REPUBLIC OF ALBANIA
COUNCIL OF MINISTERS

DECISION

No. 308, dated 04.06.2025

ON

ON ADOPTION OF METHODOLOGY FOR ASSESSING AND ANALYSING CYBERSECURITY RISK

Pursuant to Article 100 of the Constitution and Article 9(ë) of Law no. 25/2024 "On Cybersecurity", upon the proposal of the Prime Minister, the Council of Ministers

HEREBY DECIDED:

1. Adoption of the methodology for the assessment and analysis of cybersecurity risk, in accordance with the text attached to this Decision, which constitutes an integral part thereof.

2. The National Cyber Security Authority and the operators of critical and important information infrastructures are hereby charged with the implementation of this Decision.

This Decision shall enter into force upon its publication in the Official Journal.

PRIME MINISTER
EDI RAMA

In the absence and by order of:
DEPUTY PRIME MINISTER
BELINDA BALLUKU

METHODOLOGY FOR THE ASSESSMENT AND ANALYSIS OF CYBERSECURITY RISK

Contents

List of Figures

List of Tables

1 Introduction

Albania has, on several occasions, been subject to cyberattacks targeting operators that provide critical and important services. Ongoing efforts in the digitalization of services bring convenience and flexibility to citizens' vital, social, and economic functions, but on the other hand, increase the likelihood of cyberattacks, emphasizing the growing interdependence and interconnection of information technology systems among themselves. Furthermore, dependence on global supply chains means that information infrastructure operators are also exposed to systemic cyber risks beyond their direct control and consequently become more vulnerable to the immediate disruptive effects of cyberattacks.

In order to understand, improve, and facilitate the most favorable decision-making within the framework of the national cybersecurity risk position, the National Cyber Security Authority, must constantly understand the cybersecurity risks associated with each sector in which the Critical and Important Information Infrastructure Operators (CII/III) operate and cooperate in the identification of cyber risks. Building trust and collaborating with operators is very fundamental for the identification and mitigation of cybersecurity risks.

This document shall set out the Methodology for Assessment and Analysis of Cyber Security Risk (*hereinafter referred to as the Methodology)* for the National Digital Space. The National Cyber Security Authority (NCSA) conducted this standardized analytical process through the bottom-up approach (as illustrated in Figure 1), contextualized with cyber threat intelligence and other information. The methodology is based on standards[1] and the best international practices of cyber risk management and is in accordance with the provisions of Law no. 25/2024, *"On cybersecurity",* and the requirements of the European Union Directive (NIS2).

This methodology shall consist of three main steps:

- Step 1. NCSA conducts individual cybersecurity risk assessments for operators of critical and important information infrastructures (CII/III) based on the sources defined in point 6 of this Methodology.
- Step 2. NCSA conducts sectoral assessments of cybersecurity risk.
- Step 3. NCSA conducts the national assessment of cybersecurity risk.

