ICTRECHT

FACTSHEET

NIS2 / Cyberbeveiligingswet

Everything you need to know about the new rules.

SCOPE

What is the Cyberbeveiligingswet (Cbw)?

The Cbw is the Dutch implementation of the European NIS2 Directive. The law aims to strengthen the digital resilience of the Netherlands by imposing requirements on the security of network- and information systems.

Objectives

Focuses on 4 pillars:

Risk management
Managing risks to network and information systems

Prevention
Preventing incidents

Damage limitation
Limiting the consequences of incidents

Information sharing
Obtaining and providing information about incidents, threats and vulnerabilities

Sectors:

The Cbw applies to organisaties in the following sectors:

Highly critical sectors (Annex I)

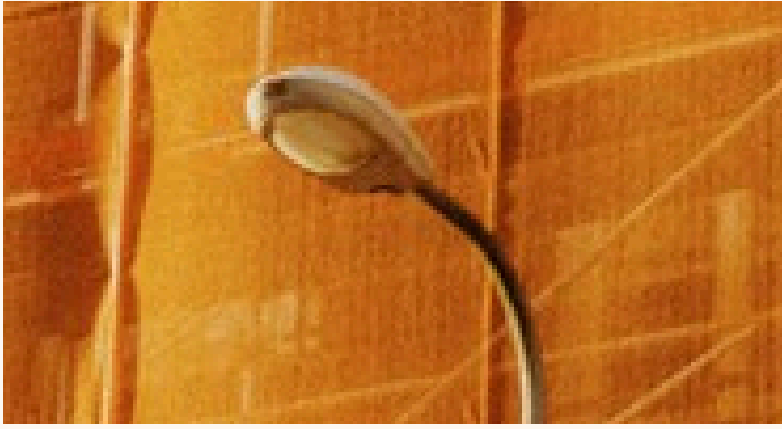
- Energy
- Transport
- Banking
- Infrastructure for the financial market
- Healthcare
- Drinking water
- Wastewater
- Digital infrastructure
- ICT-service management (business-to-business)
- Government
- Space
- Higher Education*

Other critical sectors (Annex II)

- Postal- and Courier Services
- Waste Management
- Manufacturing, production and distribution of chemicals
- Production, processen and distribution of food
- Manufacturing
- Digital providers
- Research

*Higher Education has been designated by the Minister of Education as a sector required to comply with the Cbw.

Who does it apply to:



The NIS2/Cbw applies to organisaties that:

1. Are active in one of the listed sectors, and;
2. Meet the size criteria:

Criterion	Medium- Sized Organisation	Large Organisation
Employees (FTE)	50-249	>250
Annual turnover	€10-50 milliion	>€50 million
Balance sheet total	€10-43 million	>€43 million

Note:
The size criteria do not apply to certain sectors, such as:

- Trust service providers
- Providers of public electronic communications networks
- TLD name registries and DNS service providers
- Government bodies
- Entities designated by the government

Excluded: The law does not apply to:

- Small organisations: <50 FTE and an annual turnover or balance sheet total <10 milion
- Entities that exclusively carry out activities in the area of:
  - National security
  - Public security
  - Defense
  - Law enforcement

Essential or important entity

The Cbw distinguishes between 2 categories of entities:

Type of entity	Characteristics
Essential entity	Large organisations in highly critical sectors
Important entity	Medium-sized organization in highly critical sectors and medium-sized/large organization in other critical sectors

Why is this distinction important?

Aspect	Essential Entity	Important Entity
Supervision	Proactive (ex ante)	Reactive (ex post)
Sanctions	Higher sanction regime	Lower sanction regime

Self-assessment

Organizations must assess for themselves whether they fall under the law and which category they belong to. This forms the basis for the registration obligation

Obligations

Registration obligation

Entities must register with the supervisory authority via MijnNCSC . They must provide at least the following information:

- Name of the entity
- Address and contact details (including email address and telephone numbers)
- Relevant sector and subsector
- Member States where the entity operates
- IP addresses and domain names

Updating: Changes must be reported within **two weeks**

Governance

The management of entities is required to:

Obligation	Explanation
Approve	Risk management measures must be approved by management
Supervise	Management supervises the implementation of the measures
Complete training	Board members must acquire sufficient knowledge and skills to identify and assess risks. Within 2 years of the law coming into force and certificate of participation
Liability	Board members can be held liable for non-compliance

Employee training:
Management must ensure that employees also receive regular cybersecurity training.

