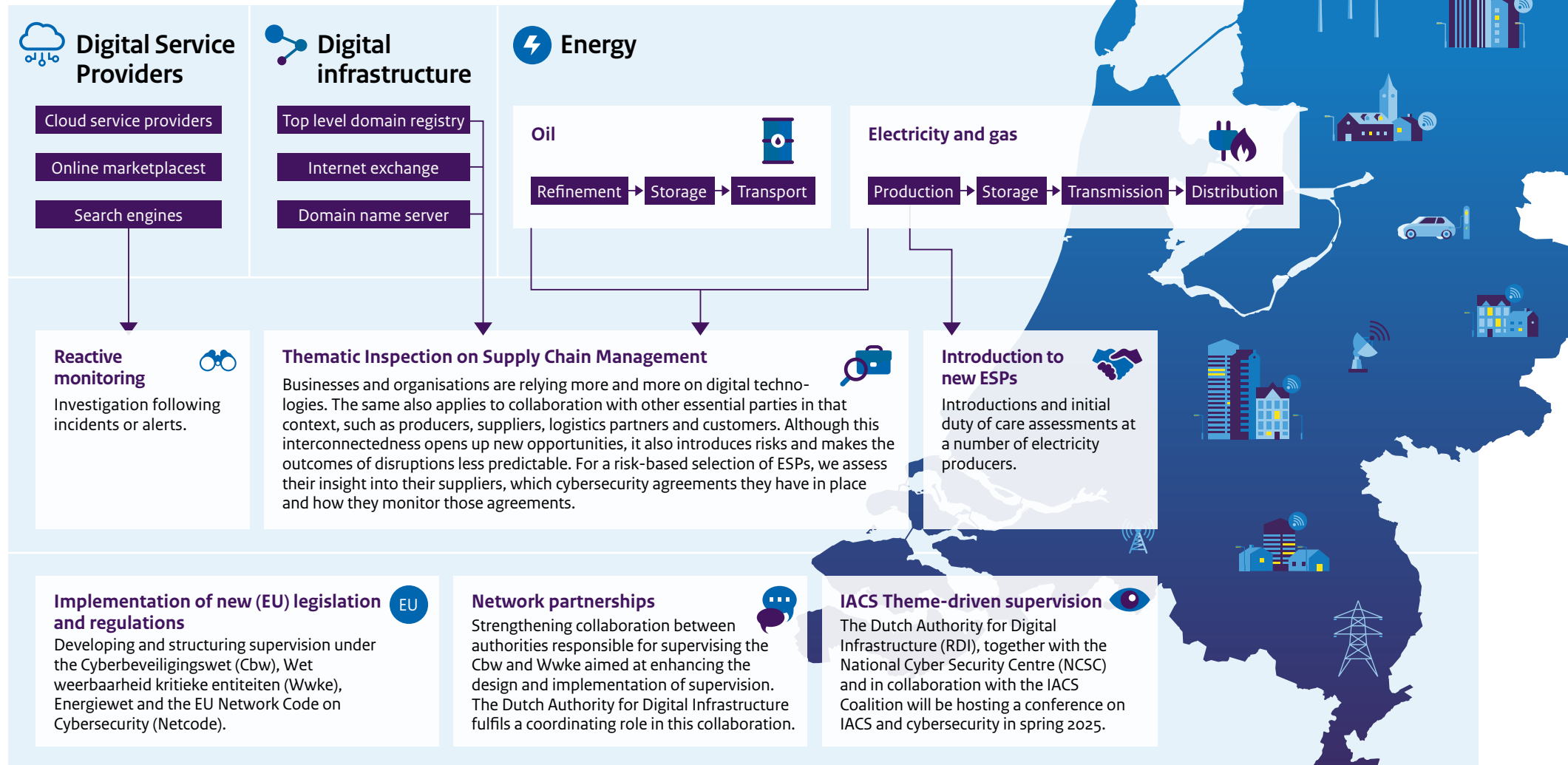




Network and Information Systems Security Act

Priorities in 2025





Network and Information Systems Security Act – Priorities for 2025

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 2025.

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) as well as 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 cybersecurity situation
- Thematic inspections: we examine one or more aspects of security in depth
- Incident inspections: when an incident is reported, we join entities in examining 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 2024

In 2024, the Dutch Authority for Digital Infrastructure conducted a thematic inspection of Asset Management at a selection of ESPs from different sectors. This is an important subject. 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'. The Dutch Authority for Digital Infrastructure will share the results of these inspections in the first quarter of 2025. In 2024, the Dutch Authority for Digital Infrastructure published the results of earlier inspections, focused on Risk Management, Black Start and Business Continuity Management, on its website.

Key developments in 2025

Work continues on the bills for the Cyberbeveiligingswet (Cbw) and Wet weerbaarheid kritieke entiteiten (Wwke). Furthermore, the Ministry of Justice and Security, together with the other relevant departments, is also developing the orders

in council for the elaboration of the Cbw and Wwke. Next, the bills and further elaboration of the Acts will be submitted to the House of Representatives for parliamentary debate. Should the Senate also give its consent, both laws are expected to be enacted in the third quarter of 2025.

The emergence of new technologies such as AI and quantum (including quantum encryption and networks) demands that we remain constantly alert to such developments and evaluate their implications for our mission. While our mission will often remain unchanged by these technological advancements, they nonetheless call for investment in knowledge and/or skills.

Priorities in 2025

- Introductions and initial duty of care assessments at a number of new ESPs in the electricity sector.
- Thematic inspections in the area of supply chain management at a risk-based selection of the ESPs.
- Theme-driven supervision, among other things hosting a conference on IACS and cybersecurity together with the National Cyber Security Centre (NCSC) and in collaboration with the IACS Coalition.
- Further developing and structuring supervision under the Cyberbeveiligingswet (Cbw), Wet weerbaarheid kritieke entiteiten (Wwke), Energiewet and the EU Network Code on Cybersecurity (Netcode). The Dutch Authority for Digital Infrastructure prefers to work with the various sectors toward these goals, and may reach out to market players and industry associations for this in 2025.
- Account management meetings with the ESPs.
- In 2025 also, we will focus particularly on the external communication of the results of our supervision.
- The Cbw and the Wwke demand increased collaboration among supervisory authorities. The Dutch Authority for Digital Infrastructure (RDI) fulfils a coordinating role in this.