N Network

I Information

S Security

Information brochure on the **Cybersecurity Law**

October 2026

Introduction

Much of our daily lives and work take place in the digital world. With the digital security of our society and economy increasingly under pressure, the European Union (EU) has adopted the NIS2 Directive. The aim of this directive, which succeeds NIS1, is to achieve a high common level of cybersecurity within the EU. The Netherlands implements NIS2 by way of the Cybersecurity Law (*Cyberbeveiligingswet*). Upon its entry into force, the Cybersecurity Law replaced the previous Network and Information Systems (Security) Law (*Wet beveiliging netwerk- en informatiesystemen*). At the same time, the Critical Entities Resilience Directive (CER Directive) is implemented through the Critical Entities Resilience Act (*Wet weerbaarheid kritieke entiteiten*). Both acts entered into force on 15 August 2026.

The Cybersecurity Law has consequences for organisations that fall within its scope. It applies to far more organisations than were previously covered by the Network and Information Systems (Security) Law. Organisations falling under the Cybersecurity Law are subject to a number of requirements, including registration, cybersecurity risk-management measures and reporting obligations. They also have a governance responsibility. The act additionally contains provisions for supervising compliance with these obligations.

What are the key elements of the Cybersecurity Law?



Table of contents

Introduction 2

1. Does the Cybersecurity Law apply to your organisation? 4

2. What does the Cybersecurity Law mean for your organisation? 11

3. What can organisations expect from central government? 16

4. Additional information 19

Disclaimer

This information brochure contains basic information about the Cybersecurity Law. No rights can be derived from the information contained in this brochure. This brochure is not legally binding. Organisations are individually responsible for complying with the requirements laid down in the Cybersecurity Law. This information brochure was last updated in August 2026 and will be updated again if necessary.



1.

Does the Cybersecurity Law apply to your organisation?

Does the Cybersecurity Law apply to your organisation?

Many organisations fall under the Cybersecurity Law by law. Organisations are individually responsible for determining whether this applies to them.

Self-assessment tool

Organisations can use the self-assessment tool to verify whether they fall under the Cybersecurity Law and, if so, whether they qualify as an essential entity or an important entity. In addition, the following steps can be taken to determine whether an organisation is subject to the Cybersecurity Law.

Step 1: Check whether your organisation is in one of the sectors listed below

The Cybersecurity Law applies to the sectors listed below. Schedules 1 and 2 to the Cybersecurity Law provide a detailed overview of these sectors and the types of entities they include.

Organisations providing domain name registration services are not listed in schedule 1 or 2 to the Cybersecurity Law. Not all obligations in the Cybersecurity Law apply to t hese organisations.



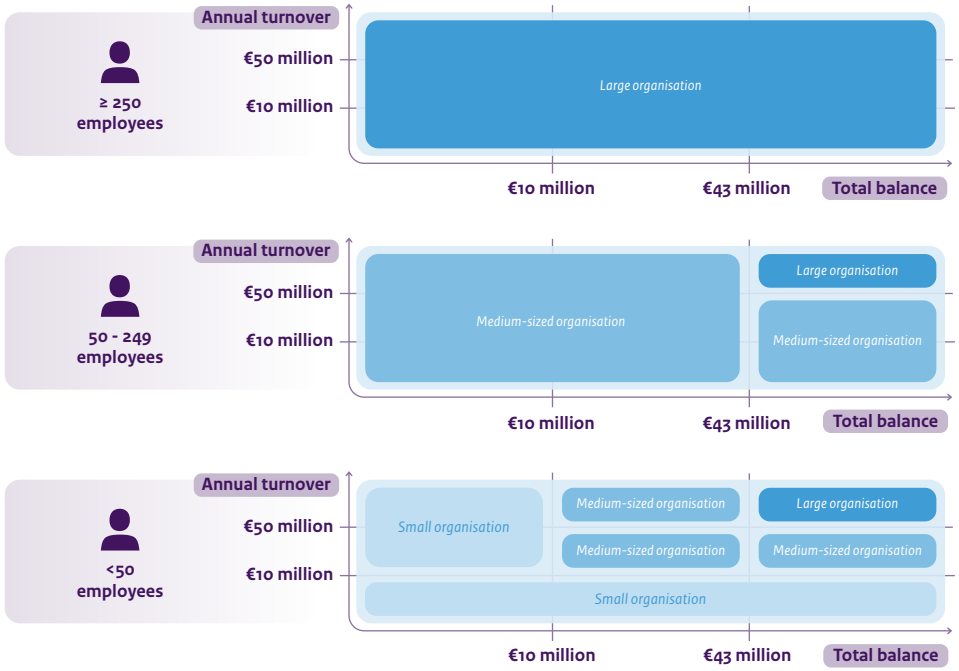
Step 2: Check whether your organisation meets the size criteria

