
# ECOWAS Regional Critical Infrastructure Protection Policy

## SECTION 1. INTRODUCTION

In any country, a certain number of material or non-material services provided by public or private operators are essential for the Nation, and in particular for the functioning of the State, the economy or for the health, safety, security and well-being of the population. These services rely on physical or digital infrastructure as well as on any data necessary for their operation.

It is therefore of the utmost importance for the State, economic operators and the population to guarantee the resilience and security of these critical infrastructure, essential services and data in view of all the risks and threats that could affect their availability or integrity.

Indeed, the resilience and security of critical infrastructure and essential services can be affected by a variety of risks and threats - breakdowns, accidents, malicious acts, physical or digital attacks, natural disasters, pandemics, etc. -, all of which can have a serious impact on a Nation. It is therefore important that the protection of each critical infrastructure or essential service takes into account all of the risks and threats, both physical and digital, it can face.

In addition, some services may rely on infrastructure and data located abroad. In this case, the protection of these services cannot be fully ensured by the country where they are provided. This justifies that each country integrates into its approach the essential services which it needs as much as the critical infrastructure located on its territory. This type of situation also justifies the regional approach to this policy.

In the rest of this document, data will be considered as an integral part of the infrastructure that stores, processes or transmits it.

## SECTION 2. SUBJECT MATTER

The purpose of this Regional Policy is to ensure the resilience and security, faced with the various risks and threats which could affect their functioning, of the region's infrastructure and services which are essential for the functioning of the State, the economy or for the health, safety, security and well-being of the population, in particular when these infrastructure and services are transnational in nature.

To this end, this Regional Policy:

- sets the minimum normative framework that Member States should adopt to ensure the protection of their critical infrastructure and essential services;
- provides elements of methodology and criteria to identify the infrastructure and services concerned in the various sectors;
- proposes a list of preventive, reactive and proactive measures that can be implemented;
- provides the principles and modalities of cooperation between Member States with interdependence in critical infrastructure or essential services.

This Regional Policy should be without prejudice to the possibility for each State to take the necessary measures to ensure protection of its essential interests and its security, safeguard public policy and public security, and to allow for the investigation, detection and prosecution of criminal offences.

## SECTION 3. DEFINITIONS

For the purposes of this Regional Policy, the following definitions shall apply:

**Cybersecurity**: set of safeguards and actions to protect the cyberspace and cyber assets from those threats that are associated with or that may harm its network and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein;

**Cybercrime**: criminal activities where computers and information systems are involved either as a primary tool or as a primary target. Cybercrime comprises traditional offences (e.g. fraud, forgery, and identity theft), content-related offences (e.g. on-line distribution of child pornography or incitement to racial hatred) and offences unique to computers and information systems (e.g. attacks against information systems, denial of service and malware);

**Critical Infrastructure**: a public or private infrastructure or process whose destruction, standstill, illegitimate exploitation or disruption for a defined period of time will cause either loss of lives or significant loss to the economy or damage significantly the reputation of the State or its symbols of governance. In this definition, infrastructure includes the networks, systems and the physical or digital data essential for providing this service. This term may refer to a certain system or process whose functioning is critical within the organization;

**Critical Information Infrastructure**: communication network or information system whose malfunction or malicious exploitation could cause the total or partial interruption of a critical infrastructure or an essential service;

**Critical Infrastructure Operator**: public or private operator that operates a critical infrastructure;

**Critical Infrastructure Protection** (CIP): set of safeguards and actions to protect critical infrastructure from any risks and threats that could cause the total or partial interruption of the essential services they provide;

**Critical Information Infrastructure Protection**: cybersecurity of critical infrastructure, i.e. set of safeguards and actions to protect communication network and information system from cyber threats whose disruption or shutdown could cause the total or partial interruption of a critical infrastructure or an essential service;

**CSIRT (Computer Security Incident Response Team)**: team responsible for alerting about threats, preventing risks and threats to information systems, reacting to security incidents and aiding in mitigation;

**Essential Service**: a service where total or partial interruption of which could have a serious impact on the functioning of the State, the economy of the country or on the health, safety, security and well-being of citizens, or any combination of these issues that does not rise to the criteria of critical Infrastructure;

**Essential Service Operator**: public or private operator that provides an essential service.

**Essential Service Protection**: set of safeguards and actions to protect essential services from any risks and threats that could cause their total or partial interruption;

**Information and Communications Technologies** (ICT): technologies used to gather, store, use and send information, including technologies that involve the use of computers and any communication system, including any telecommunication system;

**Information System**: any isolated or non-isolated device or group of interconnected devices that all or in part carries out automatic processing of data pursuant to a program.

