REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.2007 Prot Tiranë më 11.06.2025

UDHËZIM

Nr. 1, datë 11.06.2025

PËR

MIRATIMIN E METODOLOGJISË SË VLERËSIMIT TË RISKUT TË INFRASTRUKTURËS PAS NDODHJES SË NJË INCIDENTI KIBERNETIK

Bazuar në shkronjën "gj" të nenit 13 të ligjit nr. 25/2024 "Për sigurinë kibernetike",

UDHËZOJ:

1. Miratimin e metodologjisë së vlerësimit të riskut të infrastrukturës pas ndodhjes së një incidenti kibernetik, sipas tekstit që i bashkëlidhet këtij udhëzimi.

2. Ngarkohet Autoriteti Kombëtar për Sigurinë Kibernetike dhe operatorët e infrastrukturave të informacionit për zbatimin e këtij udhëzimi.

Ky udhëzim hyn në fuqi menjëherë.

DREJTORI I PËRGJITHSHËM

IGLI TAFA

REPUBLIKA E SHQIPËRISË AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE KËSHILLI I MINISTRAVE

REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

No. 2007 Prot. Tirana, on 11.06.2025

DIRECTIVE

No. 1, dated 11.06.2025

ON

"APPROVAL OF THE METHODOLOGY FOR INFRASTRUCTURE RISK ASSESSMENT FOLLOWING A CYBER INCIDENT"

Pursuant to letter "gj" of article 13 of law no. 25/2024, "On Cyber Security,"

IT IS HEREBY DIRECTED:

1. The methodology for infrastructure risk assessment following the occurrence of a cyber incident is hereby approved, according to the text attached to this Directive and forming an integral part thereof.
2. The National Cyber Security Authority and the operators of information infrastructures are charged with the implementation of this Instruction.

This Directive shall enter into force immediately.

GENERAL DIRECTOR

IGLI TAFA
[Signature and Official Seal of the National Cyber Security Authority]

Address: Rruga "Papa Gjon Pali II" No. 3, Tirana
Website: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel/Fax: 04 2221 039

METHODOLOGY FOR INFRASTRUCTURE RISK ASSESSMENT FOLLOWING A CYBER INCIDENT

I. GENERAL PROVISIONS

1. The object of this methodology is the definition of the rules through which the risk assessment of information infrastructure is carried out following the occurrence of a cybersecurity incident, when the service provided by the infrastructure has ceased to function for more than 4 hours.
2. The purpose of this methodology is to assess the impact, vulnerabilities, and the probability of recurrence of the cybersecurity incident, as well as to undertake reactive actions by the National CSIRT and information infrastructure operators to reduce risk and improve the response to future cyber incidents.
3. This methodology is issued pursuant to letter "gj" of Article 13 of Law no. 25/2024, "On Cybersecurity."
4. This methodology shall be applied by the National Cyber Security Authority (NCSA) and the operators of information infrastructures.
5. The terms used in this methodology shall have the same meaning as those defined in Law no. 25/2024, "On Cybersecurity."

II. PHASES FOR THE RISK ASSESSMENT OF INFORMATION INFRASTRUCTURE FOLLOWING A CYBER INCIDENT

1. The methodology for the risk assessment of information infrastructure following the occurrence of a cyber incident includes the following phases:

1.1. Identification and Documentation of the Cyber Incident

This phase includes the process of identifying and documenting the cybersecurity incident in order to assess its nature and scope, through the following steps:

- Describing the cyber incident, including the date and time when it occurred.
- Identifying the type of cyber incident (e.g., ransomware, data breach, DDoS attack).
- Identifying the affected systems, assets, and services that were disrupted.
- Documenting how the cyber incident was detected (security monitoring, user reporting, etc.).

1.2. Vulnerability Assessment

This phase includes the evaluation of vulnerabilities to identify the cyberattack that occurred as well as the weaknesses that were exploited, through the following steps:

- Analyzing the entry points used by the attackers.
- Determining whether the system had technical weaknesses, such as:

- Outdated systems, lack of multi-factor authentication, or software with known vulnerabilities.
- Weak security policies for managing passwords or privileged access.
- Insufficient staff training to detect *phishing or social engineering attacks.*

1.3. Impact Assessment of the Cyber Incident

1.3.1 This phase involves the assessment of the impact of the cyber incident in order to determine its effects on the operations and critical assets of the information infrastructure. This assessment includes the following steps:

- Impact on operations: Assessing whether the cyber incident caused interruptions in the delivery of critical services.
- Data loss: Identifying whether data has been stolen, altered, or permanently lost, and classifying the affected data (personal, financial, commercial).
- Financial impact: Calculating financial losses resulting from service disruptions, reputational damage, administrative measures, or repair costs.
- Reputational impact: Evaluating the impact the cyber incident had on customer trust and partnerships.

