Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

Network and Information Systems Security Act

Priorities in 2024

Digital Service Providers

- Cloud service providers
- Online marketplaces
- Search engines

Digital infrastructure

- Top level domain registry
- Internet exchange
- Domain name server

Energy

Oil

Refinement → Storage → Transport

Electricity and gas

Production → Storage → Transmission → Distribution

Reactive monitoring

Investigation following incidents or alerts.

Introduction to new ESPs

Continuation of introductions and initial duty of care assessments.

Thematic inspection on Asset Management

For a risk-based selection of the ESPs. A prerequisite for managing the risks to ensure continuity of the essential service is an accurate and complete picture of the assets included in the service. You can then take measures such as vulnerability management and/or patch management to reduce the risks to these assets. In other words: 'You can't manage what you don't know you have'.

Implementation of EU legislation and regulations

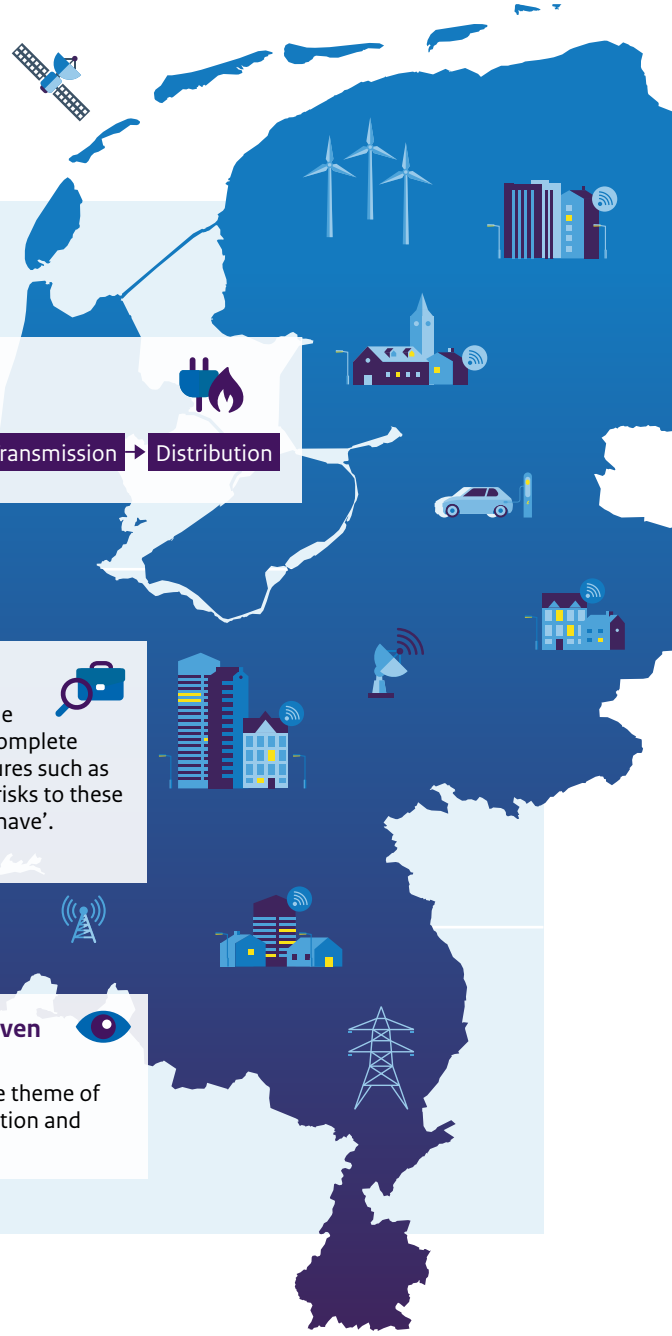
Developing and structuring supervision under NIS2, Critical Entities Resilience (CER), EU Network Code on Cybersecurity (Netcode).

Account management meetings with ESPs

NIS2 and – where relevant – Netcode are key agenda items in these meetings.

