

NIS2 and management liability for non-compliance: keys to the new cybersecurity governance framework

Summary

Directive (EU) 2022/2555 of 14 December 2022, known as NIS2, establishes a reinforced cybersecurity framework in the European Union, with broader obligations for both public and private entities that provide essential services and their management bodies.

In Spain, the Draft Bill on Cybersecurity Coordination and Governance, approved in January 2025 but not yet incorporated into Spanish law, advances the transposition of the European standard, introducing a self-assessment system (with reporting obligations and penalties for non-compliance), the role of Information Security Officer, and a graduated penalty system. In addition, it stipulates that management members may be held jointly and severally liable for the non-compliance of their respective entities, with the possibility of having to pay fines of millions of euros out of their personal assets.

The new framework involves a profound transformation in the way organisations manage digital risks, report incidents, and structure the monitoring of their cybersecurity policies from the highest organisational level.

1. A new European cybersecurity framework

The NIS2 Directive, passed on 14 December 2022, replaces the NIS1 Directive and seeks to harmonise cybersecurity levels across all Member States. Its **transposition was to be completed by 17 October 2024**, although several States, including Spain, have fallen behind schedule, prompting a reasoned opinion from the European Commission in May 2025.

NIS2 broadens the scope of the regulation by including a greater number of sectors and types of entities, covering both those considered **essential** (such as energy, transport, health, banking, space, and digital infrastructure) and those considered **important** (including manufacturing, food, postal services, waste management, and research).

2. Transposition in Spain: new developments and obligations

The **Draft Bill on Cybersecurity Coordination and Governance**, approved by the Spanish Council of Ministers on 14 January 2025, adapts the requirements of NIS2 to Spanish law and sets out a series of important new developments. However, it should be noted that the parliamentary process to convert it into law is somewhat delayed.

Firstly, it introduces a system of **self-assessment and self-registration** that requires entities to determine whether they consider themselves essential or important and to notify the competent authority within **three months**. This mechanism reinforces the joint responsibility of organisations for regulatory compliance and is accompanied by penalties ranging from **10,000 and 500,000 euros**, depending on the seriousness of the infringement.

The text also creates the role of the **Information Security Officer**, whose functions include coordinating technical and organisational protection measures, incident management, and liaising with the competent authorities. In addition, a graduated penalty system inspired by the Directive is established, with fines that, in the most serious cases, can reach **10 million euros or 2% of the annual global turnover of** the offending entity.

Informative Note

The draft bill also stipulates that executives may be held jointly and severally liable for their entity's non-compliance, with the possibility of having to pay fines of millions of euros out of their personal assets. In addition, the draft bill strengthens the institutional structure by creating a **National Cybersecurity Centre**, responsible for coordinating the response to incidents and serving as the single point of contact with the European Union.

3. Which entities does the NIS 2 regulation apply to?

In general terms, the regulation applies to all public or private entities belonging to the critical sectors defined in the Directive itself — whether they are **highly critical sectors or other critical sectors**, as detailed below — provided that these entities are at least the size of a medium-sized enterprise in accordance with Recommendation 2003/361/EC of 6 May 2003.

This means that organisations in the aforementioned sectors with **50 or more employees, or whose annual turnover or annual balance sheet total exceeds 10 million euros**.

Furthermore, the NIS2 Directive extends its scope beyond the general criterion of size (medium-sized or large enterprises) in certain cases where the nature of the service or its potential impact justifies enhanced protection. Consequently, entities belonging to high-criticality or other critical sectors will also be subject to the obligations of the regulation, regardless of their size, in any of the following cases:

- Firstly, this includes providers of public electronic communications networks or publicly available electronic services, as well as trust service providers, top-level domain name registries (TLDs) and domain name system (DNS) service providers.
- Entities that are the sole provider in a Member State of a service essential for the maintenance of critical social or economic activities, as well as those whose service interruption could have a significant impact on public safety, public order, or public health, are also considered to fall within the scope of the regulation.
- Entities whose disruption could lead to significant systemic risks, especially where such effects could have cross-border repercussions, and those that are critical due to their specific importance at national or regional level, either for their own sector or for other interdependent sectors, are also included.
- Similarly, NIS2 applies to central or regional public administration entities which, in accordance with national law, provide services whose interruption could have a significant impact on essential social or economic activities.
- The Directive also gives Member States discretion to include educational establishments — in particular those carrying out critical research activities — and local public administrations within the scope of application, where the competent authorities so determine.