**Networks**: set of means ensuring the supply of an infrastructure with products or services necessary for its operation (communications, energy, logistics, etc.);

## SECTION 4. FRAMEWORK FOR THE CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES PROTECTION

Each State should adopt a framework for protecting critical infrastructure and essential services, for all sectors of activity (Government, health, energy, transport, water, banks, industry, etc.) and in particular transverse sectors (electrical production and distribution, digital services), which set:

- Responsibilities within the State services;
- Criteria and methods for identifying critical infrastructure and essential services;
- Procedures for designating operators of critical infrastructure and essential services;
- Security obligations imposed on these operators;

Each State should identify the authority or authorities responsible, for the various business sectors, to:

- identify critical infrastructure and essential services;
- designate the corresponding operators;
- develop the security measures imposed on them;
- ensure the coordination of the action of the public authorities which must contribute to the security of critical infrastructure and essential services;
- participate in crisis management in the event of a serious incident affecting critical infrastructure;
- ensure the coordination of these different tasks with foreign counterparts for transnational critical infrastructure.

Each State should establish a body responsible for ensuring the consistency of the procedures implemented by the various national authorities.

## SECTION 5. RESPECTIVE ROLES OF THE STATE AND OPERATORS

The operators of critical Infrastructure and essential services are responsible for their protection. Regardless, the State, as guarantor of the nation's security, is responsible for ensuring country's critical infrastructure and essential services protection. In this context, it must in particular identify and designate operators of critical infrastructure and essential services, impose obligations to protect them, monitor their proper execution and enforce consequences.

Furthermore, the protection of critical infrastructure and essential services cannot be ensured by the operators concerned alone. As they have neither the legitimacy nor in general the relevant knowledge and information to intervene outside their perimeter of responsibility. The State must play its part, by providing operators with guidance and support, in a close public-private partnership. In particular, it should act to minimise risk, address threats and manage the situation in the event of a physical or digital attack, in particular with its authorities, intelligence services, law enforcement agencies, national CSIRT and judicial institutions.

## SECTION 6. RISK MANAGEMENT APPROACH

Critical infrastructure and essential services protection constitutes a heavy burden from the organizational, technical, human and financial aspects. Therefore, enhanced protection should only be required for those infrastructure and services that are genuinely critical or essential, and provided at the appropriate level.

With this in mind, a risk management approach must be put in place for the application of this policy in order to identify potential risks and threats and to proportion efforts to the probability of occurrence and the severity of impacts they could cause on the Nation.

In particular, it will allow each country to:

- Identify and declare critical infrastructure, essential services and the public and private operators concerned;
- Define the adequate level of measures to protect these infrastructure and services from physical and digital risks and threats likely to cause a serious impact on the Nation, and the measures aimed at minimizing the potential impacts.

## SECTION 7. IDENTIFICATION OF CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES AND DESIGNATION OF OPERATORS

The process must begin with the identification of essential services, then of infrastructure that are necessary to provide these services or that are critical for other reasons. A non-exhaustive list of infrastructure and services likely to be classified as critical or essential, presented by sector of activity, is provided in Annex I.

The process should continue with the identification of operators of critical infrastructure or essential services. Standard criteria are proposed in Annex II. These operators must then be subject to a formal procedure of approval and designation.

## SECTION 8. OBLIGATIONS OF OPERATORS

A non-exhaustive list of measures that can be imposed on operators of critical infrastructure and essential services is provided in Annex III.

These operators should be compelled to at least:

- set up an organization at the management level intended to organize and take into account the protection of their installations;
- comply with technical and operational rules intended to strengthen the physical security and cybersecurity of their facilities;
- report promptly to the relevant authorities any incident that could have a serious impact;
- collaborate frankly and without reserve with the authorities when necessary.

Any operator of critical infrastructure or essential services must put in place the organizational, operational and technical arrangements necessary to comply with the protection measures imposed on it. They should be described in the following documents, which are to be submitted to the competent authorities for managing cybersecurity in each Member State:

- A map of its essential services;
- An operator security plan;
- An Information Security Policy (ISP) with regard to cybersecurity, emphasizing the information systems most critical to the essential services it provides.

## SECTION 9. PROTECTION MEASURES

A risk analysis, based on scenarios taking into account the various risks and threats identified, must make it possible to develop protection measures for each operator or type of operator of critical infrastructure or essential services.

These measures are preventive, reactive and proactive that can also be organizational, operational, technical or legal.

Preventive measures must aim to prevent and mitigate risks and threats, and to reduce as far as possible the severity of potential impacts on the infrastructure or service concerned and on the Nation. Reactive measures must be planned and implemented in the event of an incident affecting the critical infrastructure or essential service. They must enable the management of the incident, until the resumption of normal activity, and the management of the crisis that this incident causes on the Nation. Proactive measures aim to prevent recurrence of incidents, by examining the possible causes of incidents that have occurred and by adopting an approach to detect and contain any identical incidents. The measures taken should be smart and have a tangible impact on the objectives mentioned.

