LOYENS & LOEFF
Law & Tax

Further. Better. Together.

August 2026

Quoted

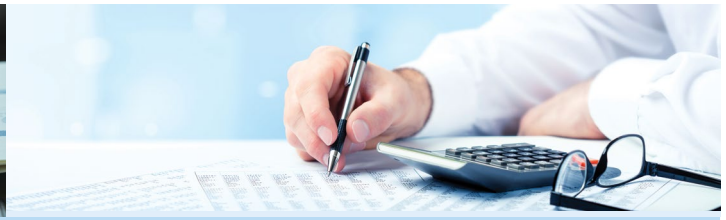
Development of digital legislation in Europe: focus on cybersecurity

Continue ›

loyensloeff.com

Edition 172





In this edition

Development of digital legislation in Europe: focus on cybersecurity

With digital transformation, cybersecurity issues have become a daily concern for businesses. This Quoted article zooms in on three key pieces of EU cybersecurity legislation – the NIS2 Directive, the Digital Operational Resilience Act and the Cyber Resilience Act – and, in each case, on how they are being implemented (or, for the directly applicable regulations, given effect) in Belgium, the Netherlands and Luxembourg, examining their impact on businesses and how they shape the EU's overall cybersecurity landscape.

1. Introduction

Digital transition is a key element in the economic development of the European Union (**EU**) and the EU's ability to maintain strategic autonomy. However, it comes with serious threats such as cyberattacks, which can undermine trust and compromise the functioning of vital sectors of society and institutions. Therefore, the topic of cyber resilience is considered as one of the greatest challenges by the EU legislator.

It was in this context that the Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems in the Union (**NIS1 Directive**) was adopted in 2016.

While the NIS1 Directive marked a step forward, it fell short of adequately addressing current and emerging challenges, such as the disparity in cybersecurity levels among Member States, the evolving nature of cyber threats, the expanding number of critical sectors, and the absence of coordinated crisis response mechanisms. In response to these gaps, the EU introduced a comprehensive cybersecurity strategy consisting of several complementary instruments. The Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (**NIS2 Directive**) provides more comprehensive cybersecurity measures for operators across critical sectors. Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act, **DORA**) specifically targets the financial sector. And the Regulation (EU) 2024/2847 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act, **CRA**) addresses the cybersecurity of connected products placed on the EU market. Together with the Critical Entities Resilience Directive (**CER**), these measures form an integrated approach to protecting the EU's digital and operational landscape. This article examines each of the three key instruments in turn, thereby also addressing the implementation, respectively direct effect, in Belgium, the Netherlands and Luxembourg.

2. NIS2 Directive

2.1 What are its objectives?

The first recital of the NIS2 Directive sets out its main objective: "*to build cybersecurity capabilities across the Union, mitigate threats to network and information systems used to provide essential services in key sectors and ensure the continuity of such services when facing incidents, thus contributing to the Union's security and to the effective functioning of its economy and society*." The measures it imposes follow an "all-hazards" approach.

In practice, this means that each entity (typically a legal person, such as a company or public body) should ask itself: what would a cyberattack on its network and information

systems mean *for society*? Answering that question upfront both clarifies whether the entity is caught by NIS2 and calibrates the depth of the measures and controls it needs to put in place. The more severe the potential consequences, the more robust the response required; the more limited the impact, the more the efforts can be moderated.

It is important to understand that a directive requires Member States to incorporate its provisions into their national laws. However, the deadline for implementation of the NIS2 Directive has now passed, and there are significant differences in how Member States have approached this. For instance, Belgium has transposed the NIS2 Directive through the law of 26 April 2024 establishing a framework for the cybersecurity of network and information systems of general interest for public security, the Netherlands has adopted the *Cyberbeveiligingswet* (Cybersecurity Act) on 8 July 2026, and Luxembourg has adopted the law of 5 May 2026 on measures for a high level of cybersecurity.

For organisations with entities spread across different EU countries, compliance becomes more complex because national implementations vary. Each entity must comply with the local law that applies to it, and the group as a whole must maintain a coordinated approach aligned with the NIS2 Directive's broader objectives.

2.2 What is its scope of application?

The new regime significantly expands the regulatory scope in comparison with NIS1 Directive, increasing the number of sectors from 6 to 18. Under NIS2, the entities are listed in two annexes: Annex I, which lists *sectors of high criticality*, and Annex II, which identifies *other critical sectors*.

Highly critical sectors (Annex I)	Other critical sectors (Annex II)
• Energy (electricity, district heating and cooling, oil, gas, hydrogen) • Transport (air, rail, water, road) • Banking sector • Financial market infrastructures • Public health • Drinking water • Waste water • Digital infrastructure • ICT service management • Public administration • Space	• Postal and courier services • Waste management • Manufacture, production and distribution of chemicals • Food production, processing, and distribution • Manufacturing (medical devices and in vitro diagnostic medical devices; computer, electronic and optical products; electrical equipment; machinery and equipment n.e.c.; motor vehicles, trailers, and semi-trailers; other transport equipment) • Digital providers • Research organisations

A cumulative selection criterion is based on the size of the companies: generally, medium or large enterprises as defined in article 2 of the Annex to the European Commission Recommendation 2003/361 (**SME Recommendation**) are concerned, *i.e.* companies that employ more than 50 FTEs or of which the annual turnover and/or total annual balance sheet exceeds 10 million euros. The notion of "*enterprise*" also generally includes affiliated companies and certain partner entities. For certain sectors, the size criterion does not apply; entities in these sectors (*e.g.* providers of critical infrastructure or essential services) fall within the scope of the NIS2 Directive regardless of their size.

Additionally, the NIS2 Directive provides the possibility for Member States to extend the scope of the Directive through national legislation, which means that certain sectors and entities may be in-scope in one Member State, and out-of-scope in other Member States.

Belgium. The law of 26 April 2024 uses the option to extend the scope of the Directive. Beyond entities of a type listed in Annexes I or II that meet the size criterion, Article 3 brings within scope, irrespective of size:

- public administrations dependent on the federal State and on the federated entities identified for that purpose, together with *secours zones* and the Brussels fire and emergency medical service;
- entities identified as operators of critical infrastructure under the law of 1 July 2011; and
- any entity providing domain-name registration services.

At the same time, Article 5, §4 carves out:

- the intelligence and security services, the Coordination Unit for Threat Assessment (**OCAM**), the Ministry of Defence, the police and general inspection, the judicial authorities and the FPS Justice when it manages databases for them;
- the network and information systems of Belgian diplomatic and consular missions in non-EU countries; and
- Class I nuclear establishments (subject to a narrow exception for elements of a nuclear installation used to transport electricity).

The Netherlands. The *Cyberbeveiligingswet* (**Cbw**) extends the scope of the NIS2 Directive to sub-national governments. Under Article 8(1)(h) of the Cbw, provinces, municipalities and *waterschappen* (regional water authorities), together with public bodies, joint bodies and shared-service organisations set up under the *Wet gemeenschappelijke regelingen*, are essential entities to the extent that they qualify as public administration entities. The size threshold for small and medium-sized enterprises (**SMEs**) does not apply to their inclusion. Higher education institutions are not designated by operation of law: under Articles 11 and 13, the Minister of Education, Culture and Science may bring an institution within scope as either an essential or an important entity by ministerial regulation or decision.

Luxembourg. The law of 5 May 2026 transposing the NIS2 Directive extends the scope of the Directive. In addition to the entities listed in the Annexes, the law also applies to administrations and entities involved in activities related to national security, public security and defence.

The NIS2 Directive also categorises all in-scope entities into two categories: essential entities and important entities. This classification drives the supervisory and monitoring powers that competent authorities may exercise and the sanctions that may follow a breach. Importantly, essential entities may be subject to proactive enforcement measures (such as regular on-site inspections, targeted security audits and routine information requests), whereas important entities may only be subject to reactive enforcement measures (such as ex post inspections and information requests triggered by evidence of non-compliance).