IACS Theme-driven supervision

Supervision on the theme of Industrial Automation and Control Systems.



Dutch Authority for Digital Infrastructure
Ministry of Economic Affairs and Climate Policy

Network and Information Systems Security Act – priorities for 2024

In this infographic, the Dutch Authority for Digital Infrastructure (RDI) sets out its priorities for monitoring compliance with the Network and Information Systems Security Act (Wbni) in 2024.

Wbni - What is the Act?

The Network and Information Systems Security Act (Wbni) is the Dutch implementation of the European NIS Directive into national law. The Act requires essential service providers and digital service providers to put in place appropriate and proportionate technical and organisational measures to secure their ICT resources, and to take appropriate measures to prevent incidents and mitigate to the greatest possible extent the impact of any incidents that do occur.

Wbni - Who does the Act cover?

The Minister for Climate and Energy Policy has designated electricity producers and the national and regional grid operators as essential service providers (ESPs). Essential service providers have also been designated in the oil and gas sector. The digital infrastructure sector covers internet exchanges and the administrator of the .nl domain (SIDN, the foundation in charge of registering internet domain names in the Netherlands), and, from 1 July 2023, also a number of large DNS service providers. The Dutch Authority for Digital Infrastructure actively monitors compliance with the Act among these target groups.

Digital service providers are not designated and it is up to them to determine whether or not they are subject to the provisions of the Act. The Dutch Authority for Digital Infrastructure carries out reactive monitoring of compliance with the Act among this target group, based on reports and alerts.

Wbni - How is the Act monitored?

The Dutch Authority for Digital Infrastructure monitors compliance with the Act in four ways:

- Regular inspections: we take a wide-ranging look at the overall security situation
- Thematic inspections: we examine one or more aspects of security in depth
- Incident inspections: when an incident is reported, we examine its cause and how it can be prevented in the future
- Thematic monitoring: taking specific investigations and activities as our starting point, we encourage and support the entire sector in achieving and maintaining digital resilience.

Wbni - Monitoring the Act in 2023

In 2023, the Dutch Authority for Digital Infrastructure conducted a thematic inspection of Risk Management at a number of electricity producers. This is an important subject that is indispensable for ensuring the continuity of essential services. After all, it provides insights into the vulnerabilities and threats that exist, so that risks can be managed. Research on black-start facilities also took place at a number of entities in the energy sector, continuing the Business Continuity Management theme from 2022. In addition, introductions and initial duty of care assessments were carried out among a group of more than 30 major entities in the oil and gas sector.

Key developments in 2024

Those responsible are hard at work translating the revised NIS Directive (NIS2) and the Critical Entities Resilience Directive (CER) into Dutch legislation. It is expected that the public consultation on the draft bills will take place in the first quarter of 2024. At the same time, the Dutch Authority for Digital Infrastructure will implement the changes to its supervision resulting from these draft bills. For example, we will further refine our method for the regular inspections to make it NIS2-proof. We will also involve the ESPs in this work.

The enhanced approach to critical infrastructure, the changing geopolitical situation and the expanded scope of NIS2 all underline the importance of cooperating with other regulators, both nationally and internationally.

Priorities in 2024

- Continuation of introductions and initial duty of care assessments at a number of DNS service providers.
- Thematic inspections in the area of Asset Management at a risk-based selection of the ESPs.
- Theme-driven supervision, among other things further developing the Industrial Automation and Control Systems (IACS) theme. This includes participation in the IACS coalition.
- Developing and structuring supervision under NIS2, CER and the EU Network Code on Cybersecurity (Netcode).
- Account management meetings with the ESPs. The agenda for these meetings will specifically include NIS2 and CER, and – where relevant – Netcode.
- In 2024, we will focus particularly on the external communication of the results of our supervision.
- NIS2 calls for regulators to engage in further cooperation. We will do so, for example, through more intensive cooperation as part of the Inspection Overview.