Once it has been established that your organisation is a type of entity listed in Annex 1 or Annex 2 to the Cybersecurity Law, the next step is to establish whether the size criteria are met. This is determined by, among other things, the number of employees, annual turnover and total assets.

For some organisations these size criteria do not apply: they fall within the scope of the Cybersecurity Law regardless of their size. This is the case with: providers of public electronic communications networks, providers of public electronic communications services, qualified trust service providers, top-level domain name registries, domain name system (DNS) service providers and public administration entities, and providers of domain name registration services.

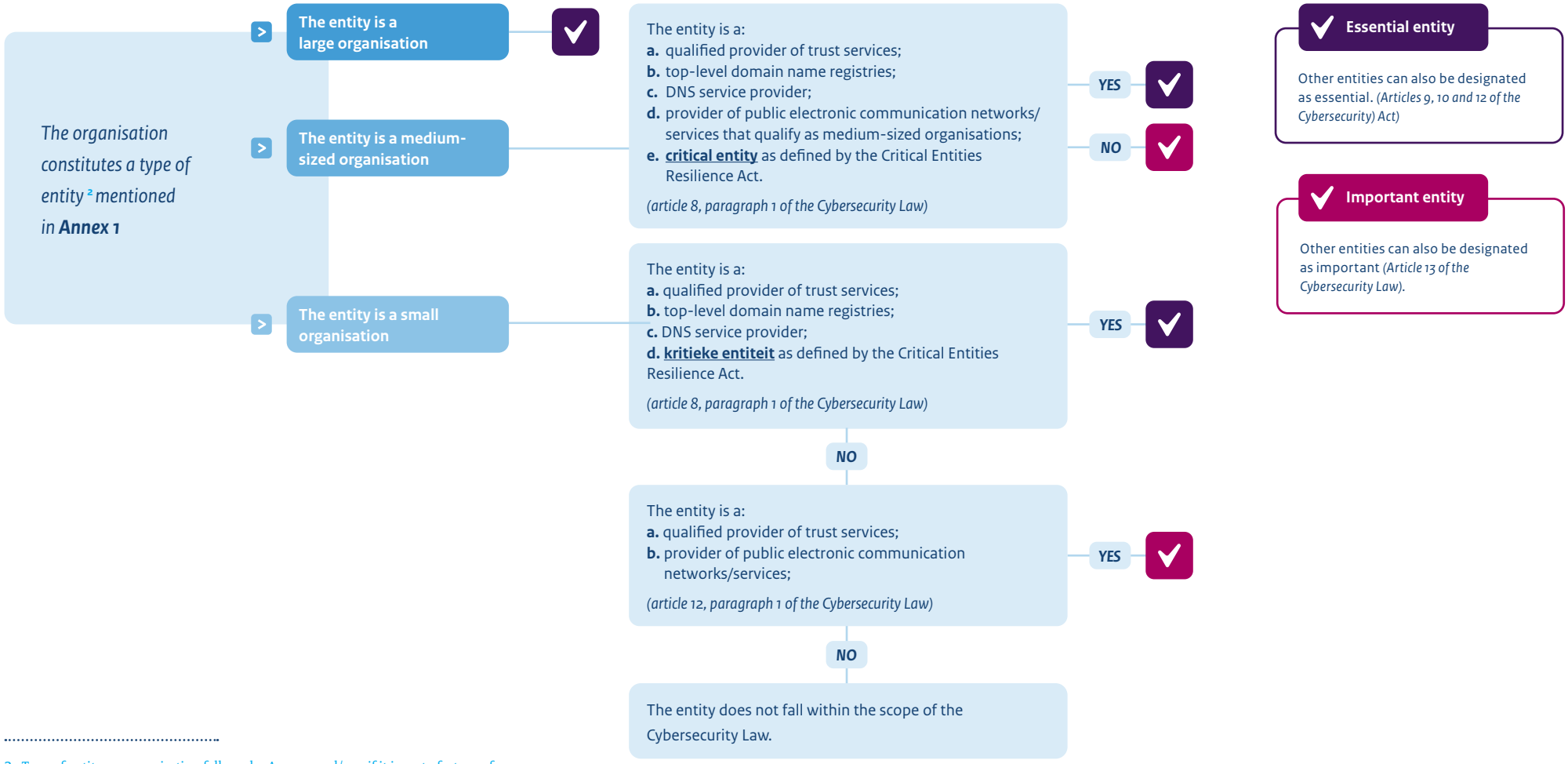
Step 3: Using the flow chart, determine whether your organisation is an essential entity or an important entity

