NIS2 in Croatia

NIS 2 transposition with the new role of the NRA

RIPE NCC 6th SEE Roundtable meeting, Belgrade

April 2026

HAKOM

CONTENT

- NIS2 basic requirements
- Transposition of the NIS2 in Croatia - timeline
- New organization after NIS2 transposition
- NIS 2 Sectors and Authorities
- National Crisis Management Programme
- National Incident Reporting Platform - (PiXi)
- Role of the NRA in the new set-up and what we have done so far
- What are the main challenges at the moment

Basic requirements of NIS2 and the new Cybersecurity Act (ZKS)

- A response to the high level of **dependence of modern society on digital technology** and a foundation for further economic development
- An organizational way **to manage cybersecurity** and be prepared for the further rapid development of digital technology
- Development of a **cybersecurity risk management culture**

Transposition of the NIS2 in Croatia - timeline

- The new Cyber Security Act (NN 14/2024)-issued by the national working group (Q1/2024)
- National Regulation (NN 135/24) - national working group (Q4 2024)
- National Cyber Crisis Management Programme –Security and Intelligence Agency (SOA) Q1/2025
- The Guideline for competent authorities on national cybersecurity risk assessment - (SOA) (Q1/2025)
- The Guideline for conducting a cybersecurity self-assessment – –issued by Cyber Security Certification Authority (ZSIS) (Q2/2025):
    - Appendix A - Calculator for cyber security self-assessment,
    - Annex B - Framework for evaluation of cyber security risk management measures,
    - Appendix C - Catalog of controls (145- mainly ISO and NIST standards) for the implementation of security measures from the Regulation
- National Certification Scheme for the Revision – ZSIS-Q3/2025
- New National Cyber Security Strategy- national working group - 2026

New organization after NIS2 transposition

SECTORAL AUTHORITIES

- HNB – Croatian National Bank
- HANFA – Croatian Financial Services Supervisory Agency
- HACZ – Croatian Civil Aviation Agency
- MZOM - Ministry of Science, Education and Youth
- HAKOM - Croatian regulatory authority for network industries
- MPUDT - Ministry of Justice, Public Administration and Digital Transformation

Security and Intelligence Agency

National Cyber Security Centre
NCSC-HR (www.ncsc.hr)

- Central national cyber security authority
- Single point of contact
- Government CERT and Sectoral CSIRT
- Nacionalni SOC SK@UT System
- Cyber Crisis Management Authority – Croatian CyCLO

MoI
Cyber Crime, CER Directive

ZSIS
Cyber Security Certification Authority

CARNET
National CERT, Sectorial CSIRT

MoD
Military CERT

5

New organization after NIS2 transposition

Results of the NIS2 transposition :

- the **Security and Intelligence Agency** of the Republic of Croatia (**SOA**) became the national cybersecurity authority (NCSC-HR),
- a **National Cyber Security Centre** (**NCSC-HR**) established as part of SOA

The roles of NCSC-HR:

- Central national cyber security authority (policy@ncsc.hr)
- Single point of contact (SPOC@ncsc.hr)
- Cyber Crisis Management Authority – Croatian CyCLO in EU-CyCLONe since **2020**
- National Security Operation Centre (SOC) w/distributed sensor network [SK@UT] – since **2019**
- Sectoral competent authority for most of the NIS2 sectors (policy@ncsc.hr)
- Government CERT and CSIRT for most of the NIS2Dsectors (CSIRT@ncsc.hr)

The role of the sectoral authorities like (HAKOM):

- Sectoral competent authority (ECS/N)

NIS 2 Sectors and Competent Authorities

SECTORS – Annex I	COMPETENT AUTHORITY	CSIRT
ENERGY	NCSC-HR	**NCSC-HR**
TRANSPORT	NCSC-HR HACZ	**NCSC-HR**
BANKING	HNB	**NCERT**
FINANCIAL MARKET INFRASTRUCTURE	HANFA	**NCERT**
HEALTH	NCSC-HR	**NCSC-HR**
DRINKING WATER	NCSC-HR	**NCSC-HR**
WASTE WATER	NCSC-HR	**NCSC-HR**
DIGITAL INFRASTRUCTURE **(ECS/N)**	NCSC-HR MZOM MPUDT **HAKOM**	**NCERT** **NCSC-HR**
ICT SERVICE MANAGEMENT (B2B)	NCSC-HR	**NCSC-HR**
PUBLIC SECTOR	UVNS	**NCSC-HR**
SPACE	NCSC-HR	**NCSC-HR**