Notification obligation

When to notify? In the event of a significant incident, the entity must notify the CSIRT and the supervisory authority (via mijn.ncsc.nl)

What is a significant incident? An incident is significant if it:

- Causes (or may cause) serious operational disruption of services or financial losses
- Causes (or may cause) considerable material or immaterial damage to other natural or legal persons

Check the ministerial regulation for the relevant sector for the thresholds to determine when a significant incident occurs.

Please note!
If the significant incident also qualifies as a data breach, a separate notification to the Dutch Data Protection Authority (AP) is still required.
Notification deadlines

Meldtermijnen

Phase	Deadline	Content
Early warning	Within 24 hours	Initial notification: suspected cause, cross-border effect, possible intent
Incident notification	Within 72 hours	Initial assessment: severity, impact, indicators of compromise
Final report*	Within 1 month	Detailed description, cause, measures taken, cross-border impact

***For ongoing incidents:**
Instead of a final report, a progress report after 1 month, and the final report within 1 month after resolution.

Duty of care

Core obligation - Entities must take **appropriate and proportionate technical, operational and organisational measures** to manage risks.

Required measures (minimum)

Measure*

- Policy on risk analysis and information system security
- Incident handling
- Business continuity, backup management, disaster recovery plans and crisis management
- Supply chain security
- Security in the acquisition, development and maintenance of systems (incl. vulnerability management)
- Policies and procedures to assess the effectiveness of measures
- Basic cyber hygiene practices and training
- Policy on the use of cryptography and encryption
- Security aspects relating to personnel, access control, and asset management
- Where appropriate, multi-factor authentication, secure communications and emergency communication systems

*Check the sector-specific ministerial regulation to verify how you must comply with the duty of care. In some cases, you comply with the duty of care if you comply with:

- ISO 27001:2022,
- NEN7510:2024,
- BIO 2.0.

Considerations - When determining the appropriate measures, take into account:

- The state of the art
- Implementation costs
- European and international standards
- Degree of exposure to risks
- Size of the entity
- Likelihood of incidents and their severity (including societal and economic consequences)

Please note! Art. 21a Cbw:
The responsible minister may require an essential or important entity to exclude products/services from a specific supplier from designated systems, where this is necessary for national security. A reasonable replacement period applies to products already in use. Does not apply to providers of public electronic communications networks/services.

Sanctions and timeline

Sanction regime

The supervisory authority may impose various sanctions for non-compliance:

Sanction	Explanation
Warning	For less serious infringements
Binding instructions	Mandatory instructions to achieve compliance
Periodic penalty payment	Penalty payment until compliance is achieved
Administrative fine	Financial sanction

Maximum fines

Type of entity	Maximum fine
Essential entity	€10 million or 2% of worldwide annual turnover (whichever is higher)
Important entity	€7 million or 1.4% of worldwide annual turnover (whichever is higher)

Personal liability

Board members can be held personally liable for non-compliance with the obligations under the law.

Additional measures for essential entities

In cases of serious non-compliance, additional measures may be imposed:

- Temporary prohibition on exercising management functions
- Temporary suspension of certificates or licences