Once you have a clear sense of whether your organisation falls under Annex 1 or Annex 2 to the Cybersecurity Law and you know its size, the flow charts can be used to determine whether it is an essential entity or an important entity. This distinction is important because it determines how the entity is supervised..



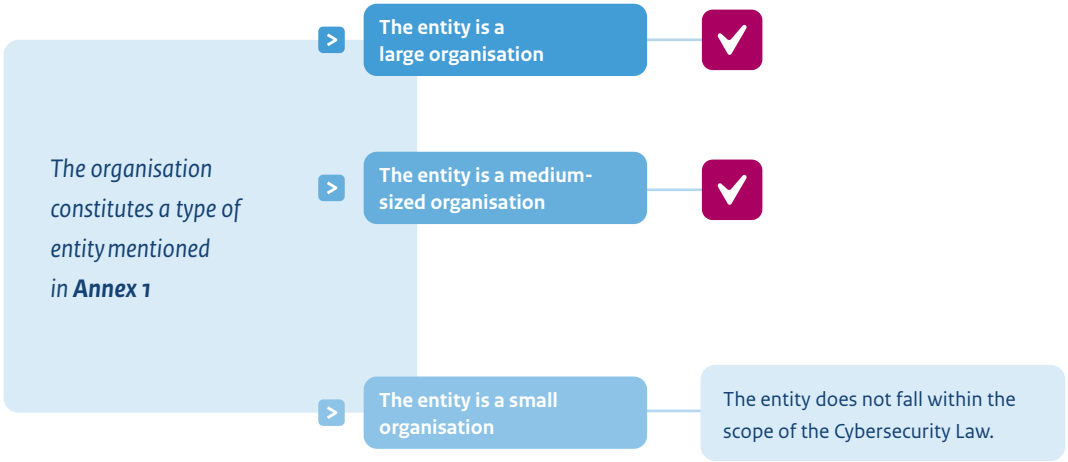
- **Essential entities:** Essential entities are subject to proactive supervision: compliance with obligations is actively monitored, even if there are no indications of a possible infringement.
- **Important entities :** important entities are subject to reactive supervision: checks are post hoc, for example on the basis of indications or information about a possible infringement. As shown in the flowchart on the following page, there are also certain exceptions in this regard.

Flowchart: entity falls under Annex 1 to the Cybersecurity Law



2 Type of entity: an organisation falls under Annex 1 and/or 2 if it is part of a type of entity within a sector or subsector listed in the schedules. For example, if the organisation is active within the energy sector, in the electricity subsector, and qualifies as an electricity company, it falls under Annex 1.

Flowchart: entity falls under Annex 1 to the Cybersecurity Law



Important entity

Other entities can also be designated as important *(Article 13 of the Cybersecurity Law)*.

