principles.
   - *Threat landscape:* Exploration of network security and common cyber threats, including malware, ransomware, phishing and insider threats.
   - Best practices: Emphasis on strong password policies, regular software updates, encryption and access control measures.

- Frameworks: Overview of established frameworks like NIST Cybersecurity Framework and ISO 27001 for implementing robust security practices.

Operational training

This module focuses on enhancing both technical and non-technical skills in critical areas.

- Threat analysis: Techniques for identifying and analysing potential cyber threats using real-world scenarios.
- Vulnerability assessment: Hands-on training in identifying system weaknesses and recommending mitigation measures.
- Penetration testing: Practical exercises on simulating attacks to evaluate system defences.
- Digital forensics: Introduction to forensic tools and methods for investigating cyber incidents and preserving evidence.

Incident response

This module equips participants with the skills to manage cybersecurity incidents effectively.

- Incident management procedures: Step-by-step guidance for detecting, triaging and responding to incidents.
- Escalation protocols: Best practices for managing communication and decision-making during high-severity incidents.
- Remediation techniques: Strategies for containing threats, eradicating malicious activity and recovering systems post-incident.

Threat analysis

A specialised module designed to develop expertise in threat intelligence management.

- Threat identification techniques: Methods for recognising emerging threats through data analysis.
- Threat intelligence integration: Leveraging intelligence sources to enhance organisational security posture.
- Risk assessment skills: Evaluating potential risks based on identified threats and prioritising mitigation efforts.

ii. **CERT-specific practices:** Since CERTs are generally equipped with numerous tools including both software and hardware used in day-to-day operations, personnel should have thorough knowledge of their functionality and measures taken to secure them. Training should be on CERT tools such as SIEM systems, threat intelligence platforms, social media management systems and ticketing systems.

It is important for CERTs to be well versed with relevant national and international regulatory compliance and standards (for example, ISO 27001, GDPR, NIST). Also, the training should include standard operating procedures (SOPs) for incident handling, as needed by each specific CERT based on its mandate.

iii. **Cryptography:** Provides basics of cryptography and encryption, key management and secure communication protocols.

iv. **Cyber diplomacy:** Provides knowledge and skills necessary to become involved in international cyber diplomacy negotiations.

v. **Soft skills: Provides CERT personnel with attributes such as:**

- Communication and reporting: This should include effective communication and proper documentation skills, as effective incident handling involves multiple stakeholders. These should be designed to enhance collaboration, proper documentation of incidents and timely response.
- Team co-ordination and management.
- Training in effective collaboration in multi-disciplinary teams to work cohesively.
- Crisis-management, effective communication and public relations during incident handling.

3.4.2. Exercises and simulations

CERTs should incorporate exercises and simulation scenarios in training as they improve retention, enhance engagement, improve team co-ordination, develop critical thinking, improve learners' confidence, promote active learning and provide real world application, among other benefits. These may include:

- Tabletop exercises: To practically gauge team understanding using simulated discussion-based scenarios with a focus on the decision-making processes and communication strategies of the CERT personnel.
- Cyber range exercises: To provide hands-on cybersecurity training that simulates real-world attack scenarios in a safe environment. Cyber range exercises help CERTs improve their cybersecurity posture, identify vulnerabilities and advance their employees' skills.
- Red team/blue team exercises: Simulation scenarios (attack and defence) that help identify vulnerabilities, improve incident response, enhance collaboration, highlight gaps in security and develop awareness on potential attack vectors.
- 'Capture the Flag' (CTF) competitions: Cybersecurity challenges that simulate real-world scenarios to assess participants' cybersecurity knowledge. The objective of the assessment is to exploit the vulnerabilities in a system to capture a hidden piece of information symbolised by the 'flag'.

3.4.3. Recommended approach for training and exercise

- To maximise learning and application, it is essential that all training modules incorporate interactive segments. Interactive training tools and scenario-based exercises play a crucial role in reinforcing knowledge and preparing personnel to effectively handle cyber incidents.
- Training sessions can be conducted either in person or virtually, utilising a variety of platforms. However, it is important not to underestimate the value of regular on-site training and exercise sessions, which are vital for fostering team cohesion and facilitating in-depth technical discussions.
- Examples of interactive training tools include cybersecurity quizzes, cyber incident simulations, virtual cybersecurity labs and threat analysis workshops. These tools help create a dynamic learning environment that engages participants and enhances their readiness to respond to real-world cybersecurity challenges.

3.4.4. Other important considerations

- Customisation: Exercises should be tailored to align with specific threats, industries and team maturity levels, for example, 'Ransomware Outbreak Response', since ransomware is currently a global increasing threat and relatively new to Africa.
- Scalability: Scalable frameworks should be adopted such that they allow adaptation for small organisations or large national CERTs.
- Evaluation and feedback mechanisms: There should be post-exercise reviews to assess performance and identify improvement areas documented after the exercises and training, elaborating on the findings and recommendations.
- The establishment of key performance indicators (KPIs) for future benchmarking.
- Continuous improvement: With the dynamic nature of cyberspace, it is critical to ensure regular training updates based on evolving threat landscapes.
- Availability of necessary resources for the training and exercises.