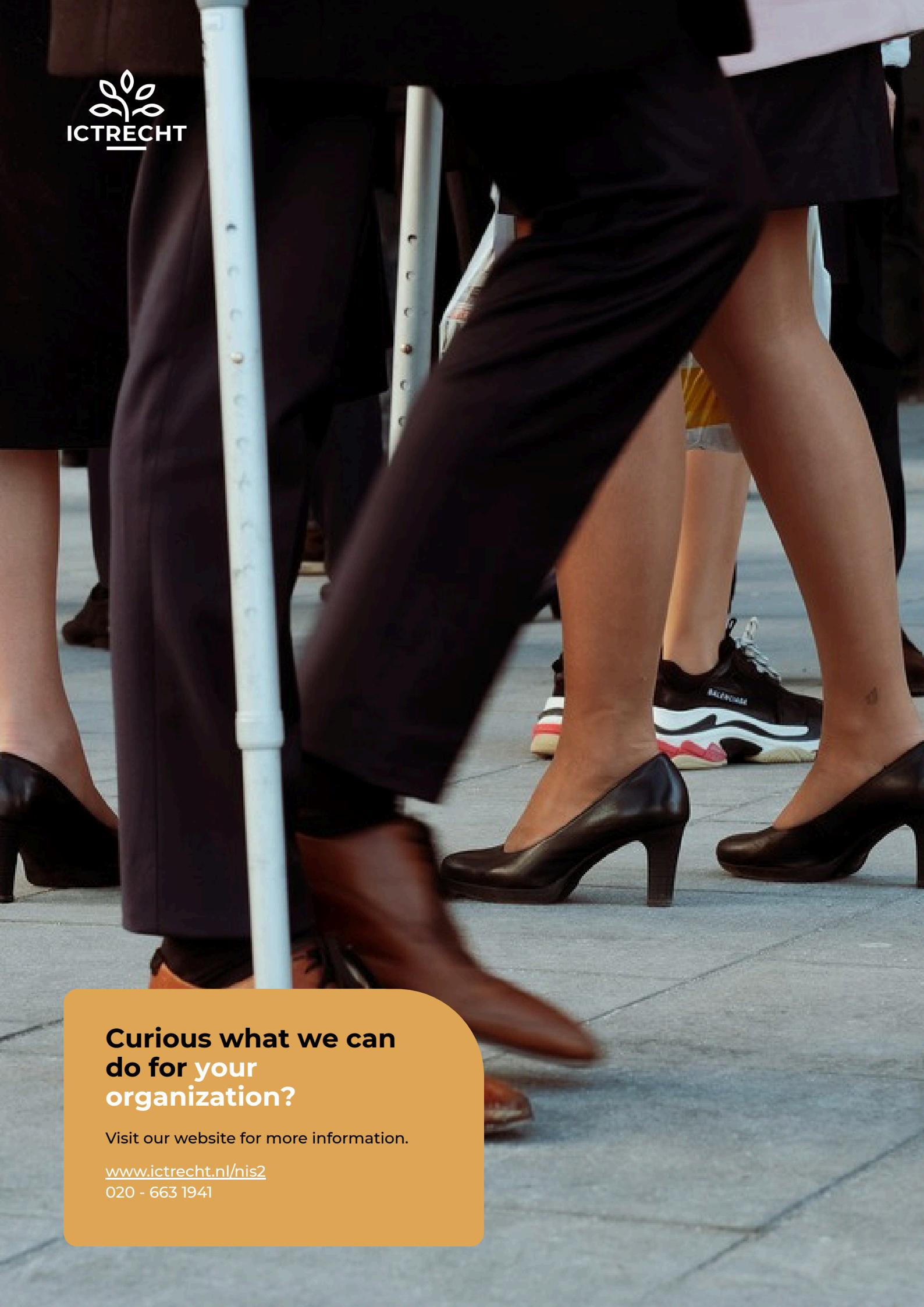
Timeline:

Date	Event
16 January 2023	NIS2 Directive entered into force
17 October 2024	NIS2 Directive must be transposed into national legislation. Dutch legislation has been delayed
June 2025	Bill submitted to the House of Representatives
15 April 2026	House of Representatives approves the Cyberbeveiligingswet
7 July 2026	Senate approves the Cyberbeveiligingswet
15 August 2026	**Cyberbeveiligingswet enters into force**

Recommended actions:

1. Determine whether your organisation falls under the Cbw and which classification your organisation receives
2. Conduct a GAP analysis
3. Draw up an implementation plan
4. Start training management and employees
5. Prepare registration and notification procedures

These are actions ICTRecht can assist with.



ICTRECHT

Curious what we can do for your organization?

Visit our website for more information.

www.ictrecht.nl/nis2
020 - 663 1941