Please note

For some types of organisations, exceptions apply to the main rules. This is the case, for example, for public authorities, publicly funded universities, including universities of applied sciences (*hogescholen*), providers of electronic communications networks and certain digital service providers. These exceptions are explained in more detail below.

Essential entities

Large organisations that belong to one of the sectors listed in Annex 1 to the Cybersecurity Law qualify as essential entities. The following organisations constitute essential entities under the Cybersecurity Law, regardless of their size: central and decentralised public authorities (see below for further details), qualified trust service providers, providers of top-level domain name registries and DNS service providers. Medium-sized providers of public electronic communications networks or services are also essential entities.

Important entities

Medium-sized organisations that belong to one of the sectors listed in Annex 1 to the Cybersecurity Law (and do not qualify as essential entities on the basis of the above) qualify as important entities. Medium-sized and large organisations that belong to one of the sectors listed in Annex 2 to the Cybersecurity Law qualify as important entities as well. Small or micro organisations that provide trust services or public electronic communications networks or services also qualify as important entities.

Public authorities

Within the public sector, various organisationsconstitute as essential entities under the Cybersecurity Law. These include ministries (including all underlying departments

Relationship to the Critical Entities Resilience Act

Organisations that are designated by the line minister as critical entities under the Critical Entities Resilience Act automatically qualify as essential entities under the Cybersecurity Law. These organisations are therefore also subject to the obligations set out in the Cybersecurity Law, such as the cybersecurity risk-management measures, registration and reporting obligations.

and agencies), independent management bodies that qualify as public authorities, provinces, municipalities, water authorities and organisations established on the basis of the Joint Arrangements Act (*Wet gemeenschappelijke regelingen*).

No size criteria apply to these organisations: smaller organisations can also fall under the Cybersecurity Law. However, they must meet the definition of a public authority laid down in Article 1 of the Cybersecurity Law.

Certain public authorities fall outside the scope of the Cybersecurity Law because they carry out their activities mainly in the areas of national security, public security, defence or law enforcement. These include the Ministry of Defence, the intelligence and security services, the Public Prosecution Service, the police and the safety regions.

Education

The Minister of Education, Culture and Science has used the option in the Cybersecurity Law to designate publicly funded universities, including universities of applied sciences, as important entities.

Through the ministerial order and designation, these institutions now officially fall under the Cybersecurity Law.

Complex business models

For organisations with a complex corporate structure, such as organisations with locations in several EU countries, determining whether the Cybersecurity Law applies can be complicated. In some cases, it is not the Dutch Cybersecurity Law that applies, but rather the national legislation of another EU member state. The guide to complex business models can assist you in determining which legislation applies to the organisation.



2.

What does the Cybersecurity Law mean for your organisation?

What does the Cybersecurity Law mean for your organisation?

Organisations that fall under the Cybersecurity Law have a number of obligations:



Registration obligation

Since the entry into force of the Cybersecurity Law, organisations covered by the Act are subject to a registration obligation. Organisations must register with the National Cyber Security Centre (NCSC) at MijnNCSC (My NCSC). Among other things, this gives organisations access to the services of the relevant Computer Security Incident Response Team (CSIRT) for their sector. For more information on completing a successful registration, please consult the NCSC website.



Cybersecurity risk-management measures

The cybersecurity risk-management measures requires both essential and important entities to take appropriate and proportionate technical, operational and organisational measures to manage the risks to the security of their network and information systems. This concerns the network and information systems that they use for their activities or for providing the services for which they fall under the Cybersecurity Law. An overview of the measures organisations must take as part of their cybersecurity risk-management measures is provided below.



Reporting obligation

Essential entities and important entities must report significant incidents to their CSIRT and the supervisory authority. A central reporting portal has been set up on MijnNCSC for submitting these significant incidents. In this portal, organisations can notify both their CSIRT and their supervisory authority simultaneously. Following the report of a significant incident, assistance can be obtained from the CSIRT. An incident is considered to be significant if it causes or may cause a serious disruption of services or financial losses for the organisation, or has affected or may affect other entities by causing considerable material or non-material damage. The ministerial orders issued by the ministers responsible for the various sectors establish threshold values for each sector in order to determine when an incident is significant. Organisations are therefore advised to consult the ministerial order for their sector. See an overview of the ministerial orders for each sector.