4. Policy and Framework Resources

Establishing comprehensive policies and procedures is crucial for the effective operation of National Computer Emergency Response Teams (CERTs) in Africa. While specific templates tailored exclusively for African CERTs may be limited, several resources offer adaptable frameworks suitable for this context. Table 4.1 details the CERT services alongside associated policy areas for consideration.

Table 4.1 Policy and framework resources.

	CERT services	Policy areas
1	Incident response and management	• Incident reporting and disclosure: Guidelines for organisations and the public to report cybersecurity incidents. • Co-ordination and communication: Policy/guidelines for collaboration between CERTs, government, the private sector and international entities. • Crisis management: Guidelines for managing large-scale cyber incidents and national-level co-ordination.
2	Vulnerability management	• Vulnerability disclosure: Guidelines to establish responsible disclosure processes for reporting security flaws. • Patch management: Policy/guidelines to mandate timely application of security updates. • Critical infrastructure protection: Guidelines to safeguard essential systems against vulnerabilities.
3	Cyber threat intelligence sharing	• Information sharing protocols: Guidelines to ensure secure and effective exchange of threat intelligence. • Cross-border collaboration: Guidelines to enable regional and international sharing of cyber threat intelligence.
4	Capacity building and awareness	• Education and training: Guidelines to developing national programmes to train IT and cybersecurity professionals. • Public awareness: Campaigns to educate citizens and organisations on safe online practices.
5	Risk management	• Risk management: Policies to incorporate cybersecurity risks into broader organisational and national risk management.
6	Digital forensics and analysis	• Legal framework for evidence handling: Policies governing the collection, preservation and admissibility of digital evidence. • Cybercrime investigation: Guidelines for co-operation between CERTs and law enforcement.
7	Collaboration and co-ordination	• Inter-agency co-ordination: Guidelines to establish co-operation between CERTs, regulators and law enforcement. • Regional and international co-operation: Aligning with initiatives like AfricaCERT, ITU and the African Union's cybersecurity programmes. • Public–private partnerships: Guidelines to establish collaboration between CERTs and the private sector to enhance cyber resilience.

4.1. Policy and framework resources repository

The policy and framework resources repository provide a structured and centralised collection of key policies, guidelines and frameworks to support the mission of national CERTs in delivering effective cybersecurity services. See Appendix G.

Implementation considerations.

- Customisation: Adapt templates to reflect the specific legal, cultural and operational contexts of the respective African nation.
- Stakeholder engagement: Involve relevant stakeholders, including government agencies, private sector entities and civil society, to ensure comprehensive and applicable policies.
- Continuous improvement: Regularly review and update policies to address evolving cyber threats and incorporate lessons learned from incident responses.

By leveraging these resources and approaches, national CERTs in Africa can develop robust policies and procedures that enhance their cybersecurity posture and resilience.

5. Communication and Co-ordination Mechanism

A robust communication and co-ordination mechanism is critical for a National CERT to effectively manage cybersecurity incidents, collaborate with stakeholders and maintain public trust. Below is a detailed framework tailored to African contexts, emphasising inclusivity, transparency and scalability.

5.1. Objectives of the communication and co-ordination mechanism

The communication and co-ordination mechanism aims to:

- ensure timely and accurate sharing of information during cybersecurity incidents.
- facilitate collaboration among stakeholders, including government, the private sector, academia and international partners;
- promote public awareness of cybersecurity threats and mitigation strategies; and
- maintain a unified response to cybersecurity incidents at the national, sectoral and regional levels.

5.2. Stakeholders involved in communication and co-ordination

A CERT's communication network involves diverse stakeholders, each with specific roles and responsibilities:

Internal stakeholders

- *CERT staff:* Incident handlers, threat analysts and public relations officers.
- *CERT board:* Oversight body for strategic decision-making and crisis escalation.

External stakeholders

- *Government agencies:* Ministries of ICT, defence, interior and other relevant bodies.
- *Critical infrastructure operators:* Energy, finance, transportation, healthcare and telecommunications providers.
- *Private sector organisations:* Businesses, industry associations and internet service providers (ISPs).
- *Academia and research institutions:* For technical expertise and capacity building.
- *Civil society:* Advocacy groups and non-governmental organisations.
- *Regional and international partners:* African Union, ITU, regional CERTs and global cybersecurity organisations.

5.3. Components of the communication and co-ordination mechanism

5.3.1. Communication protocols

Incident reporting

All organisations operating critical infrastructure must report incidents to the CERT. The reporting mechanisms are depicted in Figure 5.1.

