REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

DRAFT NATIONAL CYBER SECURITY RISK ASSESSMENT METHODOLOGY

CONTENT

Lista of Figures

1. Introduction

Albania has occasionally faced cyber-attacks against operators that provide critical and important services. Continuous efforts in the digitalization of services bring ease and flexibility to the vital, social, and economic functions of citizens. However, on the other hand, they increase the possibility of cyber-attacks, highlighting the growing interdependence and interconnection of information technology systems among them. Additionally, dependence on global supply chains means that organizations are also exposed to systemic cyber risks beyond their direct control, and as a result, they become more vulnerable to the immediate disruptive effects of cyber-attacks.

To understand, improve, and make the most favourable decisions regarding the national cyber security risk position, the National Cyber Security Authority (NCSA) must continuously understand the cyber security risks related to each sector in which Critical Information Infrastructure (CII) and Important Information Infrastructure (III) operate and collaborate in identifying cyber risks. Building trust and cooperation with operators is very important for identifying and mitigating cyber security risks.

This document presents the National Methodology for Cyber Security Risk Assessment (*hereinafter referred to as the Methodology*) for the National Digital Space. The National Cyber Security Authority (NCSA) developed this standardized analytical process through a bottom-up approach (as illustrated in Figure 1), contextualized with cyber threat intelligence and other information. The Methodology is based on international standards[1] and best practices in cyber risk management and is in compliance with the requirements of the European Union Directive (NIS2).

[1] ISO 27001/5, ENISA and NIST SP 800-53

This methodology consists of three main steps:

- Step 1: Critical and Important Information Infrastructure Operators (CIIO/IIIO) conduct individual cyber security risk assessments
- Step 2: The National Cyber Security Authority (NCSA) conducts sectoral cyber security risk assessments.
- Step 3: The National Cyber Security Authority (NCSA) conducts the national cyber security risk assessment.

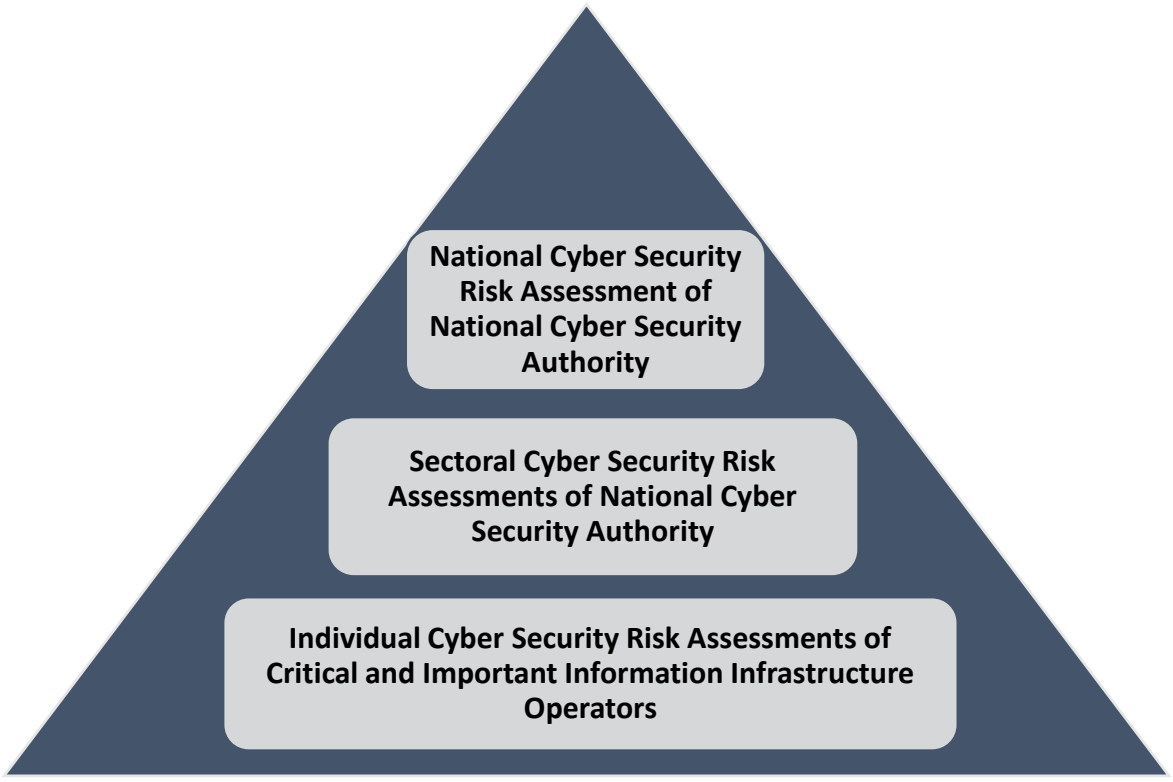

Figure 1 Three levels of cyber security risk assessment

2. Applicability

The National Cyber Security Risk Assessment Methodology is drafted in implementation of Law No. 25/2024, "*On Cyber Security*," to create a unified and transparent approach in assessing cyber risks that threaten important and critical services in Albania

As part of this approach, each Critical and Important Information Infrastructure Operator (CIIO/IIIO) is:

- Responsible for identifying and managing the risks to the organization and the services they provide, by implementing best practices in cyber security and applicable controls in accordance with international standards, to protect and maintain the confidentiality, integrity, and availability "CIA" of their services and data.
- Responsible for conducting periodic cyber risk assessments (at least once a year), or in case of changes classified as major by the operator itself.