	Medium-sized enterprise	Large enterprise
Annex I services	Important	Essential
Annex II services	Important	Important

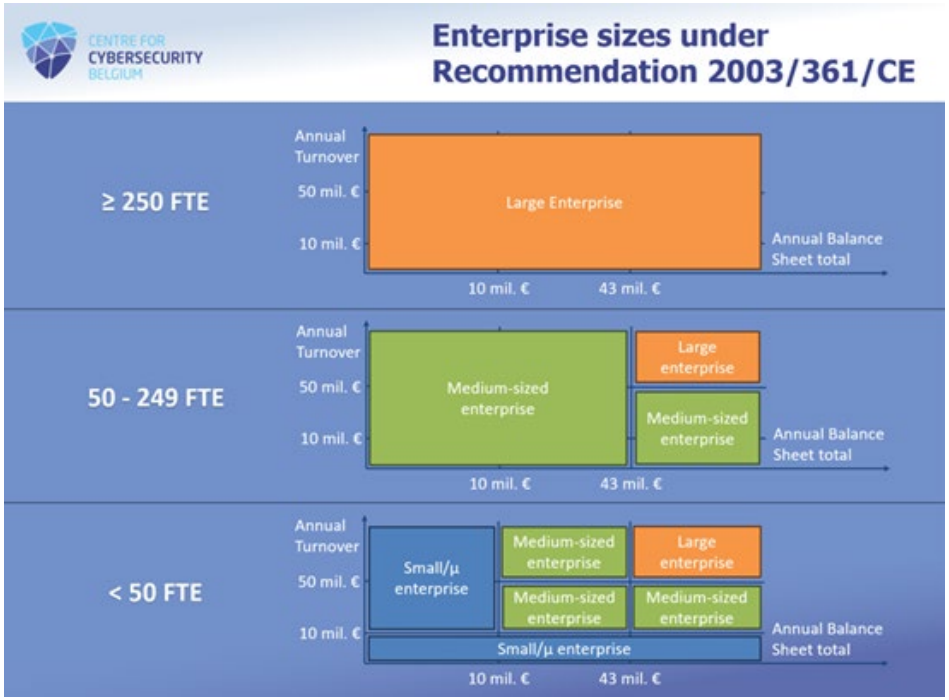
Two further points on scope are worth flagging. First, unless the definition of the activity listed in the Annexes takes account of whether the activity is primary or secondary, an entity falls within scope even if the relevant activity is *only* a secondary or ancillary part of what it does. Second, the size criterion is assessed at the level of the whole entity, not just the part of the business that brought it within scope. To avoid disproportionate results for entities that sit within a larger group, the Directive allows Member States to take the entity's degree of independence from its partners and affiliates into account when applying the SME Recommendation's calculation methods, but this option is at the Member State's discretion and must be reflected in national law to have effect.

In addition, recital 16 of the NIS2 Directive allows Member States to treat an entity as independent where the network and information systems it uses are completely separate from those of other entities within the same "enter prise". In other words, even where an entity is wholly owned by a parent company, if its networks and information systems stand on their own, the size criterion can be assessed against the entity's own figures alone, provided national law allows this.

Belgium. The law of 26 April 2024 expressly transposes recital 16 in Article 3, §2: when applying Article 6(2) of the Annex to the SME Recommendation, the national cybersecurity authority takes account of the degree of independence enjoyed by an entity vis-à-vis its partner enterprises and linked enterprises, in particular as regards the network and information systems it uses to provide its services and the services it provides. On that basis, the entity is treated as neither constituting a medium-sized enterprise nor exceeding the corresponding thresholds if, once that degree of independence is taken into account, it would not have been so treated had only its own data been used. The King may set the criteria on which the degree of independence is assessed.

The Netherlands. The *Cyberbeveiligingswet* does not contain an express independence-of-systems adjustment along the lines of the Belgian Article 3, §2. Articles 8 and 12 apply the size test by reference to Article 2 of the Annex to Recommendation 2003/361/EC, but expressly disapply Article 3(4) of that Annex (the public-body exception), leaving the linked and partner enterprise rules in place. The government has published a guidance document (*Handreiking voor organisaties met complexe bedrijfsmodellen*) that gives practical support to organisations with complex business structures on whether they fall under the *Cyberbeveiligingswet* and which national implementation law applies in cross-border situations.

Luxembourg. The law of 5 May 2026 does not appear to contain an equivalent express provision transposing recital 16: the scope threshold in Article 11 is set by reference to Article 2, paragraph 1 of the Annex to Recommendation 2003/361/EC without any independence-of-systems adjustment, and to our knowledge no dedicated published guidance has been issued on the treatment of entities within a group whose network and information systems are operated independently. Assessments accordingly need to be conducted on a case-by-case basis under the general SME Recommendation methodology.



2.3 What are the main obligations?

Under the NIS2 Directive, three main obligations are imposed:

The first obligation is a general requirement whereby entities in scope must adopt "appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services." This general requirement is supplemented by a list of minimum measures that all entities must implement. The list in the NIS2 Directive is a minimum harmonisation baseline, so Member States may add further measures in national law.

Belgium has used this flexibility in Article 30, §3, 11° of the law of 26 April 2024, which adds a coordinated vulnerability disclosure policy to the list of minimum risk-management measures for essential and important entities. The Dutch *Cyberbeveiligingswet* goes further in certain respects: Article 21a lets the responsible minister, in agreement with the Minister of Justice and Security, require an essential or important entity to stop using, in designated parts of its network and information systems, products or services from parties linked to states or entities that threaten, or are reasonably suspected of threatening, national security (a power that does not apply to public electronic communications network or service providers); and Article 24(5) requires each board member to hold a training certificate demonstrating their cybersecurity knowledge and skills. In Luxembourg, the law of 5 May 2026 largely mirrors the NIS2 catalogue of minimum risk-management measures (Article 12) and does not layer on additional substantive requirements of the type introduced by Belgium or the Netherlands.

One of the listed measures in the NIS2 catalogue is "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers". All companies subject to the NIS2 Directive will therefore need a stringent supply-chain policy with clear selection criteria, and must ensure that external providers apply robust cybersecurity measures throughout the engagement. The requirement is broadly framed and detailed guidance is still limited. While the NIS2 Directive does not specify exactly which suppliers are affected, it requires entities to consider coordinated security risk assessments of *critical* ICT supply chains (Article 22(1) NIS2). The specific suppliers in scope will depend on the European Commission's final determination of the ICT services, systems and products that are deemed "critical" under Article 22(2) NIS2. Recital 91 NIS2 sets out several criteria that help predict which supply chains are likely to be affected:

- Suppliers whose ICT services, systems, or products are heavily used by essential and important entities will likely be affected. This could include providers of cloud services, cybersecurity solutions, and core infrastructure technology.
- Suppliers whose products are crucial for the performance of critical functions, or the processing of sensitive data are more likely to be considered within the scope of NIS2 Directive. This includes providers whose systems support vital sectors such as energy, healthcare, financial services, and government operations.
- Supply chains where alternatives are scarce may also be classified as critical. Suppliers offering unique or specialised ICT products that have limited substitutes are likely to be more affected.
- The overall resilience of the supply chain throughout its lifecycle will be a factor. This means suppliers will need to demonstrate that their ICT products and services are robust and can withstand disruptions, such as cyberattacks or supply shortages.
- For suppliers of new and emerging ICT services or products, the potential future significance of their offerings for entities' activities may also lead to them being classified as critical under the NIS2 Directive.
- Special consideration will be given to suppliers whose ICT services, systems, or products are subject to specific security requirements stemming from third countries, suggesting that providers of products with foreign origins or dependencies may face heightened scrutiny.

It is anticipated that the competent national and/or European authorities may issue guidelines on this matter in the coming months. In the interim, entities might consider incorporating clauses in their contracts that impose certain minimum obligations.
For in-house lawyers, the drafting, negotiating and monitoring or auditing of contracts with third parties involved in their supply chain, which impact the company's networks and information systems, is likely to become a bigger part of their job.

