East African Communications Organisation

REGIONAL STRATEGY FOR ESTABLISHING AND OPERATIONALIZING OF COMPUTER INCIDENT RESPONSE TEAMS (CIRTS/CERTS)

Table of Contents

Abbreviations and Acronyms

CIRT	: Computer Incident Response Team
CERT	: Computer Emergency Response Team
EAC	: East African Community
EACO	: East African Communication Organisation
ENISA	: European Union Agency for Cybersecurity
EU	: European Union
FIRST	: Forum of Incident Response and Security Teams
GCI	: Global Cybersecurity Index
ITU	: International Telecommunication Union
OAS	: Organization of American States
OIC	: Organisation of Islamic Cooperation
SADC	: Southern African Development Community
SPIDER	: Swedish Program for ICT in Developing Regions

1. Introduction and Background

A Computer Incident Response Team (CIRT/CERT) is an organizational unit that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents in accordance with its mission.

A properly deployed CIRT/CERT has a clear mandate, a governance model, a tailored service framework, technologies, and processes to provide, measure, and continuously improve defined services.

Because there is no standard method for developing or operationalizing a National/Sector CIRT/CERT, this document serves to provide guidelines for various CIRTs/CERTs throughout the EAC area based on best practices and lessons learned. Kenya, Uganda, Tanzania, Rwanda, South Sudan, and Burundi are all at various stages of establishing a National CIRT/CERT. In order to address the demands of its constituents, CIRTs/CERTs must first grasp their objectives. As of January 2023, there are around 665 CERTs[1] worldwide.

Because of its social, political, and economic environment, the EAC Region has almost the same cybersecurity problems as the rest of the world. Socially, a common language and culture; politically, shared boundaries and political blocs; and economically, through the wide adoption of mobile money, one-area-network, cross-border trade, among others.

1.1. Types of Computer Incident Response Teams

Different CIRTs/CERTs can be classified as formal or informal, with examples being national CERTs, multi-organizational CERTs, organizational CERTs, sectoral CERTs, etc. Formally incorporated CIRTs are specified by statute, court order, or regulatory framework, whereas informal CIRTs may operate via consensus or agreement. A semi-formal CIRT falls under a third category that falls between the two. An example of a formal CIRT in the EAC Region is Tanzania CERT (TZ-CERT)[2], Kenya CIRT (National KE-CIRT/CC)[3], Uganda CERT[4], South Sudan CERT, Rwanda CERT[5] and Burundi CERT.

[1] https://www.first.org/members/teams/
[2] https://www.tzcert.go.tz/wp-content/uploads/2019/05/epoca.pdf
[3] https://ke-cirt.go.ke
[4] https://ug-cert.ug/services/
[5] https://cert.gov.rw/home

CIRTs may be categorized by responsibility to its constituents. These categories are National, Sectorial, Regional and Organizational.

1.2. Benefits of CERT/CIRT

The benefits accrued from a National/Sector CIRT are outlined below:

a) Establish and maintain operational and relational mechanisms in order to maintain trust with its stakeholders including both regional and international entities that are involved in the management of cybersecurity incidents;
(b) Maintain a trusted sector focal Point of Contact (PoC) within and beyond the national borders that responds to cybersecurity incidents within the communications sector;
(c) Develop and define communication approaches and information sharing among the constituents, service providers and stakeholders;
(d) Develop and deliver a set of crucial reactive and proactive services to the public for continuous awareness and knowledge sharing;
(e) Forecast and broadcast alerts on cybersecurity incidents;
(f) Develop a collaborative relationship with other similar organizations and associates;
(g) Raise awareness and provide support to other CERTs.
(h) Escalate received incidences to national security or law enforcement agencies for further action including prosecution;
(i) Collaborations with other CERTs in and outside its constituency.

1.3. Role of Regional Organizations in Development of CERTs

The establishment and development of CERTs/CIRTs have been addressed by various international and regional organizations. These international organizations include the International Telecommunications Union (ITU), the European Network and Information Security Agency (ENISA) of the European Union (EU), and the Organization of American States (OAS). This underscores EACO's role in the development of CERTs in the EAC region.

2. Objectives

The key objectives of the strategy are:

1. To support the establishment and enhancement of National CIRTs in the EAC region.

2. To share best practices among EACO members states in the establishment and enhancement of National CIRTs.

3. Framework for Operationalization

The framework for operationalization of CIRT/CERT draws from the ITU CIRT framework[6]. The framework provides for the following phases: assessment, design, establishment and enhancement.

