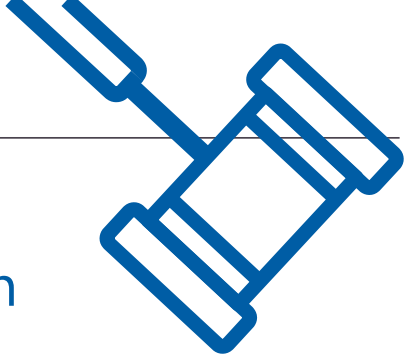


NIS2 and CRA: delaying is no longer an option

New EU rules compel organisations to take action

Both the NIS2 and the Cyber Resilience Act will come into force in the near future. Complying with these European cybersecurity and cyber resilience regulations may require considerable efforts from the organisations that have to comply with them, Louise de Gier notes.

THE NIS2, THE NETWORK AND INFORMATION SECURITY DIRECTIVE, WILL FINALLY BE IMPLEMENTED into the Dutch Cyber Security Act (Cyberbeveiligingswet "Cbw") in 2026. This should already have happened in October 2024. The Cbw is expected to come into force in the second quarter of 2026. Companies can no longer afford to put off taking action. The Cyber Resilience Act ("CRA") came into force in December 2024, with a three-year phased coming into force to give companies time to comply with it. The CRA, which covers the cyber resilience of products with digital elements, will come into force at the end of 2027. However, from 11 September 2026, companies will already be required to comply with the reporting requirements.

> There is no prescribed method for risk analysis under the CRA

So, in this respect too, companies will need to get going. There will be hefty fines for failing to comply with this reporting requirement.

Applicability

The NIS2 applies to organisations that provide services or that engage in activities in the EU, even if they are based outside the EU. The NIS2 applies to 18 sectors, including energy, transport, digital infrastructure, the management of ICT services, the manufacture of chemical products, manufacturers of machinery, equipment, tools, means of transport and government bodies, among others. The NIS2 applies when organisations meet certain thresholds. The minimum is a turnover or balance sheet total of €10 million or a workforce of 49 people or more. In addition, the NIS2 applies to certain organisations that are not required to meet a threshold, such as public bodies and public electronic communication networks or services. Furthermore, another distinction has been made between an important and an essential entity.

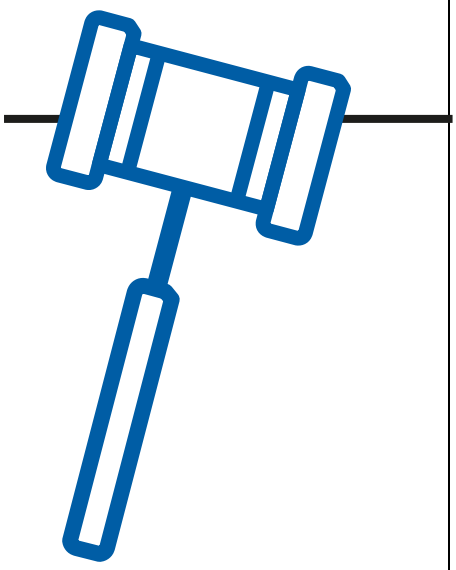
Images: Shutterstock

Essential entities (minimum annual turnover of €50 million or a balance sheet total of €43 million or more than 249 employees) are subject to proactive oversight. Supervisory authorities are allowed to enter a company's premises of their own accord or request information. The fines are higher than for important entities.

It is not easy to determine whether the NIS2 is applicable. Annexes I and II to the NIS2, listing the sectors, refer to other European regulations containing definitions of terms such as transport, energy, manufacturers of machinery or managers of ICT services.

Sometimes the definitions cannot be applied directly to an organisation's services.