Governance responsibility and training obligation for management bodies

The Cybersecurity Law also imposes certain obligations regarding the governance of an essential or important entity. The board must approve the measures taken by the entity in the context of the cybersecurity risk-management measures and monitor the implementation of those measures.

In addition, members of the board must attend a training to acquire the knowledge and skills needed, for example, to assess the implications of risks and risk-mitigation measures.



Supervision

An organisation's compliance with the obligations arising from the Cybersecurity Law, such as the Cybersecurity risk-management measures and the reporting obligation, is monitored by supervisory authorities. In the event of infringements, enforcement measures will primarily affect the organisation itself, but in certain cases (for example the training obligation mentioned above) they may also have implications for individual board members.

Which cybersecurity risk-management measures must an organisation take?

The Cybersecurity Law stipulates that organisations must in any case implement measures in the following areas:



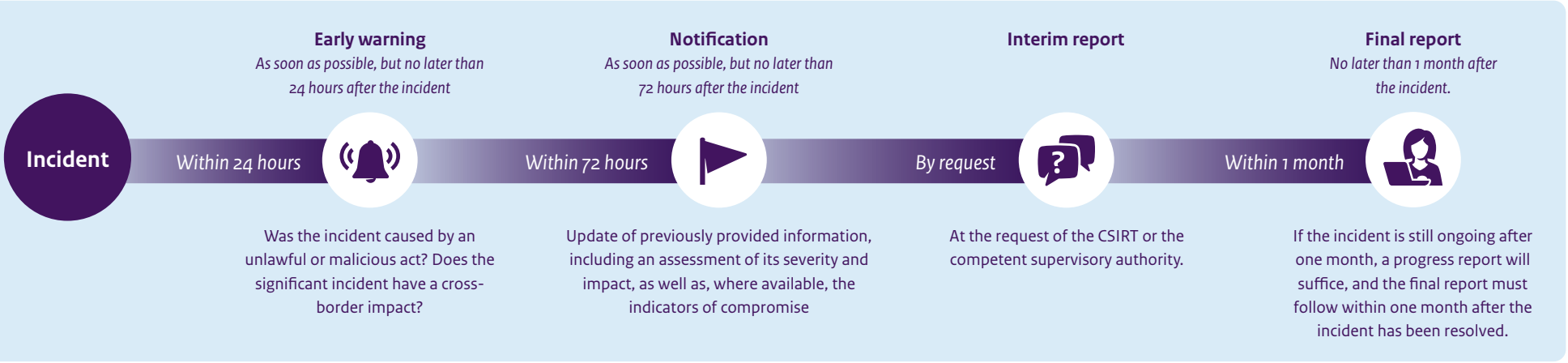
Measure 1	Policies on risk analysis and information system security;
Measure 2	Incident handling;
Measure 3	Business continuity, such as backup management and disaster recovery, and crisis management;
Measure 4	supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
Measure 5	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
Measure 6	Policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
Measure 7	Basic cyber hygiene practices and cybersecurity training;
Measure 8	Policies and procedures regarding the use of cryptography and, where appropriate, encryption;
Measure 9	Human resources security, access control policies and asset management;
Measure 10	The use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate;

These cybersecurity risk-management measures are further elaborated in subordinate legislation, the Cybersecurity Decree (Cyberbeveiligingsbesluit). In addition, sector-specific requirements have been laid down for various sectors in ministerial orders.

What does the reporting obligation entail?

Essential entities and important entities must report significant incidents to their CSIRT and supervisory authority. A central portal has been set up on MijnNCSC for this purpose. There, organisations can notify both their CSIRT and supervisory authority simultaneously.

A phased reporting obligation applies:



Significant incident

An incident is considered to be significant if it causes or may cause a serious disruption of services or financial losses for the organisation, or has affected or may affect other entities by causing considerable material or non-material damage.The ministerial orders issued by the line ministers responsible for the various sectors establish threshold values for each sector for determining whether an incident is significant. These threshold values may differ from sector to sector.

