TopHic | dig deeper

June 2025

Cyber Insights: security, compliance, third parties

Expert's opinion

Third parties and cyber risk management

*by **Roberto Antoniotti***

Head of Technology and Innovation - Bernoni Grant Thornton

In today's environment, characterized by increasing digital interconnectedness and increasingly globally distributed supply chains, third-party cyber risk management has become an indispensable element of organisations' security strategies. The fact that 48% of data breaches in 2024 were estimated to be caused by vulnerabilities arising from access or relationships with external providers confirms how these players represent a privileged entry point for cyber criminals. Faced with this scenario, it is no longer sufficient to rely on sporadic compliance audits or static partner assessments: it is necessary to adopt evolved technological solutions and structured processes capable of ensuring dynamic, continuous and...

read more

Overview

Cybersecurity today: from an option to a need for companies

*by **Francesco Carraro***

Manager - Bernoni Grant Thornton

Due to the increasingly pervasive digitization, cybersecurity is no longer an option: it has become a necessity. Indeed, the expansion of digital technologies and services means that the attack surface for cybercriminals is increasing exponentially, and the most serious issue is that users are not always fully aware of this. According to the most recent CLUSIT Report, 3,541 serious cyber-attacks were recorded globally in 2024, the highest number ever recorded, with a 27% growth compared to the previous year In Italy, the picture is particularly alarming: the country suffered 10% of global attacks, despite representing only...

read more

Focus on

NIS2: a strategic priority for businesses

*by **Mattia Campagner***

Manager – Bernoni Grant Thornton

The NIS2 Directive is one of the most significant and discussed regulatory novelties, not only for its broad scope, but also for the strategic role it recognises to cybersecurity governance. After providing an overview in the previous paragraph, it is useful to analyse more in depth the main contents of the Directive, from the categories of subjects involved, to the obligations provided and the operating deadlines already defined domestically. Directive EU 2022/2555, better known as NIS2, entered into force on 16 January 2023 and is an evolution of the previous NIS Directive (2016/1148), aimed at strengthening and harmonising digital resilience all over...

read more

Supplemento Notizie flash n° 107 del 25 febbraio 1984

Grant Thornton

Overview

Cybersecurity today: from an option to a need for companies

by **Francesco Carraro**
Manager - Bernoni Grant Thornton

Due to the increasingly pervasive digitization, cybersecurity is no longer an option: it has become a necessity. Indeed, the expansion of digital technologies and services means that the attack surface for cybercriminals is increasing exponentially, and the most serious issue is that users are not always fully aware of this. According to the most recent CLUSIT Report, 3,541 serious cyber-attacks were recorded globally in 2024, the highest number ever recorded, with a 27% growth compared to the previous year. In Italy, the picture is particularly alarming: the country suffered 10% of global attacks, despite representing only 1.8% of global GDP. With 357 known serious attacks in 2024, Italy is permanently in the signs of cyber criminals. Cybercrime is responsible for approximately 86% of cyber-attacks globally, a phenomenon that is constantly growing. Among the main factors fuelling this trend is the spread of low-cost "as-a-Service" tools on the dark web, which make illicit activities accessible even to individuals with limited technical skills.

Cybersecurity governance represents a coordinated set of policies, standards, organizational arrangements and compliance mechanisms aimed at ensuring a rigorous supervision of digital security. Areas such as energy, healthcare, finance, telecommunications and transport are recurrent targets of increasingly complex and persistent cyber threats. Moreover, it is not only large corporations or critical infrastructures that are affected, but also and above all small and medium-sized enterprises, which are often less structured and therefore more vulnerable.

An effective governance model creates a protected digital environment, protects sensitive information, ensures continuity of essential services, and contributes to economic stability. Because of its systemic impact, cybersecurity is now increasingly recognized as a priority: governments and regulatory authorities have for some years now been promoting the application of international regulations and standards, which serve as a reference for the development of mature and sustainable security strategies.