Measures to protect critical infrastructure or essential services from risks and threats using or affecting information and communication technologies must be consistent with the Regional cybersecurity and cybercrime Strategy.

In addition, Member States should take into account in their national policy the protection measures already provided for in international regulations for all key sectors (air transport, maritime navigation, banking transactions, etc.).

## SECTION 10. SANCTIONS

Sanctions including criminal and administrative sanctions where necessary must be provided against operators and other parties who fail to comply with the protection measures.

In addition, the Criminal law may impose stronger penalties (criminal and administrative) for offenses by operators and other parties which disrupt or attempt to disrupt the proper functioning of critical infrastructure and essential services.

## SECTION 11. INTERDEPENDENCIES OF CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES

The approach must take into account the interdependencies that may exist between critical infrastructure and essential services. For example, all infrastructure and services are, with rare exceptions, dependent on the power grid and electronic communications services.

Therefore, each State should put in place circumvention measures[1] to avoid any interruption in the operation of critical infrastructure and essential services that could cause a serious impact on the Nation.

## SECTION 12. NATIONAL COORDINATION

Each State should mobilize all authorities and public actors concerned, including in particular the body responsible for the national cybersecurity, to establish a national policy for the protection of critical infrastructure and essential services and to define the contribution of each to its implementation, in relation to both preventive and reactive measures.

Public authorities and actors should engage in dialogue with operators of critical infrastructure and essential services to identify major vulnerabilities, the measures likely to reduce them and the reasonable timeframe for the implementation of these measures.

## SECTION 13. INTERDEPENDENCIES BETWEEN COUNTRIES IN THE REGION AND REGIONAL COOPERATION

Interdependencies between countries continue to grow within ECOWAS, also in relation to essential services.

In addition to interlinked services such as public telecommunications, financial transactions or international air transport, there is an increasing number of infrastructure serving several countries, for example in the areas of road corridors, Internet connectivity (especially global transit), electricity, mining, gas and the West Africa Police Information System (WAPIS) set up in all ECOWAS Member States.

Certain services may be classified as essential by all Member States concerned. Others, deemed essential in one country, may depend on infrastructure located in another country that does not identify them as critical.

Faced with this dual problem, it is necessary to set up a dialogue and cooperation among Member States of the region, based on a common understanding of the issues, similar and sufficient protection measures in all countries.

Member States with interdependence in critical infrastructure and essential services should establish cooperation between their competent authorities to:

- Identify transnational critical infrastructure and essential services, as well as the nature of their interdependencies;

[1] For example: installation of electric generators or a redundancy of power feeds and electronic communications links.

- Take into account as much as possible the needs of other Member States in the designation of their critical infrastructure;
- Harmonize the protection measures imposed on the operators concerned;
- Exchange information on threats and risks and, in a coordinated manner, take any additional measures necessary to respond to an increasing or imminent threat or risk;
- Coordinate the measures to be taken in the event of a crisis linked to a transnational critical infrastructure.

## SECTION 14. MONITORING AND UPDATING OF THIS REGIONAL POLICY

The ECOWAS Commission shall set up a committee to monitor this policy. The monitoring committee comprised of the ECOWAS Commission and a high-level representative provided by each Member State will meet at least once a year to ensure the monitoring of the provisions of this regional policy over time and to propose any new actions and changes that may be necessary.

## ANNEXE I

## INFRASTRUCTURE AND SERVICES THAT MAY BE CLASSIFIED AS ESSENTIAL OR CRITICAL

The process of identifying operators of critical infrastructure and essential services must consider the non-exhaustive list of infrastructure and services appearing in the table below:

| Sectors | Infrastructure and services |
|---|---|
| 1. Government activities | - Public security<br>- Homeland security<br>- Judicial services<br>- National Defence<br>- Public finances<br>- Parliament<br>- Election processes<br>- Electronic administration, in particular certain online public services |
| 2. Energy | - Electricity production, transport and distribution<br>- Production, transport, refining, storage and distribution of petroleum products<br>- Production, transport, treatment, storage and distribution of gas<br>- Nuclear installations |
| 3. Transport | - Air, road, rail, sea and river transport<br>- Air traffic control<br>- Airport and port platform management (including security systems)<br>- Road and rail infrastructure management |
| 4. Logistics | - Logistics platform management |
| 5. Finances | - Distribution of social minima (security intervention/financial hand out/social incentives)<br>- Management of the recovery and the treasury of social organizations<br>- Bank transactions<br>- Financial services and credit clearing<br>- Financial market infrastructure |
| 6. Health | - Unique health care capabilities or procedures (in healthcare establishments or by telemedicine)<br>- Pharmaceutical distribution<br>- Research laboratories<br>- Medical records databases |
| 7. Water and sanitation | - Production, transport, storage and distribution of drinking water (by pipeline or bottled)<br>- Wastewater collection and management systems |
| 8. Electronic Communications | - National Internet network and interconnection to the regional and global Internet (submarine and terrestrial cables, cable landing points, Internet exchange points, etc.)<br>- Internet domain name management (DNS)<br>- Internet access<br>- Telecommunication services (telephony, etc.)<br>- Data centres including National Data Centres |
| 9. Information | - Radio and television stations |
| 10. Food | - Supply, storage and distribution of the main foodstuffs |
| 11. Industry | - Essential industries for the country |
| 12. Miscellaneous | - Industries likely to cause serious damage to the population in the event of accidental or malicious damage or destruction (dam for example) |