Finally, entities identified as critical in accordance with Article 2.1 of Directive (EU) 2022/2557 of the European Parliament of 14 December 2022 on the Critical Entity Resilience (CER) are also covered, ensuring consistency between the two European regulatory frameworks.

3.1. Highly critical sectors

- Drinking water
- Wastewater

Informative Note

- Banking
- Energy
- Space
- ICT service management (B2B)
- Digital infrastructure
- Financial market infrastructure
- Healthcare industry (both healthcare and pharmaceuticals)
- Transport

3.2. Other critical sectors

- Manufacturing, production, and distribution of chemical substances and mixtures
- Manufacturing of certain products (sanitary, IT and electronic products, electrical equipment, machinery, motor vehicles, and transport equipment)
- Waste management
- Research
- Food production, processing, and distribution
- Digital service providers (search engines and social networks)
- Postal and courier services

4. Management and supervisory duties: direct involvement of management bodies

One of the main innovations of NIS2 lies in the **direct liability of the management body** in the approval, supervision, and review of cybersecurity measures. Directors and board members must ensure that risk management policies are adequate and that the teams responsible have the necessary resources and training. The Directive also requires that members of the management body receive **specific training in cybersecurity**, to ensure a real understanding of the threats and decisions taken in this area. It also requires them to ensure that other staff within the organisation receive cybersecurity training.

5. IT security measures, incident reporting, and supervision

The Directive requires the implementation of a minimum set of information security measures, including legal, IT, and organisational measures. However, these measures include an IT risk analysis and the adoption of appropriate measures to mitigate the impact and probability of risk, so strictly speaking, not all entities have to adopt exactly the same measures.

The Directive also imposes a **tiered notification regime** for significant security incidents. Entities must issue an early warning within 24 hours, an interim report within 72 hours and a final report within one month of detecting the incident.

6. Integration with criminal compliance and recent case law

NIS2 imposes supervisory obligations and cybersecurity measures on management bodies, and it is important to remember that **failure to comply with these obligations** may result in administrative and financial penalties and even **subsidiary civil liability arising from the offence** (STS 699/2025, of 19 February).

In this regard, recent case law from the Supreme Court has reinforced this idea by recognising the **subsidiary civil liability of companies for virtual crimes linked to their computer systems, when a deficiency in their security measures facilitates fraud or damage to third parties**. In this context, the correct implementation of the NIS2 requirements not only contributes to regulatory compliance, but can also act as an exonerating factor in matters of civil liability arising from the offence.

Informative Note

Consequently, compliance with NIS2 regulations is not only a legal obligation and a measure aimed at preventing certain computer crimes (such as damage or personal data protection), but also becomes a key element within a global corporate defence strategy framework: **the Corporate Compliance system**.

7. Next steps

As the Draft Bill progresses through Parliament, organisations should prepare in advance by, **assessing their status as an essential or important entity**, appointing a security officer, and **adapting their internal risk management and incident response policies**. Alignment between technical, legal, and compliance teams will be crucial to ensuring effective implementation and avoiding future liabilities. It is not advisable for a single department to manage compliance with this regulation; at a minimum, the legal, IT security, and regulatory compliance departments must collaborate and coordinate.

Any questions?

From our Compliance and Digital Law and Data Protection Areas, we strive to answer any questions that may arise from the current situation. If you have any questions, please do not hesitate to contact us.

Contact:

Íñigo de Ros Raventós

Corporate Crime and Compliance Partner
ideros@rcd.legal

David Molina

Digital Law and Data Protection Director
dmolina@rcd.legal

www.rcd.legal