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

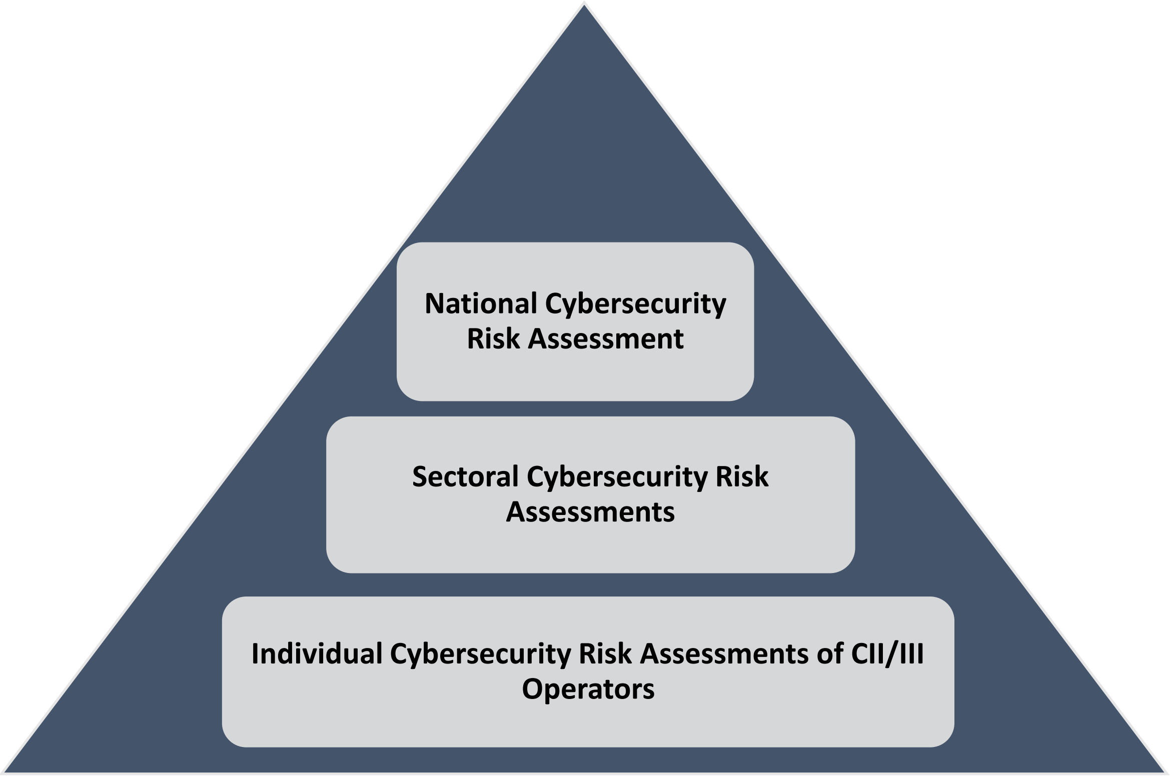
National Cybersecurity Risk Assessment
Sectoral Cybersecurity Risk Assessments
Individual Cybersecurity Risk Assessments of CII/III Operators

Figure 1 three levels of risk assessment

2 Subject matter

The subject matter of this Methodology is to establish a comprehensive framework for the identification, assessment, mitigation, and management of cyber risks in critical and important information infrastructures, with a view to enabling infrastructure operators to strengthen their cyber resilience and contribute to the protection of national security, economic stability, and public safety.

3 Purpose

The purpose of this Methodology is the identification, analysis, and assessment of vulnerabilities in information infrastructures, with the aim of protecting them by addressing these weaknesses and ensuring cyber resilience, thereby raising the overall level of cybersecurity at the national level.

4 Definitions

The terms used in this Methodology shall have the same meaning as those defined in Law no. 25/2024, “On Cybersecurity”

5 Responsibilities of NCSA and CII/III Operators

NCSA shall be responsible for the assessment of cyber risk from the infrastructure level, to the sectoral level, and up to the national level, in accordance with the provisions of this Methodology.

Each CII/III operator shall be responsible for:

- Identifying and managing the risks of the information infrastructure and services they provide, by applying best cybersecurity practices and relevant controls, in compliance with international standards, to protect and preserve the confidentiality, integrity, and availability ("CIA") of their services and data.
- Carrying out periodic cybersecurity risk assessments (at least once per year) or, in the event of changes classified as major, by the operator itself.

CII/III operators may, at their discretion, choose the methodology for conducting the cybersecurity risk assessment, based on international standards, but they shall report to NCSA whenever required on the risk assessment, in accordance with the specifications of this Methodology (as per the format determined by NCSA).

6 Objectives

The main objectives of this methodology shall include:

a) Identifying and assessing cyber threats and vulnerabilities for important and critical information infrastructures.
b) Prioritizing risks based on their potential impact to ensure the effective allocation of resources.
c) Developing strategies aimed at mitigating risks to improve national cybersecurity.
c) Promoting cooperation among interested parties to foster a unified approach to cybersecurity.
d) Improving incident response capabilities to address cyber incidents quickly and effectively.
dh) Ensuring the resilience and continuity of critical services in the face of evolving cyber threats.

