LAW·P
STUDIO LEGALE E TRIBUTARIO

COMPLIANCE

NIS 2 COMPLIANCE IN ITALY

*APPROACHING THE **31 DECEMBER DEADLINE** AND ANALYSING STRATEGIC AND SUPERVISORY **DUTIES OF THE MANAGEMENT BODIES***

AUTORI

avv. MAURIZIO MARULLO
marullo@lawp.it

avv. CLAUDIA MARONGIU
marongiu@lawp.it

1. INTRODUCTION

In view of the **31 December 2025 deadline** for notifying the designation of the **CSIRT contact point** (the Computer Security Incident Response Team established within ACN), it should be noted that the "Aggiornamento dati" section of the ACN Services Portal now includes a dedicated area for entering the details of the designated contact person and any substitutes.

Although formal in nature, this requirement forms part of the broader regulatory framework introduced by Legislative Decree No. 138/2024 (the "**NIS2 Decree**"), which has significantly reshaped corporate obligations in the field of cybersecurity.

With Italy's implementation of Directive (EU) 2022/2555, the legislator has transformed cybersecurity from an organizational best practice into a **legal obligation** for entities falling within the scope of the NIS2 framework. The regulatory intervention pursues a dual objective: on the one hand, strengthening companies' ability to prevent and manage cyber-attacks; on the other, contributing to the development of a national **digital resilience** system, recognizing the crucial role played by private operators in safeguarding the country's overall security.

The NIS2 Decree applies directly to entities classified as **Essential** and **Important Entities**, operating in sectors deemed critical (a complete overview is available in the mapping published by the National Cybersecurity Agency). The impact of the framework, however, extends beyond these subjects: **companies that do not formally fall within the NIS2 perimeter but act as suppliers or business partners of regulated entities are also affected.** This is due to the obligation imposed on Essential and Important Entities to ensure adequate levels of security across the entire **supply chain**, requiring contractual counterparties to meet **minimum cybersecurity standards.**

In this context, the NIS2 Decree establishes a direct and significant **link** between **cybersecurity and corporate governance**. Cyber risk is now treated as a strategic business risk, which management bodies must oversee in a structured and well-documented manner. Directors therefore acquire responsibilities not only operational in nature, but also relating to strategic direction, supervision and training, as highlighted in Assonime Circular No. 23/2025 (the "**Assonime Circular**").

This highlight aims to provide an operational overview of the main obligations, responsibilities and sanctioning profiles introduced by the NIS2 Decree for management bodies, with the goal of supporting companies in correctly applying the framework and defining the most appropriate governance measures.

2. NON-DELEGABLE DUTIES OF THE MANAGEMENT BODY

The NIS2 Decree places on the administrative body **strategic duties** which, by their nature, **cannot be delegated** to lower-level technical staff. These obligations are set out in Article 23 of the NIS2 Decree and are structured around the three main areas outlined below.

a. Strategic direction and approval of cybersecurity measures

The administrative body is first and foremost required **to approve the modalities for implementing cyber risk management measures** (Article 23(1)(a) of the NIS2 Decree). This obligation must be interpreted in conjunction with Article 24 of the NIS2 Decree and with the broader notion of **an adequate organizational framework**, as clarified, *inter alia*, by the Assonime Circular.

The measures required by the NIS 2 Decree do not consist solely of technical aspects, but include a

structured set of **organizational measures**, such as plans, procedures, protocols, internal roles, control systems, and risk assessment and treatment processes, which directly affect both **corporate governance** (responsibilities, information flows, and duties of top management) and **internal governance**, specifically the internal organization responsible for implementing strategic decisions.

In this context, the **cybersecurity strategy and overarching security policies** cannot be entrusted exclusively to the Chief Information Security Officer **("CISO")** or to technical functions. They must be **reviewed and approved by the administrative body**, which is responsible for ensuring that the company is equipped with an organizational structure suitable for preventing and managing cyber risks.

As clarified by the National Cybersecurity Agency (ACN) and by the Assonime Circular, these **obligations are non-delegable,** as they relate to strategic planning and overall risk governance.

The approval of cybersecurity measures by the administrative body therefore plays a central role. On the one hand, it makes it possible **to verify** that the **measures adopted are adequate, proportionate, and up to date** in light of the state of the art and the evolving threat landscape; on the other hand, it constitutes the basis both for **the company's external liability**, including supply-chain security and the protection of service recipients, and for the **liability of directors vis-à-vis the company** in the event of inadequate organizational arrangements.

b. Oversight and supervision

The administrative body is also required to **supervise the proper implementation** of the cyber risk prevention and management measures it has

approved (Article 23(1)(b)). This duty of oversight consists in **continuous monitoring of the effectiveness of the measures adopted**, as well as in **verifying** that **incident notification processes** are timely and compliant with statutory deadlines.