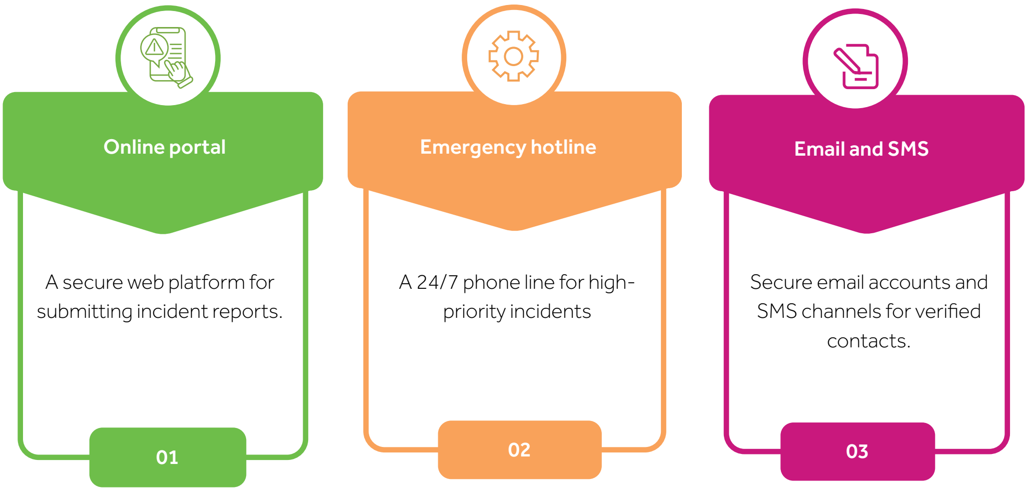
- Information should be disseminated through threat intelligence reports (periodic updates on emerging threats and vulnerabilities) and advisories and alerts (real-time notifications for critical vulnerabilities, malware or ongoing attacks).
- Situation reports (SITREPs) should be given - regular updates during major incidents or crises.

Escalation levels

Define escalation levels based on the severity of an incident:

- Level 1: Minor, localised incidents managed at the organisational level.
- Level 2: Sector-wide incidents requiring co-ordination with the CERT.

Figure 5.1 Incident reporting mechanisms.



Online portal

A secure web platform for submitting incident reports.

01

Emergency hotline

A 24/7 phone line for high-priority incidents

02

Email and SMS

Secure email accounts and SMS channels for verified contacts.

03

- Level 3: National-level incidents requiring cross-sector co-ordination and government intervention.

5.4. Communication tools and infrastructure

5.4.1. Incident management system (IMS)

This is a centralised software platform for tracking and managing cybersecurity incidents. Features include:

- automated ticketing for incident reports;
- real-time updates on incident resolution progress; and
- analytics and reporting capabilities.

5.4.2. Secure communication channels

- Virtual private network (VPN): Secure remote access for stakeholders.
- Encrypted email services: Protect sensitive information during communication.
- Collaboration platforms: Tools like Slack or Microsoft Teams with enhanced security settings.

Table 5.1 shows the co-ordination mechanisms.

Table 5.1 Co-ordination mechanisms.

Mechanism	Description	Key activities	Examples
National cybersecurity co-ordination centre (NCCC)	Centralised co-ordination of cybersecurity activities.	Convenes stakeholder meetings, facilitates information sharing	CERT as hub for NCCC
Sector-specific CERTs	Collaborates with sectoral CERTs to address industry-specific threats.	Shares technical expertise and sectoral threat intelligence	Finance, energy, healthcare, telecommunications
Public–private partnerships (PPPs)	Establishes formal agreements for information sharing and joint incident response.	Conducts joint cybersecurity drills and tabletop exercises	Formal agreements with private entities
Regional and international co-operation	Participates in regional CERT forums and collaborates with international partners.	Addresses cross-border threats, accesses advanced threat intelligence	AfricaCERT, FIRST, international partnerships

Table 5.2 Challenges and mitigation strategies.

Challenge	Mitigation strategy
Lack of trust in information sharing	Establish confidentiality agreements and safe harbour policies
Limited technical infrastructure	Seek funding and support from international partners
Ineffective public communications	Employ skilled public relations officers and media consultants
Language barriers	Provide multilingual communication resources
Co-ordination with multiple stakeholders	Use a centralised co-ordination platforms and clear escalation paths

Cybersecurity implementation in developing regions often faces challenges such as limited infrastructure, coordination difficulties, and language barriers, which require context-appropriate mitigation strategies including capacity development, multilingual resources, and stakeholder coordination frameworks (ITU, 2020).

5.4.3. Threat intelligence sharing platforms

- Facilitate the sharing of indicators of compromise (IOCs), malware signatures and threat actors' tactics.
- Example: Integration with platforms like MISP (Malware Information Sharing Platform).

5.4.4. Communication strategies

Public awareness and engagement

Public advisories

- Issue easy-to-understand alerts about current threats and mitigation steps.
- Use social media, radio and television for wide reach.

Cybersecurity campaigns

- Conduct national awareness campaigns during events like Cybersecurity Awareness Month.
- Focus on topics like phishing, ransomware and secure online practices.

Community engagement

- Partner with local organisations to raise awareness in underserved areas.
- Provide multilingual resources to ensure inclusivity.

5.5. Crisis communication

Pre-incident planning

- Develop a crisis communication plan (CCP) outlining roles, responsibilities and communication channels.
- Conduct regular training and simulations.

During an incident

- Activate a joint information centre (JIC) to manage media inquiries and public communication.
- Deliver regular updates to stakeholders and the public through press releases and social media.

Post-incident review

- Publish an incident report summarising key actions, lessons learned and recommendations.
- Engage stakeholders in a post-incident debriefing session.