6.1 Specific objectives

NCSA shall, based on this methodology, pursue the following specific objectives:

a) Assessing the cyber risk of CII/III services on a semi-annual basis;
b) Reassessing the level of cyber risk of CII/III following a major change in:
   - Architecture of Systems.

- New services provided.
- Infrastructure.
- Third-party supply
- Regulatory framework.
- Restructuring of the institution.
- case of a high-impact incident, etc.

7 Scope of Application

The Methodology shall focus on identifying cybersecurity risks to the services of the country's critical and important information infrastructures, related to the analysis of factors such as: human resources, processes, technology, geopolitics (issues directly linked to the country's national policy), and others (other important elements not included in the above categories, but which may affect cybersecurity and are taken into consideration by NCSA depending on new technological, legal, geopolitical, or operational developments).

8 Sources of Information for Cyber Risk Assessment

To assess the national risk related to the country's cybersecurity, the NCSA shall analyze the information received from:

- CII/III operators through semi-annual questionnaires, approved by order of the Director General of the NCSA.
- Cyber Risk Assessment Reports of operators.
- Reports of the Conformity Assessment Body for cybersecurity.
- Internal/external audit reports from CII/III operators, or controls/inspections carried out by the NCSA at these information infrastructures.
- Reports and analyses conducted by the NCSA or CII/III operators regarding incidents, threats, techniques and tactics and procedures used by the attacker, vulnerabilities, etc.
- Information from the Intelligence, Security and Defense Services.
- Information from international partners.
- Media (social media, online portals, television, print).

9 Risk Registry of CII/III Operators

NCSA shall establish, maintain, and update a risk registry of CII/III operators. The registry will consist of operator profiles, which will include basic information about infrastructures, their architectures, systems, services, supply chains, as well as information on internal cybersecurity risk assessments, based on data generated from controls, audits, testing, reports, and analyses carried out by the NCSA or CII/III operators concerning incidents and cyber threats. In the construction and population of operator profiles, information shall be collected from publicly available data, as well as through mandatory questionnaires initiated and sent to each operator by the NCSA.

NCSA shall maintain and update this registry through proper access management and controls, based on the principle of "need-to-know."

10 Steps for the implementation of the Methodology

For the implementation of the Methodology for for the assessment and analysis of cybersecurity risk at the national level, the NCSA shall follow the steps below:

10.1 Collection of Information

The NCSA carries out the process of collecting information based on the sources defined in point 8 of this Methodology.

10.2 Risk Analysis and Assessment

This phase includes the following steps:

a) The analysis of the information collected by the NCSA for the identification of risks;
b) The risk assessment in quantitative and qualitative formats for each CII/III operator in accordance with point 12 of this Methodology;
c) The inclusion of Geopolitical and Other risks in the national risk assessment;
ç) Prioritization of risks;
d) Assessment of risks at the sectoral and national level.

10.3 Reporting and Monitoring.

The NCSA shall draft, twice a year, the National Risk Assessment and Analysis Report, which will be delivered to the information infrastructure operators.
The NCSA shall continuously monitor and evaluate cyber risk, with the aim of enabling the remediation of risks by CII/III operators, in line with the time-based prioritization set out in Table no. 6 of this Methodology.

11 Assignment of the Survey Weights

11.1 Detailing of Technological Weights (Impact)

According to technological impact, weights reflect the importance and influence that each technical security measure in the "survey" has on the overall security of the system, based on its potential impact on the confidentiality, integrity, and availability (CIA triad) of the data.

11.2 Detailing of Process Weights (Impact)

According to process gaps, the impact shall be the sum of five (5) categories considered under ISO 27005, as follows:

1. **Financial impact**

   a) ***Revenue losses***: Cyberattacks may result in loss of revenue due to operational downtime or service disruption;
   b) ***Recovery costs***: The costs associated with detection, response, and recovery from cyberattacks can be very high;
   c) ***Fraud-related damages***: Involvement in illicit activities, such as identity theft or financial fraud, may cause significant financial harm.