SECTORS – Annex II	COMPETENT AUTHORITY	CSIRT
POSTAL AND COURIER SERVICES	NCSC-HR	**NCSC-HR**
WASTE MANAGEMENT	NCSC-HR	**NCSC-HR**
MANUFACTURE, PRODUCTION AND DISTRIBUTION OF CHEMICALS	NCSC-HR	**NCSC-HR**
PRODUCTION, PROCESSING AND DISTRIBUTION OF FOOD	NCSC-HR	**NCSC-HR**
MANUFACTURING	NCSC-HR	**NCSC-HR**
DIGITAL PROVIDERS	NCSC-HR	**NCSC-HR**
RESEARCH	MZOM	**NCERT**
EDUCATION	MZOM	**NCERT**

7

Coordination in the National Cyber Crisis Management Programme

Strategic and Political Level

National Security Council

- **Homeland Security Coordination**
  - Civil Protection, Emergency Services, …

Full Life Cycle:
- **Regular** operating mode
- **Warning** mode of operation
- **Crisis** mode of operation

Operational Level

Cyber Crisis Management Authority (SOA/NCSC-HR)

- **Cyber Crisis Management Coordination**
  - **NCSC-HR**, MoI, MoD, MZOM, UVNS, ZSIS, MPUDT, HAKOM, CARNET, HNB, HANFA, HACZ

Participating institutions have their internal SOP

Sectorial and Functional Authorities

- CERT/CSIRT/SOC technical authorities
- Functional areas as cyber crime, cyber espionage, military, …
- Sectorial Competent Authorities

Escalation Process:

1. **Warning Mode -** Operational Level responsibility with information to the Strategic and Political Level
2. **Crisis Mode -** Operational level and the Strategic and Political Level as needed

PIXI Incident Reporting Platform

- National platform for reporting significant incidents according to the Cybersecurity Act (Article 43) and the Law on the Implementation of the Dora Regulation, for reporting and exchanging information on other incidents, near misses and cyber threats
- PiXi Platform – CARNET- one of the two national CSIRT (another one is NCSC-HR)
- Enables easier reporting to the national and EU authorities
- Accelerates the process of informing the Single Point of Contact and their timely reaction in case of cross-border or cross-sectoral impact of the incident

Role of the HAKOM in the new set-up and what we have done so far

- HAKOM remained the competent authority for the ECS/N sector
- Collected data:
  - total revenues of the company and
  - total number of employees
- According to *Guidelines for competent authorities on national cybersecurity risk assessment* we made national cybersecurity risk assessment for each operator within the initial categorization process
  - each subject is categorized as a essential or important entities

Role of the HAKOM in the new set-up and what we have done so far

- The national risk assessment is carried out based on data:

  a) the size of the entity (small, medium or large based on EU size criteria) and

  b) cybersecurity risks calculator (issued by NCSC). NCSC use all available experience at the global and national level of cybersecurity.

- HAKOM categorized 94 operators until the end of March (**9** essentials and **85** important entities) and **33** operators were additionally categorized as important entities in July 2025.

- So far, the total number of categorized operators is **127**.

The current challenges

1. There are still no clear procedures for cross-border cooperation between EU member states (e.g. for cross-border incidents or oversight obligations for an entity that provides a service in Croatia but is registered and has its infrastructure in another EU country)

2. Some ECS/N providers have their headquarters in one EU member state but provide services in multiple EU member states, some of them without any infrastructure in those other member states and therefore not subject to the general authorization rule under the EECC (e.g., OTT providers, satellite providers). Furthermore, there is a specific feature of the ECS sector, regardless of the location of the headquarters, each entity must be categorized in each country in which it provides services. Taking into account all obligations after categorization (especially external audit or self-assessment, supervision by the competent authority, etc.), HAKOM sees a problem in the implementation of NIS2 for these entities, and we believe that NIS2 should be amended in such a way that rules such as for cloud service providers are applied, the obligations limited to the member state where the company has its headquarters.

3. How should companies that own only passive physical infrastructure, such as optical cables without any active equipment, be treated under NIS2? Specifically:

Should such ECN providers be categorized under NIS2? If categorization is required, which revenue should be considered for classification—revenues from the passive infrastructure-related activities, or the company's total revenues, particularly in cases where the company’s primary business activity falls outside the scope of NIS2 (e.g., the construction sector)?

Thank you !
Questions?

Vesna Gašpar

vesna.gaspar@hakom.hr