CIIO/IIIO may choose their individual decision-making methodology for cyber risk assessment based on international standards, but they must report to the National Cyber Security Authority (NCSA) on the risk assessment according to the specifications in this methodology *(using the template specified by NCSA).*
NCSA will use this methodology to assess cyber risk from the infrastructure level, sectoral level, up to the national level.

3. Purpose

The National Cyber Risk Assessment Methodology aims to provide a comprehensive framework for identifying, assessing, mitigating, and managing cyber risks in critical and important information infrastructures. The methodology ensures the identification of vulnerabilities, assessment of potential impacts, and implementation of effective risk management strategies. It encompasses a range of factors, including threat analysis, asset importance assessment, and resilience planning, enabling operators to enhance cyber resilience and contribute to national security, economic stability, and public safety.

4. Objectives

The objectives of the National Cyber Risk Assessment Methodology, systematically address and manage cyber risks within the national infrastructure and digital ecosystems.

The main objectives include:

- Identifying and assessing cyber threats and vulnerabilities for critical and important information infrastructures
- Prioritizing risks based on their potential impact to ensure the effective allocation of resources.
- Developing strategies to mitigate risks and improve national cyber security.
- Promoting collaboration among stakeholders to foster a unified approach to cyber security.
- Enhancing incident response capabilities to address cyber incidents swiftly and effectively.
- Ensuring the resilience and continuity of critical services in the face of evolving cyber threats.

5. Scope

The methodology focuses on identifying cyber security risks to critical and important services in the country by analyzing factors such as: People, Processes, Technology, Geopolitics (issues directly related to the country's national policy), and Other (elements not related to the aforementioned factors).

Based on this methodology, the National Cyber Security Authority (NCSA) supports the following specific objectives:

a) Risk Assessment: Evaluate the risk of the operator's services (OIKI/OIRI) on a semi-annual basis.
b) Re-assessment: Reassess the cyber risk level of OIKI/OIRI following a major change (as defined in the cyber security law), including changes in:

- System Architecture
- Newly offered services
- Infrastructure
- Third-party supply
- Regulatory framework
- Institutional restructuring
- Cases of significant impact incidents, etc.

6. Information Sources for Cyber Security Risk Assessment

To assess the national cyber security risk, the National Cyber Security Authority, analyzes information received from:

- Critical and Important Information Infrastructure Operators (CIIO/IIIO): Data collected through semi-annual questionnaires (Appendix No. 1).
- Cyber Risk Assessment Reports: Reports from operators detailing their cyber risk evaluations.
- Compliance Assessment Reports: Reports from the Compliance Assessment Authority.
- Internal/External Audit Reports: Reports from internal or external audits conducted by CIIO/IIIO or by NCSA
- Incident and Threat Reports: Reports and analyses conducted by NCSA or CIIO/IIIO related to incidents, threats, tactics, techniques, and procedures (TTPs), vulnerabilities, etc.
- Intelligence and Security Information: Information from intelligence and security services.
- International Partners: Information from international partners and collaborations.
- Media Sources: Information from various media, including social media, news portals, TV, and print media.

7. Critical and Important Infrastructure Operators Risk Register

The register will consist of profiles for operators, including basic information on infrastructures, their architectures, systems, services, and supply chains, as well as data on internal cyber risk assessments based on information generated from audits and tests conducted. In constructing and populating the operator profiles, information will be collected from publicly available data as well as through mandatory questionnaires (Appendix No. 1) initiated and sent to each operator by NCSA

The information used in NCSA's Methodology will be stored in a database known as the *CIIO/IIIO Risk Register*. NCSA will maintain and update this register through proper access management and controls based on the "need-to-know" principle.

8. Implementations steps of the Methodology

To implement the methodology for national-level risk assessment, NCSA will follow these steps:

a. Information Collection

NCSA will conduct the information collection process based on the sources outlined in section 7 of this methodology..

b. Risk Analysis and Assessment

- Analysis of Collected Information: Analysing the data collected by NCSA to identify risks.
- Risk Assessment: Assessing risks quantitatively and qualitatively for each Critical and Important Information Infrastructure Operator (Appendix No. 4).
- Inclusion of Geopolitical and Other Risks: Incorporating geopolitical and other risks into the national risk assessment.
- Risk Prioritization: Prioritizing risks based on their potential impact and severity.
- Sectoral and National Risk Assessment: Evaluating risks at both the sectoral and national levels.

c. Reporting and Monitoring

NCSA prepares the National Cyber Risk Assessment Report twice a year.

Information Infrastructure Operator Risk Assessment Reports will be sent to each CIIO/IIIO

NCSA will continuously monitor and assess cyber risks for their treatment by CIIO/IIIO according to the prioritization schedule defined in Table No. 9