2. **Legal and reputational impact**

   a) ***Sanctions and fines***: Violations of data privacy and security laws and regulations may result in severe sanctions and fines;
   b) ***Criminal prosecution:*** Infrastructure operators may face criminal prosecution and legal liability for failing to adequately protect user data;
   c) ***Loss of customer trust:*** Security incidents can erode the trust of customers and partners, leading to client attrition and potential revenue loss;
   ç)Brand damage: A cyberattack may damage the image and reputation of an information infrastructure operator, potentially having long-term market consequences.

3. **Social impact**

   a) **Privacy breaches**: Cyber risks may cause violations of individuals' privacy and personal data, leading to severe consequences for individuals' private life;
   b) **Impact on citizens' health and safety**: Attacks on healthcare and public safety systems may have serious consequences for citizens' health and safety.

4. **Operational impact**

   a) ***Service disruption***: DDoS (Distributed Denial of Service) attacks and malware can disrupt critical services, hindering the normal functioning of the operator's infrastructure and systems;
   b) ***Data loss:*** Data may be deleted, destroyed, or stolen during cyberattacks, disrupting operations and causing the loss of important information.

5. **Impact on National Security**

   a) **Compromise of critical information infrastructure**: Cyberattacks on critical information infrastructure such as energy, water, and financial services, etc., can threaten national security and the lives of citizens.
   b) **Risk to national defense**: Attacks against government and military systems may threaten national security and affect international relations. Each of the above-mentioned impacts has a weight (0 or 1). The sum of weights determines the total weight of the Organizational Security Measure.

11.3 Detailing of Human Resources Weights (Impact)

Weights reflect the importance and influence that each technical security measure has on the overall security of the system, in accordance with the potential impact they may have on the *human resources gap* (i.e., whether the institution has sufficient human resource capacities in cybersecurity to meet its strategic/operational goals and objectives), as well as on the *professional gap* (i.e., whether the human resources possess adequate experience and qualifications to meet strategic/operational goals and objectives).

The human resources gap identifies and evaluates the difference between the current human resource capacity and the optimal requirements needed. The formula for assessing this gap is based on best practices in the evaluation of technical and organizational capacities in the field of cybersecurity, drawing on the key parameters defined in ISO/IEC 27001 and ISO/IEC 27005 standards regarding human resources.

a) total number of employees.
b) Geographical locations.
c) Critical services.
d) current number of experts.

The formula used in this analysis is as follows:

Human Resources Gap = {(Total number of employees × 0.02[2]) + (Geographical locations ÷ 30[3]) + (Critical services ÷ 4[4])} – Current number of IT + Sec experts.

The professional gap is evaluated based on the weight derived from the level of employee expertise in the field of cybersecurity. This weight is determined by considering years of professional experience, possession of internationally recognized certifications, as well as diplomas or certificates issued by accredited vocational and higher education institutions in the Republic of Albania, in fields such as information technology, cybersecurity, engineering, or computer science.

The following table presents the weighting from the perspective of the professional gap:

Table 1 Weight according to the Professional Gap

Years of Experience in the field of cyber security	International certifications in the field of cybersecurity	Weight
3	0	1
2	1	1
1	2	1
2	0	2
1	1	2
1	0	3
0	1	4
0	0	5

12 Risk Assessment

This phase explains the process of cybersecurity risk assessment and analysis applied in this Methodology, including the identification, evaluation, and remediation of national cyber risks that may affect the country's critical and important information infrastructures.

The cybersecurity risk assessment and analysis methodology employs a systematic approach and a structured model for analyzing typical risk factors, which include the likelihood and impact on services in terms of loss of ***confidentiality, integrity, and/or availability (CIA)*** of data and/or the functionality of a critical or important service.

The risk factors shall include the following:

- Threat – What could occur that may damage and/or disrupt the normal functioning of a given service?
- Vulnerability – Weak points in the system/architecture that may be exploited by a threat vector with the aim of causing malfunction or disruption.

[2] The multiplication of the total number of employees by 0.02 reflects a small but significant portion of the workforce required to maintain optimal operations.

[3] The division of the number of geographical locations by 30 serves to normalize the data, thereby ensuring comparability with the other parameters.

[4] The division of critical services by 4 accounts for the significance of these services in the overall operational efficiency.