You should therefore consult the ministerial order applicable to your own sector.



3.

What can organisations expect from central government?

What can organisations expect from central government?

Organisations that fall under the Cybersecurity Law can receive support from a Computer Security Incident Response Team (CSIRT). A CSIRT's main goal is to respond quickly and effectively to cyber incidents, handle them appropriately and minimise damage. A CSIRT does this by, for example, providing assistance in the event of cyber threats and incidents, as well as warning organisations and sharing information about threats, vulnerabilities and incidents. At an organisation's request, a CSIRT can also scan the organisation's network and information systems. By registering with the NCSC, organisations can benefit from the services of the CSIRT designated for their sector.

In practice, CSIRT tasks will be handled by the NCSC for most organisations. Certain sectors or types of organisations (such as the healthcare sector and water authorities) will have a different (sectoral) CSIRT. Additionally, the NCSC serves as the central point of contact required by the Cybersecurity Law and manages the nationalregistry of entities.

The Cybersecurity Law referral tree provides an overview of the competent ministries, CSIRTs and supervisory authorities for each sector.

How to ensure that your organisation complies with the Cybersecurity Law

Get started on ensuring compliance with the Cybersecurity Law and making your organisation digitally resilient:

- Determine whether your organisation falls under the Cybersecurity Law, for example by using the NIS2 NL Self-Assessment developed by the Dutch Authority for Digital Infrastructure (RDI).
- Register your organisation through MijnNCSC. This gives organisations access to the services of their sector's CSIRT, among other benefits.
- Assess your current cybersecurity measures and identify areas for improvement. The Cybersecurity Law Control Framework, developed by the Central Government Audit Service and the Dutch Association of IT Auditors (NOREA), helps those responsible for an organisation's IT identify improvements based on the obligations in the Cybersecurity Law and to take targeted steps towards compliance. Use the RDI's NIS2 Quickscan to assess whether your organisation's current measures meet the requirements in the Cybersecurity Law and its underlying legislation.
- Implement the cybersecurity risk-management measures required by the Cybersecurity Law, the Cybersecurity Decree and the sectoral ministerial order. Conduct a thorough risk analysis to identify the required measures and determine your next steps. The NCSC offers various advisory products to support you in this.

You can read more about these steps and the available tools on the NCSC website.

How does supervision work?

The supervisory authority verifies whether organisations are complying with the obligations laid down in the Cybersecurity Law, the Cybersecurity Decree and the sectoral ministerial orders.

For essential entities, proactive supervision applies. This means that the supervisory authority can actively check whether statutory obligations are being complied with, even if there are no indications of a possible infringement.

For important entities, reactive supervision applies. The supervisory authority will, in principle, only intervene when there are grounds to do so, for example after an incident, a notification or other indications of a possible infringement.

For certain obligations, such as the mandatory training of board members, the supervisory authority monitors compliance by individual board members. Supervision also extends to compliance with the obligations for providers of domain name registration services.

The enforcement instruments available to a supervisory authority are set out below for each category.

Enforcement instruments

Essential entity
- Inspection officer
- Security scan
- Security audit
- Publication of infringement
- Binding instruction
- Order subject to enforcement action
- Order subject to a penalty payment
- Request to suspend certification or licence
- Request to suspend a board member
- Administrative fine

Important entities
- Security scan
- Security audit
- Binding instruction
- Publication of the infringemen
- Order subject to enforcement action
- Order subject to a penalty payment
- Administrative fine

Entities providing domain name registration services
- Binding instruction
- Order subject to a penalty payment
- Administrative fine

Board members of essential entities and important entities
- Order subject to a penalty payment
- Administrative fine

4.

Additional information

Additional information

The Cybersecurity Law and the Critical Entities Resilience Act have been in force since 15 August 2026. Organisations that fall under the Cybersecurity Law are individually responsible for complying with the statutory obligations laid down in this Act. Further information can be found on the websites of the NCTV, the NCSC and the ministries.

October 2026

Co-funded by
the European Union