3.1. Assessment

The assessment stage is a crucial first step to starting any cybersecurity strategy, including the operationalization of CIRTs. This stage serves to assess the current incident response capabilities in the country/sector. The assessment requires that all stakeholders agree on the present incident response capabilities. These may include the country's or sector's cyber vulnerabilities, threats, and technologies.

This assessment is the first step towards operationalizing security incident response teams in a nation or sector. This holistic assessment can be a technical and procedural challenge. It requires a keen understanding of both the external threat landscape and the countries specific economic and political environment. To achieve the best outcome, the assessment should be executed without organizational or country biases.

The assessment should take into consideration important elements of a National Cybersecurity Strategy[7] such as

1. Political support as strategic stakeholders
2. Legal frameworks
3. Organizational frameworks
4. Public awareness
5. International cooperation
6. Capacity building
7. Industry development
8. Research and development

[6] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYBERSEC-2021-01-PDF-E.pdf
[7] http://www.iiis.org/CDs2019/CD2019Summer/papers/SA985PZ.pdf

9. Reporting and incident management

3.2. Establishment

The establishment and operationalization of a CIRT is the operational level in the implementation of a national cybersecurity strategy[8]. The Global Cybersecurity Index (GCI)[9], which is a trusted reference that measures the commitment of countries to cybersecurity at a global level, considers five pillars, namely: Legal, Technical, Organizational, Capacity Development and Cooperation. The establishment and operationalization of the CIRTs will consider all these factors, but with a varying degree of detail.

According to the GCI 2020, EAC countries were favorably ranked due to the cybersecurity initiatives and activities undertaken by the member states in the operationalization and establishment of CIRTs. The GCI can be used by EACO members to benchmark against best practices within the region. The establishment and operationalization of CIRTs can start through incubation by the National Regulatory Authority as it develops and grows to meet the needs of its constituents.

Capacity development is essential to the establishment and operationalization of CIRTs. To achieve this objective, it is paramount for EAC member countries to partner with industry and academia to develop cybersecurity capacity.

EAC countries can leverage EACO to build partnerships within the EAC region and globally. EACO has been instrumental in building such partnerships such as SPIDER, an independent centre focusing on the digitalization of international development.

3.3. Enhancement

EAC regional CIRTs can improve once established and operationalized by undertaking various strategic initiatives to adequately meet the needs of its constituents. These improvement measures include but not limited to building and creating awareness, establishing trust across various sectors, research, and development.

[8] http://www.iiis.org/CDs2019/CD2019Summer/papers/SA985PZ.pdf
[9] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

The foundation of the establishment and operationalization of CIRTs are all the pillars needed in the development of a National Cybersecurity Strategy that needs to be updated from time-to-time to match the ever-changing cybersecurity landscape.

4. Proposed Strategy.

To implement the strategy, the objectives have been broken down into activities and allocated resources. The activities of the implementation plan are captured in the table below.

NO	OBJECTIVE	ACTIVITIES	MEMBER STATES	TIMELINES	RESOURCES
1.	To support the establishment and enhancement of National CIRTs in the EAC region	Develop and enhance legal framework toward establishment of CIRT/CERT	South Sudan Burundi Kenya Tanzania Uganda Rwanda	2024	Member country support
		Join The Forum in Incident Response and Security Teams (FIRST)	South Sudan Burundi	2025	Financial resources
		Track country commitment to cybersecurity through ITU Global Cybersecurity Index	South Sudan Burundi Kenya Tanzania Uganda Rwanda	2024	National regulatory authorities
2.	To share best practices among EACO members states in the establishment and enhancement of National CIRTs.	Participate in regional cybersecurity capacity building activities (cyber drills, meeting, etc.)	South Sudan Burundi Kenya Tanzania Uganda Rwanda	2024	Financial resources
		Enhance collaboration and information sharing within member states	South Sudan Burundi Kenya Tanzania Uganda Rwanda	2024	National CERTs

5. Monitoring and Evaluation

Success of the strategy implementation shall be through quantitative and qualitative measures. Quantitative measures are through ITU GCI, FIRST membership, Legal frameworks in place, number of meetings and number of trainings. The qualitative measures are Internet presence, confidence, and trust in online experience among others.

EACO will carry out an evaluation each year before EACO Assemblies and Congress.

6. Conclusion

Based on the discussions in this strategy paper on the establishment and operationalization of CIRTs, specific strategies that member states should undertake to achieve the objective of their National CIRTs. The specific strategies proposed for member states are establishment of National CIRT/CERTs, cooperation, and collaboration within the EAC region and globally, the framework towards establishment and enhancement of National CIRT/CERT and tracking members commitment to cyber security through ITU Global Cybersecurity Index (GCI). It should be noted that capacity development is a cross-cutting pillar to support the achievement of this strategy.