These were the topics discussed during the meeting held in Milan, 14-16 May, between the cybersecurity teams of the member firms of the Grant Thornton international network. The event represented an important opportunity for discussing and sharing different perspectives and operational experiences, focusing on the main current cybersecurity challenges. Among the most discussed topics, the NIS2 (Network Information Security) Directive and the ISO/IEC 27001:2022 standard were particularly relevant, confirming their importance in the definition of effective and scalable cyber governance models.

The first NIS Directive (2016/1148) defined an EU-wide regulatory framework designed to improve supranational coordination in the management of network and information system security, with the aim of protecting services that are essential for the functioning of the EU economy and society. Following the rapid evolution of the digital ecosystem, the European Commission initiated a review process that led to the adoption of the NIS2 Directive, which came into force in January 2023. Member states were required to transpose the new directive into their national legislation by 17 October 2024.
NIS2 aims to standardise and further strengthen cybersecurity within the European Union by introducing more stringent risk management and incident reporting requirements and extending them to a larger number of public and private entities (NIS affected around 300 Italian companies, NIS2 involves over ten thousand).

Furthermore, the Directive lays down rules to improve cooperation between Member States, to promote information sharing and to ensure a more effective application of protection measures at national and European level.
At the same time, many companies are choosing to voluntarily adopt international standards such as ISO/IEC 27001:2022, which defines an information security management model (ISMS). This approach makes it possible to map risks, plan countermeasures, monitor the effectiveness of controls and pursue continuous improvement. The ISO/IEC 27002:2022 standard, complementary to 27001, provides detailed operational guidance for the implementation of security controls. The integration of these standards within business processes is often seen as best practice, strengthening security, improving stakeholder confidence and facilitating compliance with regulations such as NIS2 and GDPR.

[1] Clusit, *Report on Cybersecurity in Italy and the World 2025*, p. 9.
[2] Ibid, pp. 30–31.
[3] Ibid, pp. 13–14.
[4] European Commission, *Questions and answers on NIS directive – Strengthening network and information system security in the EU*, n.d.
[5] National Cybersecurity Agency (ACN), *NIS Directive*, n.d
[6] European Commission, *NIS2 Directive*, n.d.

Expert's opinion

Third parties and cyber risk management

*by **Roberto Antoniotti***
Head of Technology and Innovation - Bernoni Grant Thornton

In today's environment, characterized by increasing digital interconnectedness and increasingly globally distributed supply chains, third-party cyber risk management has become an indispensable element of organisations' security strategies. The fact that 48% of data breaches in 2024 were estimated to be caused by vulnerabilities arising from access or relationships with external providers confirms how these players represent a privileged entry point for cyber criminals. Faced with this scenario, it is no longer sufficient to rely on sporadic compliance audits or static partner assessments: it is necessary to adopt evolved technological solutions and structured processes capable of ensuring dynamic, continuous and proactive management of the entire third-party ecosystem.

Most cyber-mature organisations have already integrated advanced tools into their strategies to gain real-time visibility into the risk level of their suppliers and partners. However, these platforms alone are not sufficient to handle the growing complexity of an ever-expanding attack surface involving cloud environments, IoT/OT devices, legacy systems, and third-party applications.

For this reason, Grant Thornton proposes a holistic and integrated approach, combining the latest monitoring and detection technologies with governance, advisory and operational response services.
Central to this proposition is Cybersonar, a proprietary platform that combines Threat Intelligence and Attack Surface Management capabilities, enabling continuous monitoring of the external attack surface and early identification of vulnerabilities, misconfigurations and emerging threats, not only for the organisation but also for its critical third parties. Cybersonar enables organisations to anticipate attacks, strengthen the resilience of the entire digital ecosystem and ensure compliance with regulations such as NIS2 and DORA, which are increasingly relevant across multiple industries.

This platform integrates seamlessly with other leading technology solutions such as Cyberhunter, the proprietary SIEM & SOAR system that enables the automation of detection and response processes, and Defprobe, an NDR solution designed for anomaly and threat detection across enterprise networks, cloud and IoT/OT environments. To complete the ecosystem, Grant Thornton offers innovative tools for predictive brand protection, removal of fake sites and content, confidential dark and deep web searches, as well as AI chatbots that can be customised for specific security needs.