1.3.2 The determination of the impact assessment of the cybersecurity incident shall be made based on the following table:

Categorizations (Types) of incidents	Description (Impact)
CYBER INCIDENTS WITH LOW IMPACT	Refers to incidents with a low impact that mainly have minimal and manageable consequences. These incidents can be addressed through standard operating procedures without the need for special intervention.
CYBER INCIDENTS WITH MEDIUM IMPACT	Represents incidents with a medium impact that may have limited consequences on the integrity, availability, or confidentiality of systems or data. They require a coordinated response to address vulnerabilities and restore normal services.
CYBER INCIDENTS WITH HIGH IMPACT	Refers to a severe incident with a high impact on critical operations or sensitive data. It requires the rapid mobilization of incident response teams and may involve notifying stakeholders and regulatory authorities.

- **Low:** Minimal impact on the operations or data of the information infrastructure.
- **Medium:** Significant impact but contained within certain services of the information infrastructure.

- **High:** Major impact on critical operations or leakage of sensitive data with severe consequences.

1.4. Assessment of the Probability of Cyber Incident Recurrence

1.4.1 This phase involves assessing the likelihood of recurrence of the cyber incident in order to prevent its occurrence in the future. This assessment includes the following steps:

- Incident history: Is this an isolated incident, or does it show a recurring pattern?
- Current protection measures: Are the existing security measures sufficient to prevent a similar incident in the future?
- Possible improvements: Have security improvements been identified and implemented following the cyber incident?

1.4.2 The determination of the likelihood (probability) of recurrence of the cyber incident shall be carried out according to the following indicators:

Possibility (Probability)	Description
Low	There is a low likelihood of occurrence
Medium	There is a reasonable likelihood of occurrence
High	It is almost certain to occur

1.5. Cyber risk analysis

1.5.1 This phase involves the analysis of cyber risk in order to determine the overall risk faced by the information infrastructure following the occurrence of a cyber incident.

1.5.2 To determine the overall level of risk to the information infrastructure, the assessment shall be carried out by combining the impact and the likelihood of recurrence of the cyber incident.

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

Risk matrix:

Risk = Likelihood of Occurrence * Impact

		POSSIBILITY		
		Low (1)	**Medium (2)**	**High (3)**
IMPACT	**Low (1)**	**Low (1)**	**Low (2)**	**Medium (3)**
	Medium (2)	**Low (2)**	**Medium (4)**	**High (6)**
	High (3)	**Medium (3)**	**High (6)**	**High (9)**

Risk Value and Level:

Risk Value	Risk Level
[1-2]	Low
[3-4]	Medium
[6-9]	High

1.6. Categorization of Incidents and Risk Level

By analyzing the type of incident as well as the affected infrastructure, the corresponding risk level is determined according to the following table:

No.	CATEGORIES OF INCIDENTS	SUBCATEGORIES OF INCIDENTS	DESCRIPTION
1	**Abusive content**	Spam	Mass emailing without the recipient's approval, which may contain malware or fraudulent schemes aimed at compromising the security of users' information.
		Harmful speech	Defamation or discrimination of an individual (e.g., cyberstalking, racism, and threats against one or more persons).
		Online content that is violent/sexual/abusive towards children	Child pornography, distribution of violent materials, etc.
		Deliberate misinformation	Distortion of information, which aims to cause panic.

2	**Malicious code**	*Virus* targeting critical services	*Virus* targeting other services	Software that is intentionally installed on a system for malicious purposes.
		Worm targeting critical services	*Worm* targeting other services	
		Trojan targeting critical services	Trojan targeting other services	
		SpyWare towards critical services	*Spyware* targeting other services	
		Dialler towards critical services	*Dialler* targeting other services	
		Rootkit towards critical services	*Rootkit* targeting other services	
		Ransomware targeting critical systems	Ransomware targeting other systems	Malicious code that encrypts data on an end-user's computer systems and/or servers.
		Erasure of data *(wiper)* in critical systems	Erasure of data *(wiper)*targeting other systems	Malicious code intended to destroy or erase data from the affected system, rendering the data unusable or causing the system to become inoperable.

3	**Information Gathering**	Scanning		Requests aimed at discovering a system's vulnerabilities. This incident category also includes testing activities intended to gather information about hosts, services, and accounts. Examples: finger, DNS queries, RCE attempts, ICMP, SMTP (EXPN, RCPT, etc.), and port scanning.
		Sniffing targeting critical services	*Sniffing* targeting other services	Monitoring and logging of network traffic (eavesdropping / packet capture).
		Social engineering		Collection of information from end users by non-technical means (e.g., fraud, shoulder surfing, tailgating, piggybacking, espionage, or threats).
4	**Intrusion attempts**	Exploitation of known vulnerabilities to access critical services	Exploitation of known vulnerabilities to access other services	Attempts to compromise a system or disrupt services by exploiting vulnerabilities, e.g., backdoor, fragmentation, etc.
		Login attempts		Multiple login attempts, e.g., guessing/cracking of passwords, dictionary attack, brute force, RCE.
		0-day attack against critical services	*0-day attack against other services*	Attempts to intrude using an unknown exploit.