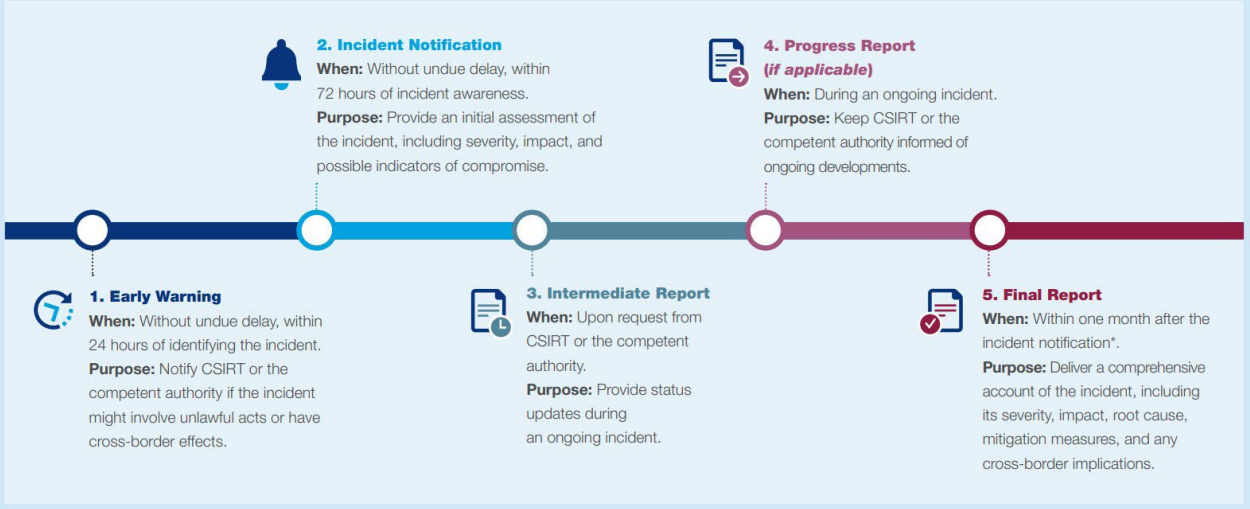
The second obligation mandates that entities in scope notify the competent national cybersecurity authority in the event of a significant incident. An incident is considered significant if it has caused, or is capable of causing, severe operational disruption of the services or financial loss for the entity concerned, or if it has affected, or is capable of affecting, other natural or legal persons by causing considerable material or non-material damage. If the significant incident could also adversely affect the provision of services in sectors vital to society, as listed in the Annexes of the NIS2 Directive, the entity should also notify the recipients of its services. Additionally, they are required to notify these recipients about the corrective measures that can be taken and, if necessary, provide details regarding the cyber threat itself.

Notification to the national cybersecurity authority must be swift and done in several stages, allowing for an appropriate and coordinated response. The notification timeline runs as follows:

- **Early warning - within 24 hours**. As soon as the entity becomes aware of the significant incident, it must issue an early warning specifying whether the incident might result from illicit or malicious activities, and whether there might be cross-border implications.
- **Incident notification - within 72 hours**. A second notification updates the previous information and provides an initial assessment of the severity and impact of the incident, as well as indicators of compromise when available.
- **Final report - within one month**. A final report must be submitted within one month after the second notification, and must include certain elements explicitly cited by law.
- **Intermediate reports - on request**. At the request of the authorities, intermediate reports may also be required.

Should an incident also trigger other notification requirements (for example, a data breach notification obligation where personal data are impacted), complying with the NIS2 Directive reporting obligation will not suffice: other notification requirements must still be complied with separately, meaning that incident response procedures should be implemented taking these different matters into account.

Key Reporting Stages:



* If an incident is ongoing, entities must submit a progress report (see step 4) and a final report within one month after resolving the incident.

The third obligation requires the management bodies of in-scope entities to ensure the entity's compliance with the legislation. The management bodies must approve and supervise the implementation of risk management measures and undergo training "in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity".

Belgium. Article 31 of the law of 26 April 2024 similarly requires management bodies of essential and important entities to approve the cybersecurity risk-management measures adopted under Article 30, to supervise their implementation, and, expressly, makes them liable for breaches of Article 30 by the entity, without prejudice to the liability rules applicable to public institutions, civil servants and elected or appointed officials. Members of management bodies must follow training so that they have sufficient knowledge and skills to identify risks and to assess cybersecurity risk-management practices and their impact on the services provided by the entity. Article 61 reinforces this by making any natural person responsible for, or acting as legal representative of, an essential or important entity personally responsible for failing in their duty to ensure the entity's compliance with the law.

The Netherlands. The *Cyberbeveiligingswet* takes this obligation further by requiring each board member of essential and important entities to obtain a training certificate demonstrating their cybersecurity knowledge and skills within two years of the law entering into force (or within two years of their appointment, if appointed later). Board members must keep this knowledge demonstrably up to date. Non-compliance with this personal obligation may result in a fine of up to € 25,000 per board member.

Luxembourg. Article 13 of the law of 5 May 2026 similarly requires the management bodies of essential and important entities to approve the cybersecurity risk-management measures adopted under Article 12, to supervise their implementation, and provides that they can be held liable for breaches of Article 12 by their entity. Members of management bodies must also follow training on a regular basis, and entities must offer equivalent training to their staff, so that they acquire sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

2.4 How is supervision handled?

Entities may be subject to periodic compliance assessments conducted by a legally approved body. These assessments are mandatory for essential entities and optional for important entities. Successfully undergoing such an assessment enables entities to be presumed compliant with the risk management obligations outlined previously. Alternatively, entities may reference other standards or methods; however, they will forfeit the presumption of conformity and must provide concrete evidence to the authority demonstrating full compliance with all required measures.

Entities may also be subject to controls by national authorities to ensure compliance with risk management measures and incident notification rules. Only essential entities are subject to both *ex-ante* and *ex-post* controls, while important entities will only be inspected *ex-post*, based on evidence, indications, or information suggesting that they are not complying with the NIS2 Directive.

Belgium. The law of 26 April 2024 designates the national cybersecurity authority (in practice the Centre for Cybersecurity Belgium, **CCB**) as the anchor for supervision, alongside any sectoral authority for a given sector. Essential entities must submit either to a regular conformity assessment carried out by an accredited conformity assessment body against a reference framework set by the King, or to an inspection by the national cybersecurity authority (Article 39). Important entities may choose to undergo the same conformity assessment on a voluntary basis (Article 41). Entities that successfully complete the conformity assessment benefit from a rebuttable presumption of compliance with the Article 30 risk-management obligations (Article 42). Beyond this, the inspection service of the national cybersecurity authority, acting on its own or jointly with, or through,

the relevant sectoral inspection service, controls compliance with the risk-management and incident notification rules, with proactive powers against essential entities and reactive (ex post) powers against important entities (Article 44).

The Netherlands. Supervision under the *Cyberbeveiligingswet* is organised on a sectoral basis. The relevant ministry for each sector is designated as the competent authority, with oversight delegated in practice to sector-specific supervisory bodies such as the *Rijksinspectie Digitale Infrastructuur* (**RDI**) for digital infrastructure, manufacturing and digital providers, *De Nederlandsche Bank* (**DNB**) for banking, and the *Autoriteit Financiële Markten* (**AFM**) for financial market infrastructure. The *Nationaal Cyber Security Centrum* (**NCSC**) acts as the primary computer security incident response team (CSIRT) for most sectors, while Z-CERT fulfils this role for the healthcare sector.

In practice, entities that fall under the *Cyberbeveiligingswet* must register in the national register maintained by the NCSC. Registration is a prerequisite for accessing the services of the sector-specific CSIRT, including incident response support, vulnerability warnings, and threat intelligence. Entities must provide their name, contact details, the sectors and subsectors in which they operate, and the Member States in which they provide their services.