In addition, for companies that are part of a group, it can sometimes be difficult to calculate the thresholds because you need to look not only at the one particular entity but also at the partner or affiliated company [(1)]. Plus, the regulations may differ from one European country to another because national Member States are allowed to make their own choices when implementing the NIS2. The same company could also qualify as both an important and an essential entity due to it operating in multiple sectors. And, if the NIS2 does not apply directly to the company, it may still (indirectly) be of great importance as companies and government bodies are responsible for the cyber security of critical direct suppliers and service providers. Regulators require the company or government body to which the NIS2 applies, to be able to demonstrate that appropriate arrangements have been made with critical suppliers and service providers.



Cyber security risks must be minimised

To whom does the CRA apply?

The CRA applies to products with digital elements marketed in the EU after 11 December 2027 or which are substantially modified after that date. This also applies to suppliers from outside the EU. This could be software or hardware with internet connectivity or network capability or consumer products connected to the internet. Services do not fall under the CRA. Separate software and hardware components do, though.

The CRA applies to products with digital elements offered commercially in the European Union. Unlike the NIS2, there are no thresholds. However, certain product categories are exempted, such as medical devices, motor vehicle products, civil aviation and marine equipment.

Again, it can be difficult to determine whether the CRA applies. An app that can be downloaded from an app store, software that is supplied with hardware such as a laptop's operating system and smart home systems do fall under the CRA. Pure SaaS, running entirely as a service on the supplier's servers, does not fall under the CRA. Other SaaS may, however, fall under the CRA. A dishwasher with embedded software for the dishwashing programme but which does not have the capability to connect to other products or networks does not fall under the CRA.

Regular products with digital elements make up the lowest category. In addition, a distinction has been made between class 1: key products with digital elements, such as software and hardware for identity management, network management systems, operating systems, virtual assistants for smart homes, security cameras, alarm systems, and class 2: key products, such as firewalls, tamper-proof microprocessors and microcontrollers. The toughest category covers critical products with digital elements, such as hardware devices with a security box and smart cards. The distinction is important for risk analysis purposes and for the conformity assessment requirements.

There are requirements for manufacturers, importers and distributors. Most of the requirements apply to manufacturers and are set out in this article. An importer or distributor which makes substantial changes to a product is considered to be a manufacturer.

Main points of the risk analysis

Both the NIS2 and the CRA require a risk analysis to be carried out.

NIS2/Cbw

The risk analysis must be carried out for each entity, based on an all-hazards approach. This means that all those involved in the security of network and information systems, the requisite equipment, access, image et cetera need to be considered. The policy must be documented and demonstrably applied. Assess what could go wrong, what the probability of that happening is, what the consequences are and what actions should be taken if an incident occurs. What is essential for the organisation?

Comments and contributions
For reactions and new contributions from IT experts:
Tanja de Vrede
020-2467230
t.d.vrede@agconnect.nl

This risk analysis should also include critical suppliers and service providers that could have an impact on the network and information systems.

An overview of the risks relating to the security of the network and information systems should be drawn up based on the risk analysis and measures should be taken if that risk analysis so requires[2].

The risk analysis to be carried out under the Cbw may be part of a larger or combined risk analysis, such as the analysis based on the CRA.

CRA

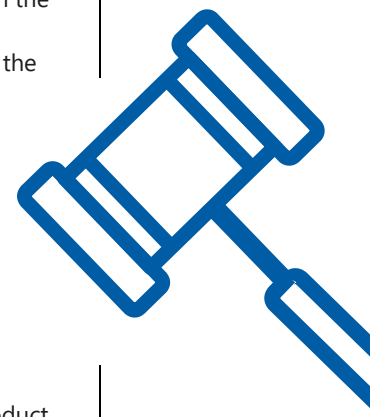
Like the NIS2, there is no prescribed method for the risk analysis under the CRA. The risk analysis covers the cyber security risks associated with a product with digital elements during the planning, design, development, production, delivery and maintenance phases.

Cybersecurity risks, including risks to the health and safety of users, should be kept to a minimum[3].

Any assessment of the management of the identified risks should be documented to ensure that the product complies with the relevant essential requirements, e.g. harmonised standards. If only part of the harmonised standard is applied or if the standard does not cover all relevant requirements, this should be documented.