		Compromise of privileged accounts		Application (service) compromise. This incident may be caused by a known or new vulnerability, or by unauthorized local access.
5	**Intrusions**	Compromise of non-privileged accounts		Application (service) compromise. This incident may be caused by a known or new vulnerability, or by unauthorized local access.
		Compromise of an application providing critical services	Compromise of an application providing other services	For example, execution of injection techniques such as SQL Injection, Command Injection, File Injection, XSS, CSRF, RCE, API attack, etc.
6	**Availability**	DoS/DDoS that has disrupted critical services		DoS is a cyberattack tactic in which a computer system is used to flood a server, service, or network with excessive traffic in order to cause overload and prevent the normal use of the service by legitimate users. When more than one infected computer system is involved, it is categorized as DDoS. DDoS often relies on DoS attacks originating from botnets, but there are also other scenarios such as DNS Amplification attacks. Some examples include ICMP flood, SYN, Teardrop attacks, and mail-bombing. Availability can also be affected by local actions (destruction, power supply interruption, etc.) or by catastrophic natural events, spontaneous failures, or human errors, without involving malicious intent or negligence.
		DoS/DDoS that has significantly affected critical services and/or has interrupted other services		

		DoS/DDoS that does not impact critical services but has significantly affected other services.		
		Sabotage that has affected the critical system	Sabotage that has affected other systems	
		Interruption of services as a result of an incident during the maintenance process and/or technical issues such as: power/fire/flood affecting critical infrastructure	Interruption of services as a result of the maintenance process and/or technical issues such as: power/fire/flood affecting other services	
		Interruption due to natural disasters that have affected critical infrastructure	Interruption due to natural disasters affecting other services	
7	**Information Content Security**	Unauthorized access to critical services	Unauthorized access to other services	The security of information content may be compromised by the successful compromise of accounts, applications, data, and systems. In addition, attacks can eavesdrop on and access information during transmission (wiretapping, spoofing, or hijacking). These attacks can be caused by human errors, configuration mistakes, or software errors.

		Unauthorized modification to critical services	Unauthorized modification to other services	
8	**Fraud**	Unauthorized use of resources		Unauthorized use of resources for personal gain unrelated to work activities, such as chain letters, using work email accounts to register on platforms unrelated to job activities, etc.
		Copyright		The provision or installation of unlicensed copies of commercial software or other copyright-protected materials.
		Camouflage/Masquerading		An attack technique in which an individual or process attempts to gain unauthorized access to resources or data by impersonating a legitimate entity. This is done by falsifying their identity, for example by using stolen credentials for authentication or by manipulating network protocols to deceive security systems into believing that traffic or requests originate from an authorized source.
		Phishing / Spear Phishing / Whaling / Smishing / Vishing		Phishing / Spear Phishing / Whaling / Smishing / Vishing — Phishing is a fraudulent technique aimed at obtaining sensitive information via emails, messages, or phone calls; it may be targeted (spear phishing), directed at senior executives (whaling), or untargeted, and the sender purports to be a legitimate entity.
9	**Vulnerability**			

		Vulnerabilities exposed to abuse in critical services	Vulnerabilities exposed to abuse in important services	Vulnerabilities exposed to abuse in other services	Vulnerabilities that are publicly disclosed by unauthorized parties and pertain to the services of an information infrastructure.
10	**Cryptomining**	Cryptomining in critical systems or in other systems			The exploitation of resources for profit through cryptocurrency mining (e.g., Bitcoin).
11	**Exfiltration**	Data exfiltration from critical infrastructure systems to a C2 server		Data exfiltration from other infrastructure systems to a C2 server	The unauthorized exfiltration of data from infrastructure systems to a C2 (command-and-control) server for malicious purposes.
12	**Incident in a testing environment**	Incident occurring in a testing environment for critical systems or other systems			Misuse of sensitive data in testing environments, e.g.: in the financial sector when a new system is implemented, and real customer data is used the PCI DSS standard should be applied: obtain authorization for data use and ultimately destroy the data permanently.

1.7. Determination of Corrective and Preventive Measures

This phase includes the determination of corrective and preventive measures aimed at improving the security of the information infrastructure as well as preventing the recurrence of the cyber incident in the future. This phase includes:

- Technical improvements: Implementation of protective measures such as stronger firewalls, IDS/IPS, enhanced encryption levels, and improved password policies.
- Policies and procedures: Reviewing and improving security policies for data and access management.
- Staff training: Increasing staff awareness through continuous and periodic trainings, including regular phishing attack simulations, workshops on secure password management, and awareness programs on emerging threats such as AI-driven attacks.
- Continuous monitoring: Ongoing monitoring to detect anomalies and signs of potential future attacks.

1.8. Recommendations, Recovery Plan, and Reporting

This phase includes providing recommendations, measures to be taken for recovery from the cybersecurity incident, as well as reporting for the purpose of assessing and documenting results and actions. This phase includes:

- Final report: Preparation of a final report that includes a description of the cyber incident, its impact, risk, and the measures taken, along with recommendations for continuity.
- Follow-up on implemented measures: Ensuring that corrective and preventive measures have been implemented and are effective.
- Reporting to stakeholders: Informing stakeholders about the cyber incident and the measures undertaken.
- Recovery plan: Drafting a plan for the rapid recovery of services and restoring user trust.