Luxembourg. Under the law of 5 May 2026, the *Institut Luxembourgeois de Régulation* will undertake such role for the vast majority of sectors while the *Commission de Surveillance du Secteur Financier* will undertake such role for the banking and the financial market infrastructure sectors, as well as the digital infrastructure sector and the ICT service management sector for the activities that fall under its supervision.

2.5 What about the sanctions?

In case of non-compliance with the national implementation laws, national authorities may impose administrative measures on the relevant entities. Such entities may also be subject to fines based on their revenue in cases of breach of their NIS2 obligations. For important entities, the fine can amount to € 7 million or 1.4% of their annual revenue, while essential entities can face a fine of up to € 10 million or 2% of their annual revenue. It is important to note that Member States have the discretion to impose higher penalties.

Belgium. Article 59 of the law of 26 April 2024 aligns with the NIS2 maxima, with a € 500 floor: important entities face fines of € 500 up to € 7 million or 1.4% of the total worldwide annual turnover of the undertaking to which the entity belongs (whichever is higher), and essential entities face fines of € 500 up to € 10 million or 2% of that turnover. The Belgian law expressly provides that the administrative fine is doubled in case of repeat for the same facts within a three-year period. Beyond financial penalties, Article 58 gives the competent authority a range of enforcement tools, including:

- warnings and binding instructions;
- orders to bring risk-management or incident-notification practices into line;
- orders to inform affected recipients of a significant cyber threat;
- orders to implement audit recommendations;
- orders to publicise breaches; and
- for essential entities, the appointment of a monitoring officer (*responsable du contrôle*) with defined tasks.

Where those measures remain ineffective, Article 60 allows the authority to ask the national cybersecurity authority to temporarily suspend certifications or authorisations covering an essential entity's relevant services or activities, or to temporarily prohibit natural persons with managerial responsibilities at CEO or legal representative level from exercising those responsibilities.

The Netherlands. The *Cyberbeveiligingswet* also adheres to the maximum fines set out in the NIS2 Directive: up to € 10 million or 2% of total worldwide annual turnover for essential entities (Article 80(3)(a) Cbw), and up to € 7 million or 1.4% for important entities (Article 87(3)(a) Cbw). A residual fine of up to € 1 million applies to other breaches of the Cbw that do not fall within the NIS2-aligned maxima (Articles 80(3)(b) and 87(3)(b)).

Beyond financial penalties, the Dutch law provides for a range of enforcement tools. For essential entities, the competent authority may:

- appoint an independent monitor (*controlefunctionaris*) at the entity's expense to oversee compliance (Article 70);
- order mandatory security scans or audits (Articles 71 to 72);
- issue binding instructions (Article 74); and
- as a last resort after prior measures have failed, request the competent civil court to suspend one or more board members (Article 78) or request that the issuing bodies temporarily suspend certifications or authorisations covering the entity's services or activities (Article 77).

Important entities are subject to a comparable but more limited toolkit, focused on reactive enforcement following indications of non-compliance. Public administration entities are expressly carved out of the escalation measures in Articles 76 to 78 (Article 79), so those coercive tools do not reach ministries, provinces, municipalities and other public bodies that would otherwise be in scope.

Two Cbw-specific timing and scope details are worth flagging. First, higher education institutions designated as essential or important entities under Articles 11 or 13 benefit from a transitional period under Article 97: the substantive risk-management duty (Article 21) and the governance duty (Article 24) only start applying 36 months after their designation. This gives universities and universities of applied sciences a material lead-in time to prepare. Second, entities providing domain-name registration services that do not otherwise qualify as essential or important entities fall under a separate, lighter regime set out in Articles 88 to 91 Cbw. Under that regime, the competent authority may issue binding instructions and orders subject to periodic penalty payments, and impose administrative fines capped at € 1 million.

Luxembourg. The law of 5 May 2026 aligns with the maximum fines set out in the NIS2 Directive: up to € 10 million or 2% of the total worldwide annual turnover of the undertaking to which the essential entity belongs, and up to € 7 million or 1.4% for important entities (Article 26(4)-(5)). In addition, for specified breaches of the notification, registration and cooperation duties, the competent authority may impose:

- a warning;
- a formal reprimand (*blâme*); or
- an administrative fine of up to € 250,000 (Article 25).

Sanction decisions may be coupled with a periodic penalty payment (*astreinte*) of up to € 1,250 per day, capped at € 25,000 in total (Article 26(7)). Beyond financial penalties, where enforcement measures adopted against an essential entity remain ineffective, the competent authority may ask the President of the Luxembourg District Court to temporarily suspend certifications or authorisations covering the essential entity's relevant services or activities, or to temporarily prohibit natural persons with managerial responsibilities at CEO or legal representative level from exercising those responsibilities (Article 22(5)).

At EU level, and reflected in the national transpositions, it is also important to note that, in addition to the financial sanctions mentioned, management bodies can be held personally liable for failing to fulfil their duties listed in point 2.3. This aligns with the NIS2 Directive's intent to encourage proactivity and a thorough approach to cybersecurity within organisations. The national authorities may temporarily prohibit individuals holding leadership responsibilities within an essential entity from exercising their responsibilities, if the administrative measures required by the national authorities are not implemented within the allotted time.

2.6 What do you need to do?

To correctly implement the NIS2 Directive, organisations should follow a structured approach to ensure compliance and secure their operations. The following steps outline key actions to take:

- **Determine if your organisation falls under the scope of the directive**:
  - Assess if your organisation operates in one of the critical sectors defined by the NIS2 Directive, and determine whether it qualifies as an essential or an important entity, as this classification drives the supervisory regime and the applicable sanctions.
  - Evaluate whether your organisation supplies services to such sectors.
  - Consider compliance obligations arising from being a supplier to critical businesses, especially those imposing strict outsourcing requirements to secure the supply chain.
- **Clarify the scope and develop a compliance plan**:
  - Secure top management support.
  - Allocate necessary resources.
  - Create a clear plan with strict deadlines to avoid delays.
- **Conduct a Business Impact Assessment**:
  - Identify the most critical operations reliant on IT systems.
  - Prioritise these operations for compliance efforts.
- **Implement a risk and information security management system**:
  - Include risk management, incident handling, business continuity, supply chain security, and vulnerability management.
  - Develop and enforce policies on:
    - Encryption.
    - Multi-factor authentication.
    - Employee cybersecurity awareness training.
- **Evaluate and secure your IT supply chain**:
  - Identify and assess risks from critical suppliers, including:
    - Cyber threats.
    - Data breaches.
    - Physical disruptions.
  - Conduct vendor due diligence:
    - Review vendor security policies, certifications (e.g. ISO/IEC 27001), and audits.
    - Evaluate suppliers' incident response plans.
  - Enforce strict access controls:
    - Use multi-factor authentication and least-privilege policies.
    - Encrypt data exchanged with suppliers.
  - Perform regular audits and penetration tests on the supply chain to identify vulnerabilities.
  - Include security clauses in supplier contracts:
    - Require adherence to specific security standards.
    - Mandate incident notifications that could affect operations.
- **Build a cybersecurity-focused culture, including at management level**:
  - Train members of the management body so that they acquire sufficient knowledge and skills to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity, and provide IT staff with training to implement the necessary controls.
  - Highlight the importance of cybersecurity to management for business continuity.

3. DORA

3.1 Overview

The Digital Operational Resilience Act (**DORA**) aims to improve the digital resilience of the financial sector in the EU and to mitigate the cyber risks associated with ICT third-party service providers. DORA has a broad scope and applies to most regulated financial entities in the EU, including, *inter alia*, banks, insurance companies and intermediaries, investment firms, pension funds, crypto-asset service providers, crowdfunding service providers and fund managers.

As of 17 January 2025, in-scope financial entities must comply with the various obligations arising from DORA. The European Supervisory Authorities (**ESAs**) have published several policy products supplementing those obligations, which are described in more detail below.