5.5.1. Challenges and mitigation strategies

Table 5.2 shows the challenges and mitigation strategies

5.5.2. Key performance indicators (KPIs)

Measure the effectiveness of communication and co-ordination mechanisms using the following KPIs:

- Incident response time: Average time to acknowledge and resolve reported incidents.
- Stakeholder participation: Number of stakeholders actively engaged in CERT activities.
- Public awareness metrics: Reach and engagement levels of cybersecurity campaigns.
- Collaboration levels: Frequency and quality of interactions with regional and international partners.

6. Conclusion

The CACF *CERTs Toolkit* serves as a vital resource for advancing cybersecurity resilience across Africa. As the digital landscape rapidly expands, so too do the threats that challenge the security of critical infrastructure, services and national stability. This toolkit provides a structured, context-aware framework to support the establishment and enhancement of Computer Emergency Response Teams (CERTs) across the continent.

Rooted in collaboration, practical experience and global best practices, the toolkit equips policy-makers, practitioners and institutions with the tools needed to build effective CERT capabilities. It addresses key areas such as incident response, threat intelligence, capacity building, legal and regulatory alignment, and inter-agency co-ordination, enabling nations to respond swiftly and effectively to cyber threats.

More than just a technical guide, the CACF *CERTs Toolkit* reflects the Commonwealth's vision of a secure, co-operative and digitally empowered Africa. By fostering local capacity, encouraging regional collaboration and promoting sustainable planning, it lays a strong foundation for safeguarding Africa's digital future.

Bibliography

This toolkit draws upon recognised international frameworks, standards, and resources to provide comprehensive guidance on the development and operationalization of Computer Emergency Response Teams (CERTs) across Africa. The following references have are recommended for further reading and alignment:

AfricaCERT. (n.d.). Africa Computer Emergency Response Team. https://www.africacert.org/

African Union. (2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Cichonski, P., T. Millar, T. Grance and K. Scarfone. "Computer Security Incident Handling Guide" Computer Security Incident Handling Guide 2, no. 2 (August 2012). https://doi.org/10.6028/nist.sp.800-61r2.

Commonwealth Heads of Government Meeting. (2018). Commonwealth Cyber Declaration. https://thecommonwealth.org/our-work/commonwealth-cyber-declaration

Economic Community of West African States (ECOWAS). (2019). ECOWAS Regional Cybersecurity Framework and Strategy.

European Union Agency for Cybersecurity (ENISA). (n.d.). Incident Classification Taxonomy. https://www.enisa.europa.eu/

FIRST (Forum of Incident Response and Security Teams). (n.d.). FIRST Service Framework. https://www.first.org/

Incident Classification Taxonomy Task Force Status and Way Forward, 2018. https://www.enisa.europa.eu/sites/default/files/publications/WP2017 2O0-3-1-1 Good practice guide on how to improve CSIRT capabilities.pdf.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO.

International Telecommunication Union (ITU). (2023). Global Cybersecurity Index (GCI) Reports. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

MISP Project. (n.d.). Malware Information Sharing Platform & Threat Sharing. https://www.misp-project.org/

MITRE Corporation. (n.d.). MITRE ATT&CK Framework. https://attack.mitre.org/

National Institute of Standards and Technology (NIST). (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce. https://www.nist.gov/cyberframework

Appendices

Appendix A: Sample threat intelligence report template

Below is a template for a threat intelligence report, tailored for use by a CERT. It includes all key sections to ensure clarity, usability and actionability.

National CERT Threat Intelligence Report

Report ID: TI-[Year]-[Number]

Date Issued: [Insert Date]

Report Classification: [Confidential/Public/Internal Use Only]

Prepared By: [CERT Name]

Contact Information: [Email, Phone, Website]

1. Executive summary

Purpose:

Provide a brief overview of the report, highlighting the most critical information, including key threats, affected sectors and recommended actions.

Summary:

- **Threat actor(s):** [Name or type of threat actor, for example, 'Unknown ransomware group.']
- **Threat type:** [For example, ransomware, phishing campaign, malware attack.]
- **Impact level:** [For example, High/Medium/Low.]
- **Affected sectors:** [For example, healthcare, energy, financial institutions.]
- **Recommended actions:** [For example, patch systems, enable multi-factor authentication.]

Indicators of Compromise (IOCs) such as file hashes, IP addresses, domain names, registry keys, and email subjects are essential for identifying and mitigating cyber threats (MITRE, 2023).

2. Threat description

- Provide detailed information about the threat.
- Threat name: [For example, 'Clop Ransomware.']
- Threat type: [For example, malware, distributed denial-of-service (DDoS).]
- First identified: [Date and source.]
- Observed activity:
- What happened?
- Where? (geographical location, network or systems affected).
- When?

3. Technical analysis

Indicators of compromise (IOCs):

Provide specific technical details stakeholders can use to identify threats in their environment (Table A1).