As emphasized by the Assonime Circular, this obligation is consistent with the general rules and principles of Italian corporate law, in particular Article 2086 of the Italian Civil Code (obligation to establish organizational arrangements adequate for crisis management) and Article 2381 of the Italian Civil Code (directors' duty to act on an informed basis).

Cyber risk now represents one of the **main potential causes of business crisis** and requires organizations to be equipped, on a preventive basis, with an adequate framework capable of containing its impacts and protecting both the company and other affected stakeholders.

c. Mandatory cybersecurity training

In addition, Article 23(1)(c) imposes on members of the administrative body a **direct obligation to undertake specific training in the field of cybersecurity.**

This is not a merely formal requirement: the legislation requires directors to acquire the knowledge necessary to consciously assess risks, approve the measures put in place, and supervise their implementation.

ACN Determination No. 164179/2025 further strengthens this obligation, highlighting the need to **extend continuous training programs also to personnel**, in order to ensure adequate cyber hygiene and a level of awareness consistent with the evolution of cyber threats.

3. INTERNAL CONTROLS AND SUPPLY CHAIN MANAGEMENT

As anticipated, the new regulatory framework on **cyber risk management** requires an evolution that goes beyond the IT function alone and **involves the entire**

corporate structure.

This evolution unfolds along two main fronts:

a. **Integration of cyber risk into internal control systems**

   It is necessary for internal control systems to extend their scope to include cyber risk, by integrating it into:

   - the **enterprise risk assessment processes**; and
   - the **information flows addressed to the management body.**

b. **Reassessment of the supply chain**:

   The NIS2 Decree places strong emphasis on **supplier security**, requiring companies to verify that their suppliers and business partners comply with security standards adequate for the prevention and management of cyber risk.

   This entails the need to:

   - **review existing supply agreements**; and
   - include **specific cyber clauses** governing, inter alia:
     - minimum security requirements; and
     - liability regimes in the event of a cyber incident.

4. DELEGATION AND THE LIMITS OF RESPONSIBILITY

It is well established that the **administrative body may delegate implementation and technical execution functions** to an internal delegated body (such as a Chief Executive Officer or an executive committee) or to specialized roles (such as the CISO or a Cybersecurity Manager).

Such operational delegation is physiological and necessary, particularly in a context such as that defined by the NIS2 Decree, where technical and organizational requirements are particularly complex.

However, as clarified by the Assonime Circular and reiterated in the ACN FAQs, **delegation does not in any way entail a transfer of responsibility.**

Even where dedicated technical roles are in place - including those expressly required by law, such as the CSIRT contact point, whose appointment is mandatory - the ultimate responsibility for obligations relating to strategic direction, supervision, and governance of cyber risk remains entirely with the administrative body.

In particular, the ACN FAQs specify that the **designation of the CSIRT contact point** serves the purpose of **operational liaison with CSIRT Italia**, but **does not replace or mitigate the duties of the management body**, which remains required to:

i. **define and approve the strategic guidelines** for cyber risk management;

ii. **verify the effective implementation of the measures** proposed by the CISO and other technical roles;

iii. **oversee the timeliness and adequacy of significant incident notification** processes.

The possible presence of a CISO or a Cybersecurity Manager (who may also act as CSIRT contact points) therefore constitutes essential operational support but does not provide any exemption from liability.

Accordingly, the **administrative body will always remain directly liable** for any **serious organizational failures**, also in light of **the applicable sanctioning and restrictive regime** provided for under the NIS2 framework.

Such operational delegation is physiological and necessary, particularly in a context such as that defined by the NIS2 Decree, where technical and organizational requirements are particularly complex.

5. ADDITIONAL OBLIGATIONS OF MANAGEMENT BODIES

a. Documentation framework

To comply with the provisions of the NIS2 Decree, as well as with the guidelines set out in ACN Determination No. 164179/2025 and its annexes, it is essential for the entities concerned to **adopt a documentation set capable of demonstrating the**

adequacy of the implemented cyber risk prevention and management system.

From this perspective, the management body is required to review, approve and periodically update all documentation deemed necessary to prevent cyber incidents and manage their consequences, as well as to attest, where requested, the company's commitment to complying with sector-specific regulations.

It should be noted that ACN Determination No. 164179/2025 does not identify a catalogue of mandatory documents but sets **out a series of minimum mandatory measures** that must be translated into operational, organizational and technical measures. Consequently, the definition of the documentation set must be tailored on a case-by-case basis, taking into account (i) the qualification of the entity (Essential or Important Entity) and (ii) the nature of the activities performed and the associated risk level, with no check-list applicable to all organizations.