One of the highly anticipated documents is the RTS "*to specify the elements which a financial entity needs to determine and assess when subcontracting ICT services supporting critical or important functions as mandated by Article 30(5) of Regulation 2022/2554*", adopted by the European Commission as Delegated Regulation (EU) 2025/532 (**RTS on Subcontracting**). Subcontracting is a crucial and complex aspect for financial entities, both in interpretation and in implementation. The RTS on Subcontracting impacts how financial entities manage their internal governance framework, as well as their existing and future contracts with ICT third-party service providers.

Financial entities must ensure ongoing compliance with DORA, including by amending existing agreements with ICT third-party service providers, updating relevant template agreements, maintaining adequate internal governance, and adapting negotiation strategies. To implement DORA, financial entities are advised to perform a gap analysis, assessing whether they comply with DORA and what needs to be done to close any gaps.

The second batch of regulatory products has since been finalised and adopted by the European Commission. Below is a high-level overview of the most relevant requirements under DORA.

The European Commission has adopted the following RTS and ITS under DORA, which supplement and further specify the obligations arising from the regulation. The **first batch**, adopted in June 2024, consists of: (i) Delegated Regulation (EU) 2024/1772, specifying the criteria for classifying ICT-related incidents and cyber threats, including materiality thresholds and reporting details for major incidents; (ii) Delegated Regulation (EU) 2024/1773, specifying the detailed content of the policy regarding contractual arrangements with ICT third-party service providers supporting critical or important functions; and (iii) Delegated Regulation (EU) 2024/1774, specifying ICT risk management tools, methods, processes and policies, as well as the simplified ICT risk management framework for smaller entities.

The **second batch**, adopted between late 2024 and mid-2025, consists of: (i) Implementing Regulation (EU) 2024/2956, laying down standard templates for the register of information on ICT third-party contractual arrangements; (ii) Delegated Regulation (EU) 2025/301, specifying the content and time limits for initial notifications, intermediate and final reports on major ICT-related incidents; (iii) Implementing Regulation (EU) 2025/302, establishing standard forms and templates for reporting major ICT-related incidents; (iv) Delegated Regulation (EU) 2025/532, the RTS on Subcontracting; and (v) Delegated Regulation (EU) 2025/1190, specifying criteria for identifying financial entities required to perform threat-led penetration testing (TLPT) and the testing methodology. The key substantive requirements arising from these regulatory products are discussed in the sections below.

3.2 Subcontracting under DORA and the RTS on Subcontracting

Article 30 of DORA broadly stipulates the key elements that should be included in the contractual arrangements with ICT third-party service providers, distinguishing between requirements applicable to all ICT services, and those applicable to ICT services supporting critical or important functions. The RTS on Subcontracting builds upon the key elements relating to ICT services supporting critical or important functions, by introducing several additional requirements relating to risk profile assessments, group-level application, due diligence and risk assessment for the use of subcontractors, the description and conditions applicable to subcontracting, monitoring of the entire subcontracting chain and changes to subcontracting arrangements between ICT third-party service providers and their subcontractors and termination.

The final version of the RTS on Subcontracting, adopted on 24 March 2025 as Delegated Regulation (EU) 2025/532, carries several important changes compared to the preceding draft version of 27 November 2023, with a notable impact on the overarching contracting requirements. Financial entities that have already begun preparations will need to carefully review these changes and adjust the existing measures accordingly. The main changes include:

3.2.1 Changes regarding the assessment of overall risk profile and complexity

Several additions have been made to the list of elements that financial entities should take into consideration when assessing their overall risk profile. For example, account must now also be taken of the type of ICT services supporting critical or important functions covered by the contractual arrangements between the financial entity and the ICT third-party service provider, as well as between the ICT third-party service provider and its subcontractors. Instead of only considering the number of ICT subcontractors, financial entities must now look at the length of the entire chain of subcontractors providing services supporting critical or important functions or material parts thereof.

3.2.2 Changes regarding the due diligence and risk assessment of subcontractor use

The RTS on Subcontracting has expanded the requirements for written agreements between financial entities and ICT third-party service providers. These agreements must now include more detailed descriptions of the services provided, as well as the eligibility criteria and conditions for subcontracting. For example, the ICT third-party service provider is responsible for the provision of the services provided by the subcontractors. Furthermore, financial entities must also be contractually notified of material changes to the subcontracting arrangement.

3.2.3 Changes in relation to the contracts between ICT third-party service providers and their subcontractors

An ICT third-party service provider is now explicitly required, under the RTS on Subcontracting, to ensure that its written contractual agreements with subcontractors address certain topics. Firstly, the RTS on Subcontracting includes the obligation to include business contingency plans put forward in article 30(3)(c) DORA and specify the service levels that the subcontractor must fulfil in line with these contingency plans in the agreement between ICT third-party service providers and their subcontractors. Any applicable ICT standards or other security measures that the subcontractor must meet are also to be specified in the written agreement. ICT third-party service providers must also ensure that their agreements with their subcontractors have the subcontractors grant the same rights of access, inspection, and audit as the ICT third-party service provider grants to the financial entities, appointed third parties or competent authorities, in line with article 30(3)(e) DORA.

Note that financial entities must contract for the possibility of obtaining information from the ICT third-party service provider in relation to the written contractual agreements between the ICT third-party service provider and its subcontractors supporting critical or important functions, as well as relevant performance indicators.

In practical terms, the RTS on Subcontracting requires financial entities to conduct a comprehensive due diligence assessment before permitting any ICT third-party service provider to subcontract critical or important functions. This assessment must verify, among other things, that the ICT third-party service provider has adequate resources, expertise and internal controls to monitor the subcontractor; that the subcontractor grants the same access, inspection and audit rights to the financial entity and competent authorities; and that the financial entity has assessed the impact of a possible failure of the subcontractor on its digital operational resilience. These assessments must be carried out periodically, taking into account changes in the business environment, risk assessments and geopolitical risks.

Importantly, any material change to subcontracting arrangements must be notified to the financial entity well in advance, with a reasonable notice period during which the financial entity may approve or object to the changes. The ICT third-party service provider may only implement the changes after the financial entity has approved or not objected within the notice period. If the financial entity considers that the proposed change exceeds its risk tolerance, it may object and request modifications. Ultimately, the financial entity has the right to terminate the contractual arrangement with the ICT third-party service provider if: (i) the provider implements material changes despite the financial entity's objection; (ii) the provider implements changes before the end of the notice period without approval; or (iii) the provider subcontracts critical or important functions not explicitly permitted under the contract.

3.3 Governance and ICT risk management

The overall objective of DORA is to strengthen the digital operational resilience of the EU financial sector. Financial entities must therefore put in place a robust internal governance and control framework that ensures the effective and prudent management of ICT risks under DORA.

As part of ICT risk management, financial entities must have policies and procedures in place to comply with DORA. Those policies should describe, among other things, ICT risk management (including business continuity and information security), ICT-related incident management, classification and reporting, digital operational resilience testing and management of ICT third-party risk.

DORA governance arrangements should include clear roles and responsibilities and consistent reporting lines. Each financial entity should appoint a function responsible for managing and overseeing ICT risk, to ensure the effective and prudent management of ICT risks. The board of directors, senior management and control functions all have ongoing training obligations under DORA: each designated individual must continuously update their knowledge and skills so that they can understand and evaluate ICT risks and their impact on the financial entity's operations.

3.4 Incident reporting

To contribute to greater digital resilience, DORA requires in-scope financial entities to detect and handle ICT-related incidents adequately. This calls for a robust management process, consistent classification and registration, and reporting to the competent authorities. DORA provides for consistent and, where applicable, expedited reporting of ICT-related incidents.

For the purposes of the reporting requirements, DORA distinguishes between 'standard' ICT-related incidents and 'major' ICT-related incidents.

ICT-related incidents qualifying as "major" are subject to strict reporting timelines to the competent authorities. These notification requirements will require financial entities to review and update their internal incident reporting processes and, where relevant, their outsourcing arrangements.