The assessment of the identified risks must be included in the technical documentation. This should also be done if certain cyber security requirements do not apply[4].

The risk analysis covers the entire product with digital elements over its lifetime including data processing and support functions.



The intended purpose of use and the reasonably foreseeable use and misuse of the product should be taken as the starting point. This can be a tricky assessment, for example for the manufacturer of a component.

Main requirements

NIS2

Risk analysis for each entity

Registration requirement: all organisations that fall under the Cbw are subject to a registration requirement.

Policies relating to: business continuity, such as backup and crisis management, supply chain security, network and information systems security, such as responses to and communications about vulnerabilities, the effectiveness of cyber security measures, the board's knowledge, assessment and approval of cyber measures (the board is responsible and liable for cyber management), cyber hygiene, such as board and staff training, cryptography and encryption, security aspects relating to staff, access policies and assets, multi-factor authentication, secure voice, video and text and emergency communication systems, targeted alerts, security advisories and information about the threats.

Incident Response Policy: a plan to prevent, detect, analyse and mitigate incidents.

Duty to report: incidents that have taken place must be reported and this consists of four stages: early/timely warning (24 hours), further incident report (within 72 hours), interim report at the request of CSIRT[5] or the competent authority, final report (within one month).

CRA

Risk analysis by manufacturers

Cybersecurity requirements for products and processes: products may only be marketed if they meet certain cybersecurity requirements and the technical documentation has been drawn up[6].

Products should be designed, developed and manufactured in accordance with these requirements.

Cybersecurity risk assessment: is to be documented and included in the technical documentation as well as being updated when necessary during the support period. The security of a product is regularly tested and evaluated.

Vulnerabilities: the product need not be free of all vulnerabilities but should not contain actively exploited vulnerabilities [7]. Vulnerabilities should be addressed and remedied without delay including through security updates. The manufacturer has appropriate policies regarding the disclosure, implementation and maintenance of vulnerabilities[8].

Component: when integrating components, manufacturers ensure that cyber security is not compromised. This also applies to open source components.

Support period: the manufacturer determines a support period that is equal to the expected lifetime of a product, being a minimum of 5 years unless the lifetime is shorter.

Conformity assessment: a product's compliance can be demonstrated by a European cybersecurity certificate or can be based on procedures. The requirements for this differ for regular, important or critical products with digital elements[9]. A product's main functionality determines the category it falls into[10].

Reporting requirement: the manufacturer must report any actively exploited vulnerability and serious incident [11] to the CSIRT and to Enisa [12] within 24 hours and provide further information within 72 hours of becoming aware of it. In the case of an actively exploited vulnerability, a final report must be provided no later than 14 days after a corrective or mitigating measure is available. In the case of a serious incident, a final report must be provided within one month of submission of the report.

References

1 Article AG Connect - 2025, Louise de Gier, Hidden impact on connected businesses (Verborgen impact op verbonden ondernemingen).
2 Cyber Security Decree, Articles 7(4) and (5)
3 Articles 13.2 and 13.4 of the Cyber Resilience Act.
4 Article 13.4 of the Cyber Resilience Act and Article 4.1.1 of the Blue Guide (Blauwe Gids) 2022.
5 The government-appointed Computer Security Incident Response Team. In the Netherlands, this is the NCSC as well as other sectoral institutions.
6 Cyber Resilience Act, Parts I and II of Annex I.
7 Actively exploited vulnerability: a vulnerability for which there is reliable evidence that a malicious actor has exploited it in a system without the system owner's consent.
8 Vulnerability: a weakness, susceptibility or defect in a product with digital elements that could be exploited by a cyber threat.
9 Cyber Resilience Act, Articles 31 and 32.
10 Commission Implementing Regulation (EU) 2025/2392, recital 2.
11 The term 'serious' is defined in the Cyber Resilience Act, Article 14.5.
12 European Union Agency for Cybersecurity.

Louise de Gier
is an IT and IP lawyer
at BOLT Advocaten
In Utrecht.