Technical details:

- Malware behaviour: [For example, encrypts files and demands ransom payment.]
- Delivery method: [For example, exploits unpatched vulnerabilities in email servers.]
- Exploitation tools Used: [For example, 'Metasploit framework.']
- Attack tactics and techniques (MITRE ATT&CK).
- Initial access: [For example, spear phishing (T1566).]
- Privilege escalation: [For example, exploit public-facing applications (T1190).

Table A1 Example indicators of compromise (IOCs).

Indicator type	Value	Description
File hash (MD5/ SHA-256)	Example12345abcdef67890	Malware file hash.
IP address	192.168.1.100	Command-and-control server.
URL/ domain	Maliciousdomain.com	Phishing site.
Registry key	HKEY_LOCAL_MACHINEIexample	Malware persistence mechanism.
Email subject	Subject Example	Phishing email subject.

4. Impact assessment

Affected sectors:

- List industries or organisations targeted by the threat.
- Mention any critical infrastructure affected.

Potential impact:

- Operational impact: [For example, downtime, disrupted services.]
- Data loss: [For example, compromise of sensitive customer data.]
- Financial impact: [For example, costs of ransomware payments or mitigation efforts.]
- Reputational impact: [For example, loss of public trust.]

Geographical scope:

- Specify whether the threat is localised, national or regional.

5. Recommendations

- Provide actionable steps stakeholders can take to mitigate the threat.

Short-term actions:

1. Isolate infected systems immediately.
2. Block the identified malicious IP addresses and domains.
3. Update and apply patches for the vulnerabilities exploited.
4. Monitor network activity for IOCs listed in this report.

Long-term actions

1. Implement multi-factor authentication (MFA).
2. Conduct employee awareness training on phishing campaigns.
3. Review and update incident response plans.
4. Collaborate with CERT to share threat-related insights.

6. Threat actor profile (if applicable)

- Name or alias: [For example, 'APT29', 'Unknown actor.']
- Motivation: [For example, financial gain, espionage.]
- Targeting: [for example, government entities, critical infrastructure.]
- Previous campaigns: [For example, known incidents attributed to this actor.]
- Tactics, techniques and procedures (TTPs):
- Summarise observed patterns of behaviour.

7. Threat timeline

Provide a chronological summary of the threat's development (Table A2).

8. Regional and global context

Describe how this threat fits into the broader cybersecurity landscape:

- Is it part of a global campaign?
- Are there similar incidents reported in the region?

9. Appendices

Include supplementary material:

- **Glossary:** Define technical terms used in the report.
- **References:** List sources of threat data, for example, OSINT, commercial feeds.
- **Incident reporting form:** Provide a template for stakeholders to report incidents to CERT.

10. Contact Information

National CERT contact details:

- Email: [insert email address]
- Phone: [insert phone number]
- Website: [insert URL]

Feedback and collaboration:

- Request feedback on the report.
- Provide instructions for sharing additional intelligence.

Maintaining a threat timeline is a crucial part of incident handling, enabling CERTs to track key events from detection to stakeholder communication for effective response coordination (NIST, 2012).

Table A2 Threat timeline.

Date	Event
Insert date	Threat first detected by CERT.
Insert date	Observed malicious activity targeting banks.
Insert date	IOCs shared with stakeholders.

Appendix B: Legal framework template for a national CERT in Africa

Below is a comprehensive legal document template that establishes the mandate, functions and governance of a National CERT in Africa. This template is tailored to align with the unique challenges and opportunities within the African context.

[Country Name] National CERT Act

An Act to establish the National Computer Emergency Response Team (CERT), provide for its mandate, governance and operations, and promote cybersecurity resilience in [Country Name].

Part I: Preliminary

Section 1: Short Title and Commencement

This Act may be cited as the [Country Name] National CERT Act, [Year] and shall come into operation on [date of enactment].

Section 2: Definitions

In this Act:

CERT: Refers to the National Computer Emergency Response Team.

Cybersecurity incident: Any event compromising the confidentiality, integrity, or availability of digital systems or data.

Critical infrastructure: Assets essential for national security, public safety or economic stability.

Stakeholders: Includes government agencies, private organisations, academia, civil society and international partners.

Incident reporting: The act of notifying the CERT of a cybersecurity breach or threat.

Part II: Establishment of the National CERT

Section 3: Establishment of the CERT

1. The [Country Name] National CERT is hereby established as the national authority for cybersecurity incident response.
2. The CERT shall function as an independent entity under the supervision of the Ministry of Information and Communication Technology (ICT).

Section 4: Objectives of the CERT

The objectives of the CERT are:

1. To enhance the nation's cybersecurity resilience.
2. To co-ordinate responses to cybersecurity incidents.
3. To foster collaboration among national and international stakeholders.
4. To promote cybersecurity awareness and capacity building.

Section 5: Functions of the CERT

The CERT shall:

1. Monitor, detect, and respond to cybersecurity threats and incidents.
2. Provide guidance on best practices for cybersecurity.
3. Collect, analyse and disseminate threat intelligence.
4. Develop and enforce cybersecurity standards for critical infrastructure.
5. Facilitate information sharing among stakeholders.
6. Conduct training, awareness campaigns and capacity-building initiatives.
7. Collaborate with regional and international CERTs and cybersecurity organisations.