The criteria for classifying an ICT-related incident as "major" have been specified in Delegated Regulation (EU) 2024/1772. An incident qualifies as "major" where it affects critical services (*i.e.* ICT services or network and information systems supporting critical or important functions, or financial services requiring authorisation) and at least two of the following materiality thresholds are met:

- more than 10% of clients using the affected service or more than 100,000 clients in absolute terms are impacted;
- the service downtime exceeds 2 hours for ICT services supporting critical or important functions;
- the economic impact (direct and indirect costs and losses) exceeds € 100,000;
- the incident entails data losses affecting the availability, authenticity, integrity or confidentiality of data; or
- the incident has an impact in two or more Member States.

Notably, any successful, malicious and unauthorised access to network and information systems supporting critical or important functions is always classified as a major incident, regardless of whether other thresholds are met. Additionally, recurring incidents with the same root cause that individually are not major must be assessed collectively on a monthly basis and may together constitute a major incident if they occur at least twice within six months.

The specific reporting timelines have been further detailed in Delegated Regulation (EU) 2025/301. Financial entities must submit reports at the following stages:

- **Initial notification**. Within 4 hours of classifying an ICT-related incident as major, and in any event no later than 24 hours from the moment the entity became aware of the incident.
- **Intermediate report**. Within 72 hours of the initial notification, even if the status of the incident has not changed, and updated without undue delay once regular activities have been recovered.
- **Final report**. No later than one month after the intermediate report.

For credit institutions, central counterparties, trading venues, and other systemically important entities, the weekend and bank holiday extensions available to other entities do not apply to initial notifications and intermediate reports.

3.5 Information register

As from 17 January 2025, financial entities must maintain and report a comprehensive information register to the competent authorities in relation to contractual arrangements on the use of ICT services provided by ICT third-party service providers. The information register must contain, among other things, information on (i) the number of new arrangements on the use of ICT services, (ii) the categories of ICT service providers, (iii) the type of contractual arrangements and (iv) the ICT services and functions being provided. Reporting must be done at least annually.

In addition, financial entities shall inform the competent authorities in a timely manner about any planned contractual arrangement on the use of ICT services supporting critical or important functions as well as when a function has become critical or important.

The ESAs have prepared a template information register for illustrative purposes. Following the DORA application date, European national competent authorities requested copies of the completed information registers of in-scope entities.

For the first reporting exercise in 2025, in Belgium, the National Bank of Belgium (**NBB**) and the Financial Services and Markets Authority (**FSMA**) collected register information from the financial entities under their respective supervision. For the Netherlands, the AFM requested register information in February 2025. For Luxembourg, financial entities reported to the competent authorities from 1 to 15 April 2025.

National regulators were required to submit the reports to the European supervisory authorities (ESMA, EBA, EIOPA) by 30 April 2025. As the reporting obligation is annual, the exercise was repeated in 2026: in Luxembourg, the 2026 submission window ran from

11 February 2026 to 31 March 2026, and comparable annual cycles apply in Belgium and the Netherlands.

3.6 Digital operational resilience testing

DORA requires certain financial entities to undergo threat-led penetration testing (**TLPT**), a sophisticated form of security testing that simulates real-world cyberattacks against live production systems. The criteria for identifying which entities must undergo TLPT and the detailed testing methodology have been specified in Delegated Regulation (EU) 2025/1190.

TLPT is primarily targeted at systemically important financial entities, including globally and other systemically important institutions (**G-SIIs** and **O-SIIs**), significant credit institutions, central counterparties, central securities depositories, and large trading venues, insurance and reinsurance undertakings. TLPT authorities assess each entity's impact, systemic character, and ICT risk profile to determine whether testing is justified.

The TLPT methodology, aligned with the TIBER-EU framework, involves three key phases. In the *preparation phase*, the financial entity establishes a control team and selects external threat intelligence providers and testers (the "red team"). In the *testing phase*, which must last at least 12 weeks, testers simulate targeted attacks using real-world tactics, techniques and procedures (including reconnaissance, social engineering, exploitation, and lateral movement) against the entity's live systems, while the entity's security team (the "blue team") remains unaware of the test. In the *closure phase*, the entity conducts replay sessions and purple teaming exercises where the red and blue teams collaborate to maximise learning. Financial entities must use external testers at least every three tests and must submit a test summary report and remediation plan to the competent authority.

3.7 Supervision and sanctions

Unlike the NIS2 sections above, DORA's supervisory and sanctions framework is channelled through the existing national financial regulators in each Member State. The Benelux-specific implementation and enforcement rules are set out below.

Belgium. The Loi/Wet of 25 March 2025 implements DORA into the financial-sector supervisory framework. The NBB is designated as the relevant competent authority under Articles 19(1)(2) and 32(5) of Regulation 2022/2554. A new Article 37undecies of the Law of 2 August 2002 designates the FSMA as competent authority for asset managers, trading venues, data reporting service providers, FSMA-authorised AIFMs, UCITS management companies, insurance and reinsurance intermediaries, IORPs and crowdfunding service providers. The FSMA exercises the supervisory powers set out in Articles 79 to 86 of the Law of 2 August 2002, and Articles 36 and 37 of that law apply to DORA infringements, allowing administrative measures and administrative fines through the existing enforcement toolkit. For IORPs specifically, Article 23 of the 25 March 2025 law amends Article 150 of the IORP law to allow the FSMA to impose administrative fines not only on the IORP itself but also on one or more members of its board of directors for DORA breaches.

The Netherlands. DORA has been implemented through the *Implementatiewet digitale operationele weerbaarheid* and its accompanying *Uitvoeringsbesluit verordening digitale operationele weerbaarheid*. DORA supervision is allocated between DNB and the AFM along the existing division of supervisory tasks under articles 1:24 and 1:25 Wft: for entities subject to shared supervision, the licence-granting authority acts as competent authority under DORA, with a specific carve-out routing central securities depositories to DNB. Enforcement operates through the standard Wft toolkit, in particular the *last onder dwangsom* and the *bestuurlijke boete*. A dedicated table of enforceable DORA provisions has been added to the *Besluit bestuurlijke boetes financiële sector*, applying *boetecategorie 3* to breaches of DORA's core obligations, *boetecategorie 1* to breaches of reporting or notification obligations, and other categories to remaining

provisions on a case-by-case basis. Publication of the infringement and the name of the offender is available on the basis of Article 50(4)(e) of Regulation 2022/2554.

Luxembourg. The enforcement framework is set out in Article 25 of the Luxembourg Law of 1 July 2024 implementing DORA. In the event of certain breaches of DORA, the CSSF and the CAA may require the responsible legal person (as well as members of its management body or any other persons responsible for the infringement) to cease the infringing conduct and refrain from repeating it, order the temporary or permanent discontinuation of non-compliant practices, and impose significant administrative fines. These fines may reach up to EUR 5 million for individuals and, for legal entities, up to EUR 5 million or 10% of annual turnover, calculated on the basis of the entity's latest approved accounts (or consolidated group accounts where applicable). In addition, the authorities may publicly disclose the responsible person and the nature of the infringement. The CSSF and the CAA may also impose penalty payments ranging from EUR 250 to EUR 250,000 on persons who obstruct their supervisory or investigative activities, fail to comply with an enforcement order, or knowingly provide inaccurate or incomplete information.

In practice, DORA supervision is expected to intensify from 2026 onwards. Competent authorities across the Benelux - including, for example, the CSSF in Luxembourg - have indicated that they will step up supervisory activity, notably in relation to ICT third-party risk management and contractual arrangements. Financial entities should therefore anticipate closer scrutiny of the register of information, the RTS on Subcontracting due diligence assessments and the governance arrangements underpinning ICT risk management.

3.8 The Next Steps

Financial entities and ICT third-party service providers have been required to comply with DORA since 17 January 2025. In-scope entities should therefore already have carried out any required gap analysis and implemented the necessary changes to their governance, processes and ICT risk-management framework. The emphasis is now shifting from initial implementation to ongoing compliance and supervisory oversight, with competent authorities - including, in Luxembourg, the CSSF - signalling a step-up in supervisory activity from 2026 onwards, notably in relation to ICT third-party risk management and contractual arrangements. Any entities that have not yet completed their implementation efforts should do so without further delay.