## ANNEXE II

## IDENTIFICATION CRITERIA OF OPERATORS OF

## CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES

The process of identifying operators of critical infrastructure and essential services can take place using all or part of the criteria indicated in the following non-limiting list:

1. The level of severity, duration and extent of the impact that an interruption of service or an incident would have on the operation of the State, on the economy or on health, safety, security and well-being of the population;
2. The size of the area or of the population likely to be affected by an incident;
3. The number of users depending on the service (expressed as a percentage of the population for example);
4. The operator's market share;
5. The dependence of other critical infrastructure or essential services to this service (case of electrical distribution and electronic communications services for example);
6. The importance of the operator in ensuring an adequate level of service, taking into account the availability of alternative means for providing the service;
7. Where applicable, sectoral factors.

**ANNEXE III**

**MEASURES THAT MAY BE IMPOSED ON**

**OPERATORS OF CRITICAL INFRASTRUCTURE AND ESSENTIAL SERVICES**

The following non-exhaustive list provides measures that can be imposed on operators of critical infrastructure and essential services.

Preventive measures

- Protection governance:
    1. Designate a security officer who is accountable to public authorities for all security related matters;
    2. Establish an organization to ensure the physical protection and cybersecurity of the operator's infrastructure;
    3. Send a report to public authorities, at a frequency to be determined by each State, on the risks, threats and vulnerabilities identified and on the main measures taken to address them;
- Physical security:
    1. Implement a risk analysis process to identify and address the main vulnerabilities that can lead to a serious impact on the Nation;
    2. Make aware and train staff;
    3. Ensure access security: management of identities and access rights, devices aimed at prohibiting or delaying unauthorized penetration, intrusion detection devices;
    4. Ensure security in the face of natural hazards and accidental risks: fire prevention and fire-fighting devices, flood prevention, accident prevention;
    5. Implement redundancies for the most critical installations or power supplies;
    6. Establish and implement an operator security plan (OSP);
    7. Have a periodic physical security audit carried out by a State service or by a provider approved by the State, at least every 5 years;
    8. Establish business continuity and recovery plans;
    9. Participate in training and exercises, at a frequency to be determined by each State;
- Cybersecurity:
    1. Implement a risk analysis process to identify and address the main vulnerabilities that can lead to a serious impact on the Nation;
    2. Transmit to the authorities a map of critical information networks and systems, and update it with each significant change;
    3. Staff awareness and training;
    4. Apply cyber hygiene rules;
    5. Apply security patches on systems and softwares;
    6. Mapp the supply chain and ensure its cyber hygiene;
    7. Take into account the alerts given by the CSIRT;
    8. Ensure network and system security: configurations rules, partitioning, remote access, filtering;
    9. Ensure network and system administration security: rules on accounts and administration systems;
    10. Ensure data security: periodic backup, setting up of redundancies and replication, encryption of storage devices and communication channels, etc.;
    11. Ensure identity and access management: rules on identification, authentication, access rights;
    12. Ensure defence of networks and systems: detection of security incidents, event logging, correlation and analysis of logs;

13. Put in place redundancies for the most critical systems or power supplies;
14. Establish and implement an information security policy (ISP);
15. Perform the security certification of critical information systems;
16. Have a periodic cybersecurity audit by a State service or by a provider approved by the State, at least every 3 years and after each incident and evolution of information systems;
17. Establish business continuity and recovery plans;
18. Participate in training and exercises, at a frequency to be determined by each State.

Reactive measures

1. Promptly notify the public authorities of any incident that could cause a serious impact;
2. Activate mechanisms and systems to collect and disseminate relevant information in a timely manner;
3. Activate the internal crisis management organization in liaison with public authorities (identified and reachable managers, premises, networks, directories, etc.);
4. Activate business continuity and recovery plans.

Proactive measures

1. After resumption of operations, analyse the cause of the disruption;
2. Transmit the results of the analysis to the competent national authorities (including the national cybersecurity authority or the national CSIRT if the incident was caused by a cyber-attack) so that the incident and its causes are integrated into a central database;
3. Incorporate into preventive measures the protection and detection measures resulting from the operator's analysis or from the recommendations transmitted by the competent national authorities.