However, technology alone is not enough: to ensure comprehensive protection, Grant Thornton complements its proprietary platforms with a comprehensive portfolio of professional services. In the area of Cybersecurity Governance, companies can count on Cybersecurity Advisory services, the definition of security strategies and governance models (Cybersecurity Strategies & Governance), CISO as-a-Service support, the management of compliance processes with standards and laws such as ISO 27001, NIS2, DORA and GDPR, as well as the development of Security Policies and customised procedures. Particular attention is paid to the Security by Design phase, so that security is integrated from the earliest stages of product, application, and service development.

On the technical side, Grant Thornton provides Cyber Defence services such as vulnerability assessment, penetration testing on networks and web applications, secure code review, forensic activities on digital, mobile and IoT/OT environments, threat modelling, targeted cyber threat intelligence and security posture assessment in complex cloud environments. In the event of an incident, companies are supported by specialised Incident Response & Forensics teams that can intervene quickly to contain, analyse and resolve even sophisticated and large-scale events.

All these capabilities converge in a state-of-the-art Security Operations Centre (SOC), equipped with Managed Detection and Response (MDR) and Network Detection and Response (NDR) functions, for continuous surveillance of IT/OT environments, automated alert management and timely incident response. To support data and access protection, Identity and Access Management (IAM, IGA, PAM), Data Loss Prevention (DLP), Network Access Control (NAC) and Email Security Gateway solutions are also available, which are essential to reduce the internal attack surface and prevent the loss or exfiltration of sensitive information.

Lastly, to mitigate one of the most significant risks, i.e., the human factor, Grant Thornton offers structured Cyber Security Awareness programmes tailored to raise awareness and train staff on secure behaviour, phishing simulation, credential management and incident response.

The experience gained with numerous customers confirms that the real challenge is not only technical, but also governance-related: IT security must move beyond the strictly IT sphere to become a leadership, risk management and governance, corporate culture and awareness objective. In Italy, as highlighted by the CLUSIT 2025 Report, awareness is growing, but the gap compared to the maturity levels of other European countries is still significant.

Italian companies are starting to shift their focus from technological tools towards governance, investing in organizational models, training and risk assessment. This change is necessary to keep up with the constantly evolving European regulatory context. The NIS2 Directive represents one of the most important security and compliance issues for all organizations operating in strategic sectors within the European Union. However, the most recent available data show that full compliance with NIS2 is still a distant goal for many Italian companies: in fact, only 61% of those that have launched a structured initiative are in line with the requirements.

Too commonly, companies show fragmented models, unclear roles and an underestimation of the impact of the supply chain: NIS2 makes these aspects a priority today. In this phase, many organizations are starting assessment and gap analysis activities, often together with ISO/IEC 27001:2022 certifications to structure effective and measurable processes.