Part III: Governance and Operations

Section 6: Governance Structure

1. The CERT shall be governed by a CERT Board, comprising:
   - A Chairperson appointed by the Minister of ICT.
   - Representatives from key government agencies (for example, defence, interior, communications).
   - Private sector representatives from critical industries (for example, banking, energy, telecommunications).
   - A representative from academia.
   - A representative from civil society.

2. The CERT Board shall:
   - Oversee the strategic direction of the CERT.
   - Approve budgets and operational plans.
   - Ensure accountability and transparency.

Section 7: Leadership of the CERT

1. The CERT shall be headed by a Director, appointed by the CERT Board.
2. The Director shall:
   - Manage the day-to-day operations of the CERT.
   - Represent the CERT in national and international forums.
   - Submit annual reports to the CERT Board and the Ministry of ICT.

Part IV: Incident Reporting and Response

Section 8: Mandatory Incident Reporting

1. All organisations operating critical infrastructure must report cybersecurity incidents to the CERT within 24 hours of detection.
2. Failure to report incidents shall result in penalties as prescribed under Section 15 of this Act.

Section 9: Incident Response Authority

1. The CERT shall have the authority to:
   - Investigate reported cybersecurity incidents.
   - Issue directives to mitigate risks or contain threats.
   - Co-ordinate responses with affected entities and stakeholders.
2. The CERT may access affected systems and data with the organisation's consent, or under a court order where consent is withheld.

Part V: Data Protection and Confidentiality

Section 10: Data Protection

1. The CERT shall ensure that all data collected during its operations:
   - Is used solely for cybersecurity purposes.
   - Is stored securely and accessed only by authorised personnel.
   - Complies with the [Country Name Data Protection Act] or equivalent legislation.

Section 11: Confidentiality

1. Information shared with the CERT shall remain confidential and shall not be disclosed without the owner's consent, except:
   - As required by law.
   - To address a national security threat.

Part VI: Funding and Resources

Section 12: Funding Sources

The CERT shall be funded through:

1. Annual government budget allocations.
2. Revenue from services, such as training and incident response consultations.
3. Grants and donations from development partners and international organisations.
4. Public–private partnerships (PPPs) with stakeholders.

Section 13: Financial Accountability

The CERT shall:

1. Maintain transparent financial records.
2. Submit annual financial statements for audit by the [Country Name Auditor-General].

Part VII: Enforcement and Penalties

Section 14: Regulatory Authority

The CERT is authorised to:

1. Enforce compliance with cybersecurity standards.
2. Issue guidelines and directives to address cybersecurity threats.

Section 15: Penalties

1. Failure to report cybersecurity incidents shall result in a fine not exceeding [amount in local currency] or imprisonment for up to [period] months.
2. Obstruction of CERT operations shall result in a fine or imprisonment as determined by the courts.

Part VIII: Regional and International Co-operation

Section 16: Collaboration

The CERT shall:

1. Collaborate with regional and international CERTs to address cross-border cyber threats.
2. Align its operations with international standards, such as the African Union Convention on Cybersecurity (Malabo Convention).

Part IX: Miscellaneous

Section 17: Regulations

The Minister of ICT may issue regulations to operationalise this Act, including:

1. Detailed reporting requirements.
2. Guidelines for public–private co-operation.
3. Procedures for handling cross-border incidents.

Section 18: Repeal and Savings

Any provisions of existing laws inconsistent with this Act are hereby repealed, but actions taken under such laws shall remain valid.

Section 19: Commencement

This Act shall take effect upon publication in the [**Official Gazette**].

Appendix C: List of national CERTs in Africa

Table C1 List of national CERTs in Africa.

Country	CERT Name	Website
Benin	BjCSIRT (Benin Incident Response Team)	https://csirt.gouv.bj/
Botswana	Botswana National CSIRT	www.cirt.org.bw
Burkina Faso	Centre de Cybersécurité du Burkina Faso	www.cirt.bf
Cameroon	National Agency for Information and Communication Technologies	https://cirt.cm
Côte d'Ivoire	CI-CERT (Côte d'Ivoire Computer Emergency Response Team)	www.cicert.ci
Eswatini	Sz-CIRT (Computer Incident Response Team for Eswatini)	https://ncsirt.org.sz/
Ethiopia	ETHIO-CERT (Ethiopian Cyber Emergency Readiness and Response Team)	https://ethiocert.insa.gov.et
Egypt	EG-CERT (Egyptian Computer Emergency Readiness Team)	www.egcert.eg
The Gambia	gmCSIRT (The Gambia National Computer Security and Incident Response Team)	https://gmcsirt.gm/
Ghana	CERT-GH (Ghana Computer Emergency Response Team)	https://www.csa.gov.gh/cert-gh
Kenya	CSIRT-KENYA (Kenyan National Computer Security Incident Response Team)	www.csirt.or.ke
Malawi	MwCERT (Malawi Computer Emergency Response Team)	www.mwcert.mw
Mauritius	CERT-MU (Mauritius Computer Emergency Response Team)	www.cert-mu.org.mu
Morocco	maCERT (Moroccan Computer Emergency Response Team)	www.macert.ma
Nigeria	Nigeria Computer Emergency Response Team (ngCERT)	https://cert.gov.ng
Rwanda	Rw-CERT (Rwanda Computer Emergency Response Team)	www.cert.gov.rw
Somalia	SOMCERT (Somalia Computer Emergency Response Team)	somcert.gov.so
South Africa	ECS-CSIRT (Member of FIRST)	www.e-comsec.com/ECSCSIRT
South Africa	CSIRTFNB (Computer Security Incident Response Team First National Bank)	www.fnb.co.za
Sudan	CERT Sudan	www.cert.sd
Tanzania	TZ-CERT (Tanzania Computer Emergency Response Team)	www.tzcert.go.tz
Tunisia	tunCERT (Tunisian Computer Emergency Response Team)	www.ansi.tn
Uganda	CERTUG/CC (Uganda National Computer Emergency Response Team and Coordination Center)	www.cert.ug
Zambia	ZMCIRT (Zambia Computer Incident Response Team)	www.cirt.zm