- Likelihood/Frequency (Exposure) – The likelihood that a threat will exploit a vulnerability to cause a negative impact.
- Impact/Severity of Consequences – If a threat materializes, the level of severity of the potential impact it could have on the functioning of the relevant service or infrastructure. This assessment is carried out in a contextualized manner, based on data collected through surveys, audits, and other relevant sources, as well as on the professional analysis of the assessment staff. This approach ensures flexibility and adaptability to the specific reality of each sector or infrastructure, avoiding the limitations that would arise from an assessment based solely on standardized scenarios.

The methodology shall analyze these risk factors in the context of ***Human Resources, Processes and Technology*** in order to determine the cybersecurity risk for CII/III operators.

To group the identified risks, the Methodology applies three (3) main gaps, as follows:

1. **The Human Resources Gap**

- Insufficient staff: An inadequate number of personnel to effectively identify, assess, and manage cybersecurity risks.
- Lack of specialized knowledge: Employees may lack the necessary expertise in risk management, data analysis, or cybersecurity.
- Lack of training and awareness: Insufficient training and awareness programs for employees to address cybersecurity risks

2. **The Process Gap**

2.1 Operational Gap. These are deficiencies in the processes or practices related to the management and protection of information systems and data. Examples include inadequate incident response plans, lack of regular security audits, insufficient compliance and penetration testing, failure to consistently enforce security policies, inadequate security updates and patching of identified software vulnerabilities, failure to review and act upon threat intelligence, and failure to mitigate/remediate vulnerabilities discovered during testing, etc.

2.2 *Management gap* This refers to the absence of a clear and documented framework for managing cyber risk, including the lack of internal mechanisms for strategic decision-making related to such risks. This gap does not concern the content of the operator's specific priorities, which remain its exclusive responsibility, but rather the existence or absence of a structured approach for their management.

2.3 *Policy and Compliance Gap*. These occur when an infrastructure operator fails to meet regulatory requirements or industry standards for data protection and information security. This may be due to outdated policies, lack of awareness of regulatory changes, inadequate controls to ensure compliance with standards, or failure to meet the Risk Remediation Plan.

3. Technology Gap

The technology gap occurs when there is a lack of necessary technological solutions to protect against current and emerging cyber threats. This may include outdated security systems, lack of advanced tools for threat detection, insufficient security features in the existing IT infrastructure, or failure to apply best practices such as “defense in depth,” network segmentation into public and private networks, etc.

For each of the above categories, the associated risks have been identified as integral components, while the risk assessment table also specifies the impacted components of the CIA triad (confidentiality, integrity, and availability) for each finding that results in a risk.

For the purposes of this Methodology, risk shall be measured in terms of likelihood and impact, i.e., the likelihood of an event occurring in combination with its consequence.

***Likelihood Assessment**:* A numerical value representing the probability of a risk occurring. This value is determined on a scale from 1 to 5, where 1 represents a very low probability and 5 represents a very high probability of occurrence.

Impact Assessment: A numerical value representing the impact of the risk, should it occur, in financial, health, environmental, or other terms. This value is also determined on a scale from 1 to 5, where 1 represents a negligible impact and 5 represents a critical or extremely high impact.

The calculation of the risk value shall be the product of the likelihood and impact values, which will be computed according to the following formula:

RISK VALUE = LIKELIHOOD * IMPACT

12.1 Likelihood of Occurrence

The likelihood of occurrence is based on the probability that an event will materialize. The key factors to be considered in assessing the likelihood of occurrence include, but are not limited to:

- The architecture and environment of the information system.
- Access to systems, cyber resilience, the strength and nature of the threat.
- Vulnerabilities and the effectiveness of existing controls, etc.

Based on the likelihood of occurrence, Table No. 2 below defines the likelihood assessment of risks, divided into five categories (very low (1), low (2), medium (3), high (4), and very high (5)), according to the likelihood of the risk materializing over time.