By way of example, documentation set may include:

- cyber risk management policy;
- risk assessment and treatment plan;
- vulnerability management plan;
- effectiveness assessment plans;
- business continuity and disaster recovery plans;
- incident response plan and incident notification workflow.

b. Incident notification

Pursuant to Article 25 of the NIS2 Decree, **incidents that exhibit significant characteristics must be promptly reported to the CSIRT**. An incident is considered "significant" when it has caused, or could have caused, a serious operational disruption of services or financial losses for the company, or when it has had, or could have had, repercussions on other natural or legal persons, causing **substantial material or immaterial losses**.

Such **notification** must **include all information** enabling the CSIRT **to assess any cross-border impact** of the incident and must take place within the following timeframes:

- **within 24 hours** of becoming aware of the significant incident, an **early warning** must be submitted, indicating, where possible, whether the significant incident may be the result of unlawful or malicious acts or may have a cross-border impact;
- **within 72 hours** of becoming aware of the significant incident, an **incident notification** must be submitted, updating, where possible, the information provided in the early warning and including an initial assessment of the significant incident, covering its severity and impact, as well as any available indicators of compromise.

From an operational standpoint, the **notification is carried out by the CSIRT contact point**, who collects and transmits the necessary information to the CSIRT within the prescribed deadlines.

However, it is essential to emphasize that **the ultimate responsibility for the proper fulfilment of the notification obligations lies with the management body**, pursuant to Article 23 of the NIS2 Decree. Directors must:

- ensure that the company has **internal procedures** capable of **promptly detecting and classifying incidents**;
- ensure **clear attribution of roles** for managing and communicating incidents;
- monitor that **notification processes** are **functioning, timely and compliant with the law.**

In other words, although the operational handling of the incident may be delegated to the CSIRT contact point, possibly supported by other technical functions, the **management body retains a**

non-delegable duty of supervision and oversight, and remains accountable for any inadequacy of organizational arrangements that may prevent timely compliance.

6. LIABILITY AND SANCTIONS

Non-compliance with the obligations set out in the NIS2 Decree gives rise to consequences on different levels.

a. Administrative fines for entities

Article 38 of the NIS2 Decree provides for significant administrative fines applicable to the entity:

- for Essential Entities, fines may reach up to EUR 10,000,000 or 2% of the worldwide annual turnover of the preceding financial year, whichever is higher;
- for Important Entities, fines may reach EUR 7,000,000 or 1.4% of the worldwide annual turnover of the preceding financial year, whichever is higher.

b. Personal sanctions for directors

The NIS2 Decree significantly strengthens the enforcement framework applicable to members of the management body, moving cybersecurity oversight firmly into the sphere of board-level responsibility.

In particular, Article 38(6) provides that, where serious, repeated or systematic breaches of obligations relating to cyber risk management or incident notification persist and the entity fails to comply with the corrective measures or orders issued by the competent authority, the **authority may adopt temporary restrictive measures**, including measures **affecting the ability of individuals performing management functions to continue exercising such functions**, until the identified deficiencies are remedied.

This is a particularly significant measure, highlighting

that cybersecurity is no longer a delegable task but an organizational and strategic duty, the omission of which directly exposes those governing the company.

c. **Civil liability and limits of the business judgment rule**

Finally, failure to implement adequate measures for the prevention and management of cyber risks, as required by the applicable legislation, constitutes a **serious management irregularity** under Articles 2392 and 2476 of the Civil Code (directors' liability in S.p.A. and S.r.l., respectively).

Where technical and procedural requirements are defined by ACN, the scope of the **business judgment rule** (which protects discretionary management decisions) **is significantly reduced**. Non-compliance with the minimum standards set out in the NIS2 Decree cannot be considered a managerial choice, but rather **a regulatory breach** that exposes directors to liability for damages suffered by the company, its creditors or its shareholders.

***

The **management body plays a central and non-delegable role** in cyber-risk management, requiring the adoption of adequate organizational arrangements, the supervision of security measures, and oversight of the proper functioning of incident-prevention and response processes.

The **obligation to be completed by the upcoming 31st December, concerning the designation of the CSIRT contact point**, forms part of this regulatory framework, which requires companies to clearly structure the internal responsibilities and information flows necessary to ensure the timely handling of incidents and compliance with notification obligations.

A structured, informed and well-documented approach to cyber risk is today not only a regulatory obligation, but an essential requirement for safeguarding the company, ensuring business continuity and reducing directors' exposure to liability.

LAW·P
STUDIO LEGALE E TRIBUTARIO

For any clarifications or assistance regarding these requirements, please do not hesitate to contact our firm.