For entities still finalising implementation, or as part of ongoing compliance and periodic reassessment, financial entities should perform a gap analysis to confirm whether their internal organisation, ICT software and hardware infrastructure, and ICT outsourcing arrangements remain compliant with DORA and the RTS on Subcontracting, and whether further amendments are required. In parallel, financial entities should be prepared for supervisory engagement on ICT third-party risk management, contractual arrangements and the accuracy of the information register.

4. Cyber Resilience Act

4.1 Overview

On 23 October 2024, the EU adopted the Cyber Resilience Act (**CRA**), formally Regulation (EU) 2024/2847, introducing the first horizontal EU-wide cybersecurity requirements for *products with digital elements*. While the NIS2 Directive targets operators of critical sectors and DORA targets financial entities, the CRA addresses the cybersecurity of connected products themselves, both hardware and software, placed on the EU market. The CRA fills a significant gap: until now, there has been no comprehensive EU framework mandating cybersecurity-by-design for connected products, even though such products are often the initial attack vector exploited in cyberattacks on businesses and critical infrastructure.

4.2 Scope

The CRA applies broadly to all products with digital elements made available on the EU market whose intended purpose or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network. In practice, this covers a vast range of products, from consumer devices such as smart home products, connected toys

and wearable health technology, to enterprise and industrial products such as routers, firewalls, operating systems, industrial control systems and IoT components. The CRA also covers the *remote data processing solutions* integrated into such products (e.g. cloud-based backends that are essential for the product to function).

Certain products are excluded from the CRA's scope where they are already subject to sector-specific cybersecurity regimes, including medical devices (Regulations (EU) 2017/745 and 2017/746), motor vehicles (Regulation (EU) 2019/2144), certified aviation products, and products developed exclusively for national security or defense purposes.

4.3 Key obligations for manufacturers

The CRA imposes a comprehensive set of obligations on manufacturers of products with digital elements, covering the entire product lifecycle:

Cybersecurity by design. Manufacturers must design, develop and produce their products in accordance with the essential cybersecurity requirements set out in the CRA. Products must be delivered without known exploitable vulnerabilities, with secure default configurations, and with mechanisms for automatic security updates. They must also protect the confidentiality, integrity and availability of data, including through encryption where appropriate.

Vulnerability handling. Throughout a *support period* of at least five years (or the expected product lifetime, if shorter), manufacturers must effectively identify and remediate vulnerabilities, provide free security updates, and maintain a coordinated vulnerability disclosure policy. Manufacturers must also generate and maintain a software bill of materials (SBOM) documenting the components contained in their products.

Incident and vulnerability reporting. Manufacturers must notify both the national CSIRT designated as coordinator and ENISA, via a single reporting platform, of any actively exploited vulnerability within 24 hours of becoming aware of it, with a full notification within 72 hours. They must also report any severe incident having an impact on the security of the product.

Conformity assessment and CE marking. Before placing a product on the market, manufacturers must undergo a conformity assessment procedure and affix the CE marking. The type of assessment depends on the product's risk category.

4.4 Product categorisation and conformity assessment

The CRA classifies products with digital elements into four risk tiers, with progressively stringent conformity assessment requirements:

- **Default products** (the majority) may be assessed by the manufacturer through an internal control procedure (self-assessment).
- **Important products - Class I** (*e.g.* identity management systems, password managers, VPNs, network management systems, security information and event management systems, boot managers, smart home products with security functionalities) may rely on self-assessment only if they apply harmonised standards, common specifications or a certified European cybersecurity certification scheme; otherwise, a third-party conformity assessment is required.
- **Important products - Class II** (*e.g.* firewalls, intrusion detection or prevention systems, operating systems, microprocessors with security features, smartcards) must always undergo third-party conformity assessment.
- **Critical products** (*e.g.* hardware security modules, smartcard-based secure elements) may be subjected to mandatory European cybersecurity certification by delegated act.

4.5 Timeline for application

The CRA enters into force in stages. The notification regime for conformity assessment bodies applies from 11 June 2026. The obligation for manufacturers to report actively exploited vulnerabilities and severe incidents applies from 11 September 2026. The full set of requirements, including the essential cybersecurity requirements and the obligation to affix the CE marking, applies from 11 December 2027.

4.6 Sanctions

Non-compliance with the essential cybersecurity requirements can result in administrative fines of up to € 15 million or 2.5% of total worldwide annual turnover, whichever is higher. Non-compliance with other CRA obligations may be subject to fines of up to € 10 million or 2% of turnover, whichever is higher. Providing incorrect, incomplete or misleading information to authorities can result in fines of up to € 5 million or 1% of turnover, whichever is higher.

4.7 Relevance for businesses

The CRA is relevant for a wide range of businesses beyond product manufacturers. Companies within the scope of the NIS2 Directive or DORA should take particular note, because the CRA directly complements their supply chain security obligations: by ensuring that the connected products they procure meet the CRA's essential cybersecurity requirements, in-scope entities strengthen their own compliance posture. Importers and distributors also bear obligations under the CRA to verify that products comply with the essential requirements and carry the CE marking before making them available on the market. For businesses that develop software or manufacture connected devices, timely preparation is essential given the CRA's broad scope and the approaching application deadline of 11 December 2027.

5. Interplay between NIS2, DORA and the CRA

Given that NIS2, DORA and the CRA were designed as complementary parts of the EU's cybersecurity strategy, understanding how they interact is essential for businesses that may fall under the scope of more than one instrument.

DORA as *lex specialis* to NIS2. The most direct interaction is between DORA and the NIS2 Directive. Recital 16 of DORA explicitly states that DORA constitutes *lex specialis* to the NIS2 Directive. In practice, only a limited subset of DORA-regulated entities is also caught by NIS2, namely credit institutions, trading venue operators and central counterparties (CCPs), reflecting the more limited scope of the Banking and Financial Market Infrastructures sectors under Annex I of NIS2. For those entities, financial entities subject to DORA are exempt from the NIS2 risk-management obligations (Article 21 NIS2) and incident-reporting obligations (Article 23 NIS2), because DORA's requirements in these areas are at least equivalent in effect. Most other financial entities captured by DORA are not, in principle, subject to NIS2. Financial entities that are within scope of NIS2 do, however, remain part of the broader NIS2 "ecosystem": they continue to benefit from the cooperation mechanisms between Member States, the services of CSIRTs and the information-sharing framework established under the NIS2 Directive. This *lex specialis* relationship means that, where DORA applies alongside NIS2, financial entities need only comply with one set of cybersecurity risk-management and incident-reporting rules (DORA) rather than two, avoiding double regulation.

The CRA as a complement to NIS2 and DORA. The CRA operates in a different dimension from NIS2 and DORA. While NIS2 and DORA regulate what *entities* must do (organisational measures, incident reporting, governance), the CRA regulates what *products* must be (cybersecurity by design, vulnerability handling, CE marking). Recital 125 of the CRA acknowledges that the CRA is intended to "facilitate the compliance with supply chain security obligations of entities that fall within the scope of DORA and NIS2 that use products with digital elements." In practice, NIS2 and DORA in-scope entities can rely on the CRA's conformity marking as a baseline assurance that the connected products they procure meet minimum cybersecurity standards, strengthening their own supply chain compliance posture.

Overlapping reporting obligations. A single cybersecurity incident can trigger multiple reporting obligations. Under NIS2, entities must report significant incidents to the national competent authority. Under DORA, financial entities must report major ICT-related incidents. Under the CRA, manufacturers must notify actively exploited vulnerabilities and severe incidents. Where personal data are affected, GDPR data breach notification obligations apply separately. These reporting obligations are cumulative, not mutually

exclusive (except where DORA displaces NIS2 as *lex specialis*). Organisations should therefore design their incident response procedures to address all applicable notification requirements in a coordinated way. The CRA acknowledges this complexity and encourages Member States to establish single entry points for reporting across frameworks.