Table 2 Likelihood of Occurrence by Expected Frequency

Likelihood of occurrence	Description
1	Annual
2	Quarterly (2-4 times per year)
3	Monthly (5-12 times per year)
4	Weekly (13-52 times per year)
5	Daily (>52 times per year)

Table no. 3 presents the Likelihood of Occurrence by categories in terms of the CIA data triad.

Table 3 Likelihood of Occurrence by categories from 1 to 5 and the triad of Confidentiality, Integrity, and Availability of data in total and by the respective components

Categorization		CIA	Confidentiality	Integrity	Availability
1	**Very Low**	There is a very low likelihood that a threat will materialize and impact the CIA triad.	There is a very low likelihood that sensitive information will be disclosed in an unauthorized manner. Advanced processes and technologies operate effectively to protect the data.	There is a very low likelihood that sensitive information will be modified in an unauthorized manner, thanks to strong access control and auditing mechanisms.	There is a very low likelihood that sensitive information will become unavailable, as a result of the adoption of strong compensatory measures.
2	**Low**	There is a relatively low likelihood that a threat will materialize and impact the CIA triad.	There is a low probability that confidential data will be disclosed, but the protective measures are relatively sufficient to prevent most attacks.	There is a low probability that data will be compromised, but controls and corrective measures are in place to quickly detect and remedy unauthorized modifications..	There is a low probability that a system will become unavailable, but regular maintenance and testing procedures help minimize this risk.
3	**Medium**	Threats are possible and may occur if protection measures are not implemented.	It is possible that confidential information may be disclosed without authorization if attackers exploit identified/unidentified vulnerabilities. Protective measures have been implemented, but continuous improvements are required.	There is a medium probability that data may be altered in an unauthorized manner, particularly if attackers gain internal access or exploit system vulnerabilities.	It is possible that a system may become unavailable due to technical failure.
4	**High**	Threats are possible and expected to occur if preventive measures are not taken.	It is possible that confidential data may be exposed due to a range of factors, including sophisticated attacks or internal system vulnerabilities. Protective	It is possible that data may be modified without authorization, particularly given the lack of effective implementation of access	There is a high probability that a system may become unavailable due to persistent attacks or technical failures of equipment.

				measures have not been effectively implemented.	control measures and continuous monitori	
5	**Very High**	Threats are potentialy certain to occur and will impact the CIA triad.		It is almost certain that confidential data will be exposed if urgent and effective protective measures are not implemented, particularly in cases of sophisticated attacks.	It is almost certain that data will be modified without authorization due to the complete absence of access controls and monitoring	It is almost certain that a system will become unavailable for a significant period of time, especially if sophisticated attacks exploit identified/unidentified vulnerabilities or the absence of adequate protections.

12.2 Impact

The impact assessment shall be carried out based on the analysis of the effect it would have on the cybersecurity of the infrastructure within the gaps in technical capacities, processes, and human resources, as well as the specific weights defined for each category, according to the surveys to be submitted to CII/III operators by the NCSA under this Methodology.

Table no. 4 presents the impact severity according to categories in terms of the data triad: confidentiality, integrity, and availability of data.

Table 4 Impact Severity by Categories from 1 to 5 and the Data Triad of Confidentiality, Integrity, and Availability, in Total and by Respective Components

Categorization		CIA	Confidentiality	Integrity	Availability
1	Very Low	Unauthorized disclosure, modification, or corruption of information, as well as disruption of access/use of IT systems or networks, is expected to have a negligible impact on the organization/company. The effects are easily manageable and are not expected to cause damage or service disruption.	A negligible breach of confidentiality that does not affect data. No effect or consequences for the organization or individuals	Negligible and insignificant changes to non-sensitive data that do not affect operations. No effect or consequences for the organization or individuals.	Minor or insignificant disruption that does not affect critical business functions or core services. Service is restored quickly without significant impacts.
2	Low	Unauthorized disclosure, modification, or corruption of information, as well as disruption of access/use of IT systems or networks, is expected to have a low impact on the organization/company. The effects are limited and manageable with existing resources and continuity procedures for service delivery	A negligible breach of confidentiality that does not affect sensitive data. The effect is minimal and has no consequences for the organization or individuals.	Changes to non-sensitive data that do not affect operations. No effect or consequences for the organization or individuals.	Service disruption affecting non-critical functions. The service is restored within a short period of time with minimal consequences.