Appendix D: Threat intelligence effectiveness assessment metrics

Table D1 Threat intelligence effectiveness assessment metrics.

Metric	Definition	Why it matters	Example measurement
Timeliness	Measures how quickly intelligence is shared after detection.	Faster intelligence sharing helps prevent attacks and minimise damage.	- **Average time** from detection to dissemination (for example, in minutes/hours).
Accuracy	Percentage of intelligence that is actionable and free from false positives.	Reduces wasted effort on false alarms and increases focus on real threats.	- **False positive rate**=(false positives / total alerts) * 100%. - **Precision rate**=(true positives / total alerts) * 100%.
Stakeholder engagement	Tracks the number of internal and external stakeholders actively using shared intelligence.	High engagement means intelligence is valuable and operationalised.	- Number of downloads/views of intelligence reports. - Number of stakeholder queries related to intelligence.
Incident mitigation success	Measures the impact of intelligence in reducing security incidents.	Demonstrates effectiveness in reducing breaches, dwell time and financial loss.	- Reduction in attack **dwell time** (time attackers remain undetected). - Decrease in **incident severity ratings** over time.
Collaboration metrics	Tracks frequency and effectiveness of intelligence sharing with external partners.	Enhances collective defence by improving global threat awareness.	- **Number of** intelligence reports shared with partners. - Participation in cybersecurity forums and information-sharing groups.
Threat detection rate	Measures how many threats are successfully identified by the intelligence system.	Ensures that intelligence sources and detection mechanisms are effective.	- **Number** of threats detected per month. - **Percentage** of threats detected before causing harm.
Threat intelligence utilisation	Tracks how often intelligence is used to make security decisions.	Ensures that intelligence is actionable and being incorporated into security strategies.	- Number of security changes made based on threat intelligence (for example, firewall rules, patches, alerts).
Impact on risk reduction	Measures how intelligence helps lower organisational risk levels.	Demonstrates long-term effectiveness of intelligence-driven security.	- Reduction in the number of successful cyberattacks. - Lower financial losses attributed to cyber incidents.
Relevance of intelligence	Assesses whether shared intelligence aligns with current threats and security needs.	Ensures intelligence is not outdated or irrelevant.	- Percentage of intelligence reports used in security operations. - **Feedback** from stakeholders on intelligence usefulness.

Appendix E: Key legal and regulatory elements necessary for establishing a strong CERT

Table A5 summarises key legal and regulatory elements necessary for establishing a strong CERT foundation, particularly in the African context. It highlights essential policies, laws and frameworks that support CERT operations and cybersecurity efforts.

Table E1 Key legal and regulatory elements for a CERT.

Category	Description	Examples	Key elements
Legal and policy foundations	Clear mandate and authority for CERTs	South Africa's National Cybersecurity Policy Framework	National cybersecurity strategy, legal mandate
Legal and policy foundations	Protect critical infrastructure, incident reporting obligations, international co-operation	Ghana's Cybersecurity Act (2020)	Prioritise critical infrastructure, mandate incident reporting
Incident reporting and information sharing policies	Mandatory reporting requirements, confidentiality, collaboration incentives	Ghana's Cybersecurity Act (2020); Kenya's Cybersecurity and Data Protection Bill	Define reporting entities, timelines, protect confidentiality
Data protection and privacy laws	Align with national and regional data protection laws	African Union Convention on Cybersecurity and Personal Data Protection ('the Malabo Convention') Ghana's Data Protection Act, 2012	Define data collection policies, ensure privacy compliance
Cybercrime legislation	Define offenses, penalties, forensic assistance	Mauritius Cybercrime Act (2021) Nigeria Cybercrime Act (2015)	Include hacking, identity theft, support law enforcement
Critical infrastructure protection (CIP) frameworks	Sector-specific standards, risk assessments, CERT designation	South Africa's Protection of Critical Infrastructure Act (2019); Rwanda's National Cybersecurity Policy (2015)	Implement sector-specific controls, mandate risk assessments
Public–private collaboration frameworks	Information sharing agreements, joint exercises, liability protection.	Require two-way threat intelligence sharing. Protect proprietary information.	Facilitate public–private co-operation
Cybersecurity standards and compliance	Adopt international standards like ISO/IEC 27001 and NIST Cybersecurity Framework	Require compliance with standards as part of regulations	Guide CERT operations, assess stakeholder compliance

(Continued)

Table E1 Key legal and regulatory elements for a CERT.