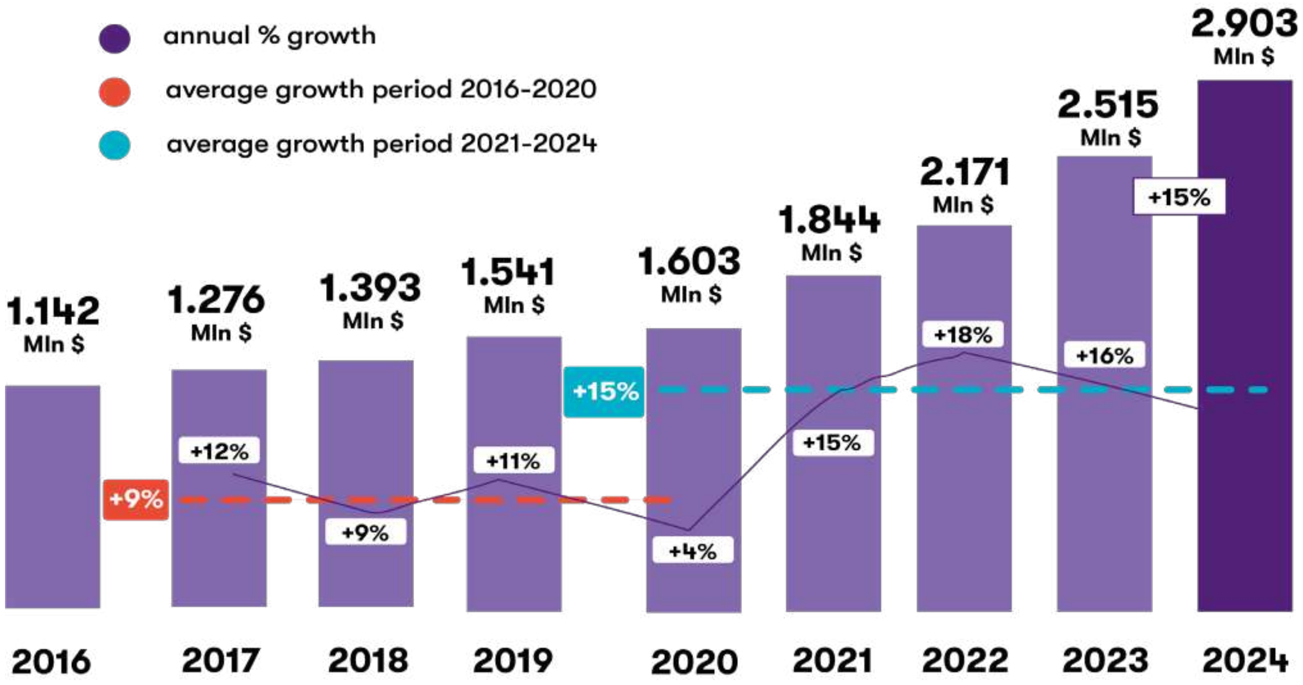
Thanks to its multidisciplinary experience and widespread presence across the territory, Grant Thornton has already successfully supported some Italian companies in starting their NIS2 implementation process. In particular, our teams have conducted in-depth assessments on various organizational levels, from governance to the supply chain, precisely identifying gaps with respect to regulatory requirements and proposing concrete, sustainable and calibrated action plans on the specific context of each company. These interventions subsequently became operational roadmaps that allowed customers to arrive prepared and anticipate regulatory deadlines, increase their IT resilience and strengthen the trust of internal and external stakeholders.

Further recognition of our commitment and expertise in the sector is represented by the ISO/IEC 27001:2022 certification, which attests to the excellence of our information security management system. This result not only consolidates our leadership in the field of cybersecurity but also represents a concrete guarantee for our collaborators: working with a certified partner means relying on professionals who operate according to the highest international standards. Furthermore, the ISO/IEC 27001:2022 certification allows us to transfer proven methods, structured governance and already tested tools to our clients, thus accelerating the compliance process (not only towards NIS2, but also towards other recent regulations such as DORA in the financial sector).

Our goal is not just compliance, but the construction of a solid cybersecurity system, capable of generating value and protecting the business in the long term. In a rapidly evolving regulatory landscape, Grant Thornton represents a reliable partner supporting Italian companies in the transition from a reactive approach to a strategic and proactive cybersecurity vision. Adapting to NIS2 is not just an obligation: it is a responsible choice, which strengthens operational resilience and stakeholder trust.

From a market point of view, the cybersecurity sector is experiencing an unprecedented expansion. The global market was estimated at $245.62 billion in 2024 and is expected to reach $500.70 billion by 2030, with a compound annual growth rate (CAGR) of 12.9% .

The trend is very positive in Italy, too: in 2024, the national market reached 2.48 billion euros, recording a 15% increase % compared to 2023. Among the most dynamic sectors are logistics, transport and services, which, favored by the implementation of the NIS2 Directive, recorded above-average increases by 25% and 24%, respectively.