3	Moderate	Unauthorized disclosure, modification, or corruption of information, as well as disruption of access/use of IT systems or networks, is expected to have a moderate impact on the organization/company. The effects in this category have the potential to cause service disruptions if mitigation or elimination measures are not undertaken.		A breach affecting a limited amount of sensitive data with restricted impact. The exposure may have negative consequences for individuals or the organization and requires corrective measures.	Changes to sensitive data that have a moderate effect on operations. Correction requires time and resources.	A disruption affecting several critical functions. Recovery requires significant time and effort, with moderate consequences for the organization.
4	High	Unauthorized disclosure, modification, or corruption of information, as well as disruption of access/use of IT systems or networks, is expected to have a serious, high impact on the organization/company. The effects are significant and may cause major service disruptions if not addressed promptly and if appropriate measures for ensuring service continuity are not taken.		A significant breach affecting a relatively large amount of sensitive data. The consequences are extensive and may include major financial loss or reputational damage.	Major alterations to sensitive data that affect operations and decision-making. Correction requires substantial time and resource efforts.	A major disruption affecting most critical functions. Recovery is complex and requires extensive resources, with severe consequences for the organization.
5	Very High / Critical	Unauthorized disclosure, modification, or corruption of information, as well as disruption of access/use of IT systems or networks, is expected to have an extremely severe, critical impact on the organization/company. The effects are at the highest level and require immediate attention. There is a very high potential for serious, irreparable damage,		A very severe breach affecting a substantial amount of sensitive data. The consequences are catastrophic, including major financial loss, reputational damage, and legal implications.	Fundamental alterations to sensitive data that severely compromise operations and decision-making. The consequences are catastrophic and require extensive recovery and remediation efforts.	A very severe disruption affecting all critical functions. Recovery is extremely complex and requires extraordinary resources, with catastrophic consequences for the organization.

	🟥	endangering business continuity and service delivery beyond the tolerated downtime.		🟥	🟥	🟥

12.3 Risk Assessment

The purpose of a risk matrix, which combines likelihood of occurrence and impact into a single metric (*likelihood of occurrence* × *impact*), is to evaluate and prioritize risks effectively.

The purpose of risk assessment is the prioritization of risks and decision-making on which risks may be accepted, and which must be treated. Risks classified as "very low" and "low," based on the product of likelihood and impact, will be considered as acceptable risks by the NCSA. For all other risk categories, critical and important information infrastructures shall be responsible for defining their risk remediation and mitigation plans, based on their respective methodologies.

The matrix in Table No. 5 shows the risk classifications, where the green areas indicate that the risk is within an acceptable threshold, while the yellow, orange, and red zones indicate that a risk does not meet NCSA's acceptance criteria and, therefore, must be addressed with the appropriate mitigation measures. Table No. 6 sets out the prioritization of remediation according to the risk matrix.

Table 5 Quantitative production (Risk Score) of likelihood of occurrence and impact

Risk = Likelihood Occurrence * Impact Severity

		IMPACT				
		Very low (1)	**Low (2)**	**Moderate (3)**	**High (4)**	**Very high/Critical (5)**
LIKELIHOOD OCCURRENCE	**Very low (1)**	1	2	3	4	5
	Low (2)	2	4	6	8	10
	Medium (3)	3	6	9	12	15
	High (4)	4	8	12	16	20
	Very high (5)	5	10	15	20	25

Risks shall be prioritized for remediation by CII/III operators according to their quantitative product and classification, so that risks with a quantitative product classified as **"High"** or **"Very High"** are recommended to be addressed before risks with lower levels for infrastructure operators.

Table 6 Prioritization of Remediation According to the Risk Matrix

Risk Value	Risk level	Remediation Time
[1-3]	Very low	No remediation required
[4-6]	Low	No remediation required
[7-11]	Medium	Requires remediation within 12 months
[12-19]	High	Requires remediation within 6 months
[20-25]	Very high	Requires remediation within 3 months