Category	Description	Examples	Key elements
CERT roles in national security frameworks	Define role in national security, emergency powers, collaboration with law enforcement	Grant emergency powers, authorise collaboration with law enforcement	Support national security efforts
Enforcement and penalties	Establish penalties for non-compliance	Impose fines for failure to report incidents, enforce penalties for non-compliance with standards	Deter non-compliance with cybersecurity laws
International and regional co-operation	Cross-border collaboration, mutual legal assistance treaties	Align with global frameworks like the Budapest Convention	Facilitate international co-operation in cybercrime investigations

Appendix F: Critical steps in a CERT checklist

Table F1 Critical steps in a CERT checklist.

Steps	Features to be implemented
Incident detection and monitoring	• **IDS/IPS deployment**: Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) like Snort and Cisco Firepower. • **Network traffic analysis**: Use tools like Zeek and Wireshark to monitor network traffic. • **Endpoint monitoring**: Deploy endpoint detection and response (EDR) tools such as CrowdStrike.
Threat intelligence and analysis	• **Threat intelligence platforms**: Utilise platforms like ThreatConnect and MISP to aggregate threat data. • **Malware analysis**: Conduct analysis using tools like Cuckoo Sandbox and VirusTotal.
Incident response and forensics	• **Digital forensics**: Use tools like FTK Imager and EnCase for incident investigation. • **Automated response**: Implement tools like TheHive for automated incident response.
Communication and co-ordination	• **Collaboration tools**: Utilise platforms like Slack and Microsoft Teams for team co-ordination. • **Secure communication**: Ensure secure communication with tools like Signal.
Vulnerability management	• **Vulnerability scanning**: Regularly scan for vulnerabilities using tools like Nessus. • **Patch management**: Automate patching with tools like WSUS.
Backup and recovery	• **Backup solutions**: Implement regular backups using tools like Veeam.
Disaster recovery:	• Ensure disaster recovery capabilities with tools like Zerto.
Integration and interoperability	• Ensure seamless integration between different tools and systems.
Post-incident review	• Conduct thorough reviews after incidents to improve response strategies.

Appendix G: Policy and framework resources repository

Table G1 Policy and framework resources repository.

Resource	Description	Examples/tools	Key elements
NIST special publications	Cybersecurity guidelines and templates	NIST SP 800-61 (Incident Response), NIST SP 800-128 (Configuration Management), NIST SP 800-30 (Risk Assessment)	Adaptable for national CERTs, procedural templates
International Telecommunication Union (ITU)	Guidelines for establishing and operating CERTs	Tailored to national contexts within Africa	Frameworks for CERT operations
African Union (AU) cybersecurity initiatives	Legal frameworks for cybersecurity and data protection	Malabo Convention	Foundational principles for policy development
Collaboration with established CERTs	Practical insights and shareable templates	CERT-MU, CSIRT-ZA	Tailored to the African cybersecurity landscape
Cybersecurity Capacity Centre for Africa (CACF)	Toolkits and resources for enhancing cybersecurity capabilities	*CERTs Toolkit* with policy and procedure templates	Designed specifically for African nations

Appendix H: Components of a cyber crisis communication plan

Table H1 Components of a cyber crisis communication plan.

Component	Description	Key elements	Examples
Crisis management team	Define roles and responsibilities	Include contact information for team members	Designate a spokesperson
Communication channels	Establish protocols for internal and external communication	Use emergency hotlines, email and social media	Ensure rapid dissemination of information
Messaging templates	Prepare pre-approved messaging for different scenarios	Include templates for media releases and internal briefings	Tailor messages for various stakeholders
Stakeholder analysis	Identify and prioritise stakeholders	List internal and external stakeholders (for example, employees, customers, the media)	Customise communication strategies for each group
Practice and review	Regularly update and practise the plan	Conduct simulations to ensure readiness and adaptability	Review and refine the plan based on lessons learned

Appendix I: Key activities in crisis communication planning

Table I1 Key activities in crisis communication planning.

Element	Description	Key activities	Examples
Pre-incident planning	Develop a crisis communication plan (CCP)	Outline roles, responsibilities and communication channels	Include messaging templates, designated spokespersons
Pre-incident planning	Conduct regular training and simulations	Practice tabletop exercises or fire drills to enhance readiness	Simulate cyber scenarios to build response muscle memory
During an incident	Activate a joint information centre (JIC)	Manage media inquiries and public communication	Co-ordinate press releases and social media updates
During an incident	Deliver regular updates to stakeholders and the public	Use press releases and social media for timely communication	Ensure consistent messaging across channels
Post-incident review	Publish an incident report	Summarise key actions, lessons learned and recommendations	Document incident response effectiveness
Post-incident review	Engage stakeholders in a post-incident debriefing session	Conduct a review to improve future responses	Gather feedback from stakeholders

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D20128