Practical implications. The interaction between these three instruments means that businesses must take a holistic view of their cybersecurity compliance. A financial entity (subject to DORA) that also manufactures connected products (subject to CRA) or operates critical infrastructure (potentially also subject to NIS2 for non-financial activities) will need to navigate multiple regimes simultaneously. Understanding the boundaries, in particular which obligations are displaced by *lex specialis* rules and which apply cumulatively, is critical for avoiding both gaps in compliance and unnecessary duplication of effort.

6. Conclusion

The EU's focus on cybersecurity is reflected in its comprehensive legislative framework, consisting of the NIS2 Directive, DORA and the CRA. Together, these instruments aim to enhance the security and resilience of critical sectors and connected products in an increasingly digitalised world. By imposing stricter cybersecurity requirements on operators, financial entities and product manufacturers alike, they help businesses across the EU prepare for the growing threat of cyberattacks which will increase with the development of AI.

The NIS2 Directive significantly expands the scope of cybersecurity obligations, requiring businesses to implement robust risk management practices and adopt a more thorough approach to protecting critical infrastructure and services. Belgium, the Netherlands and Luxembourg have now each transposed the Directive, each adding their own scope extensions, additional risk-management measures and enforcement tools on top of the NIS2 minimum. Companies are urged to act proactively by identifying their critical services, implementing risk management systems, securing their IT supply chains, and fostering a culture of cybersecurity awareness, while calibrating their compliance programmes to the specific national implementation that applies to each in-scope entity. These measures not only support compliance but also help companies safeguard their operations in a landscape of evolving cyber threats.

DORA, in particular, underscores the need for operational resilience in the financial sector, recognising the critical role digital infrastructure plays in the functioning of financial entities. With its emphasis on subcontracting arrangements and ICT-related risk management, DORA equips financial institutions with the tools to manage and mitigate risks that could disrupt their services. As a directly applicable EU regulation, DORA applies uniformly to in-scope financial entities in Belgium, the Netherlands and Luxembourg, with supervision channeled through the existing national financial authorities: the NBB and FSMA in Belgium, DNB and the AFM in the Netherlands, and the CSSF and CAA in Luxembourg.

The CRA, meanwhile, addresses a critical gap by ensuring that the connected products businesses and consumers rely on are designed and maintained with cybersecurity in mind. With its phased application timeline culminating in December 2027, manufacturers, importers and distributors should begin assessing their product portfolios and preparing for the conformity assessment requirements. For NIS2 and DORA in-scope entities, the CRA's product-level requirements directly reinforce their own supply chain security obligations, creating a more cohesive end-to-end cybersecurity framework across the EU. As an EU regulation, the CRA applies uniformly in Belgium, the Netherlands and Luxembourg; each Member State will designate the national market surveillance authorities and CSIRT arrangements that give effect to it locally, and businesses operating across the three frameworks should track those national designations as they are finalised.

In conclusion, the EU's legislative approach to cybersecurity through the NIS2 Directive, DORA and the CRA is comprehensive and forward-looking, addressing both current

and emerging challenges. For businesses, diligent and thorough preparation and a deep commitment to cybersecurity are not just regulatory necessities but strategic imperatives. By embedding cybersecurity into their operational frameworks, whether as an operator of critical infrastructure, a financial entity, or a manufacturer of connected products, companies can not only comply with EU regulations but also enhance their long-term resilience in the face of growing digital threats.

How can Loyens & Loeff help you?

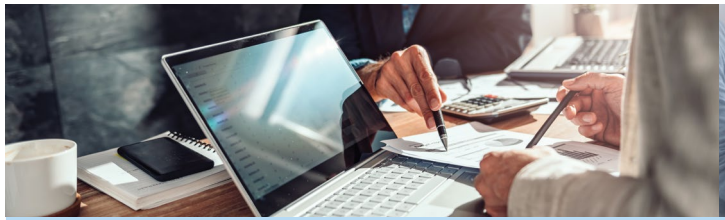
Our Tech, Data & Commercial team offers integrated support on the full EU cybersecurity stack - the NIS2 Directive and its national transpositions, DORA and its regulatory technical standards, and the Cyber Resilience Act - across Belgium, the Netherlands and Luxembourg. We help you determine which instruments apply to your organisation, how they interact (in particular where DORA displaces NIS2 as *lex specialis* and where the CRA reinforces NIS2 or DORA supply-chain obligations), and what needs to change in your governance, contracts and operations to comply.

For **NIS2**, we run scoping assessments to determine whether your entities qualify as essential or important entities under the Belgian, Dutch or Luxembourg transposition, benchmark your risk-management framework against the local catalogue of minimum measures, build supply-chain and vulnerability-disclosure policies, prepare incident-reporting playbooks aligned with the national CSIRT arrangements, and support management bodies in meeting the training requirements and reducing personal-liability risks.

For **DORA**, our firm-wide DORA team has experience establishing new regulated operations and implementing regulatory requirements. Whether you need to fully externalise the work, embed us within your project team, or use us as a subject-matter escalation point, we can run DORA gap analyses, remediate ICT third-party contracts against the RTS on Subcontracting, prepare the ICT information register and support major-incident reporting to the competent authorities. In collaboration with leading Dutch industry associations for asset managers, banks, pension funds and insurers, Loyens & Loeff has developed industry-standard addenda to help financial entities comply with both critical and non-critical subcontracting requirements: these addenda plug into existing contracts with ICT third-party service providers and give in-scope entities a straightforward route to compliance.

For the **CRA**, we support manufacturers, importers and distributors in mapping their product portfolios against the CRA's three risk tiers, in choosing the right conformity assessment route and CE-marking pathway, in setting up compliant vulnerability-handling and coordinated disclosure processes (including the 24-hour and 72-hour reporting duties to the national CSIRT and ENISA), and in preparing the required technical documentation and software bill of materials (SBOM) ahead of the December 2027 application date.

If you would like to discuss how any of these frameworks apply to your organisation, please reach out to your usual contact at Loyens & Loeff or to the Tech, Data & Commercial team.



About Loyens & Loeff

Loyens & Loeff is a leading independent, full-service law and tax firm in Europe. With offices across the Netherlands, Belgium, Luxembourg and Switzerland, and in key financial centres worldwide, we provide integrated legal and tax advice to clients operating in domestic and international markets. We combine law, tax and notarial expertise to help clients navigate complex challenges, transactions and regulatory developments across jurisdictions.
Our multidisciplinary teams work closely together to deliver pragmatic, high-quality advice that enables clients to achieve their strategic objectives. We are particularly recognised for our cross-border capabilities and our ability to support clients on the most complex matters.

Quoted is a periodical newsletter for contacts of Loyens & Loeff N.V.
Quoted has been published since October 2001.

The authors of this issue are:
Pjotr Heemskerk (pjotr.heemskerk@loyensloeff.com), Kirill Ryabtsev (kirill.ryabtsev@loyensloeff.com), Emilia Fronczak (emilia.fronczak@loyensloeff.com), Stéphanie De Smedt (stephanie.de.smedt@loyensloeff.com), Elena Mouzaki (elena.mouzaki@loyensloeff.com), Linde Vrolijk (linde.vrolijk@loyensloeff.com), and Adrien Pierre (adrien.pierre@loyensloeff.com)

You can of course also approach your own contact person within Loyens & Loeff N.V.

LOYENS & LOEFF

Law & Tax

We are Loyens & Loeff, a leading independent, full-service, law and tax firm in Europe that is uniquely on point. We provide deeply pragmatic excellence that gets you further and faster towards achieving your ambitions. We combine law and tax in teams of experts who understand better what matters most to you, and who are invested in your success. We are on point for the most complex challenges and environments, working together to get things done.

Amsterdam, Brussels, London, Luxembourg, New York, Paris, Rotterdam, Zurich

loyensloeff.com