CISO Survey Sample 2024: 131 Large Organizations

These figures demonstrate a structural transformation in the perception and management of digital risk, fueled not only by new regulations, but also by a greater awareness of the strategic importance of cybersecurity. Companies that know how to promptly invest in structured, integrated and governance-oriented solutions will gain competitive advantage, and be able to count on greater operational resilience, better market positioning and higher credibility towards customers, investors and partners.

[7] ANGI – Associazione Nazionale Giovani Innovatori. *Cybersecurity Observatory: only 61% of companies that have started a structured project towards NIS2 are compliant*, 2024.
[8] Grand View Research, *Cyber Security Market Report*, 2024.
[9] Cybersecurity & Data Protection Observatory – Politecnico di Milano, *The cybersecurity market in Italy: it grew by 15% in 2024*, 2024

Focus on

NIS2: a strategic priority for businesses

*by **Mattia Campagner***
Manager – Bernoni Grant Thornton

The NIS2 Directive is one of the most significant and discussed regulatory novelties, not only for its broad scope, but also for the strategic role it recognises to cybersecurity governance. After providing an overview in the previous paragraph, it is useful to analyse more in depth the main contents of the Directive, from the categories of subjects involved, to the obligations provided and the operating deadlines already defined domestically.

Directive EU 2022/2555, better known as NIS2, entered into force on 16 January 2023 and is an evolution of the previous NIS Directive (2016/1148), aimed at strengthening and harmonising digital resilience all over the European Union. Compared with its previous version, NIS2 significantly broadens its scope of application to include a higher number of industries and impose more stringent obligations on risk management, incident notification and corporate management responsibility.

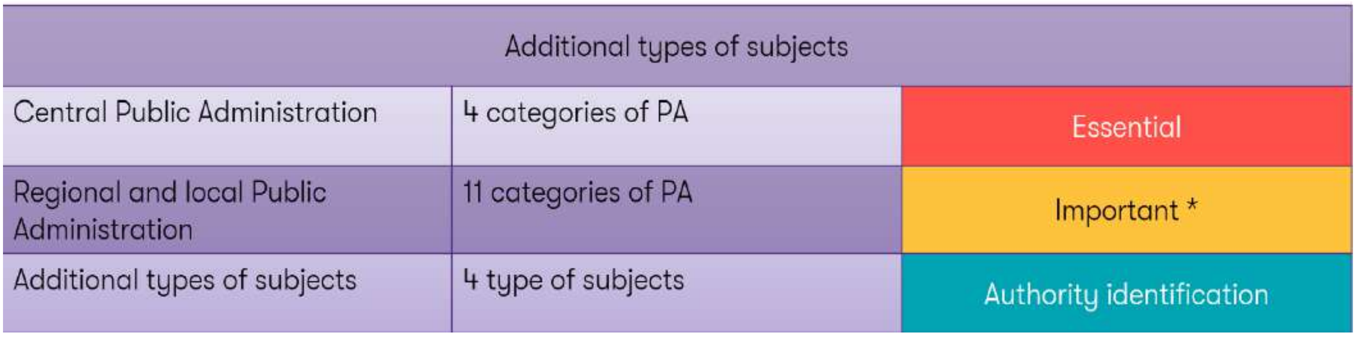
As for its scope of application, the compliance obligation mainly concerns those organisations falling under the category of medium to large enterprises, which exceed some size thresholds provided for this classification based on European Commission Recommendation 2003/361/EC. According to this definition, a medium enterprise has less than 250 employees and a yearly turnover not exceeding 50 million euros, or a financial statements result lower than 43 million euros. Smaller sized businesses, i.e. small and micro enterprises, generally with less than 50 employees and a turnover or financial statements result not exceeding 10 million euros, are - generally speaking - excluded, except for those operating in industries considered strategic or performing functions particularly relevant for national security or again for the continuity of essential services. Moreover, the new NIS2 Directive includes a total 18 industries, 11 of which considered highly critical (compared to the 8 included in the previous Directive) and 7 additional industries classified as critical. Within this framework are more than 80 categories of subjects, divided into two macro-groups: essential entities and important entities, depending on their nature and on the strategic importance of the activities performed.

Industry	Detail	Large companies	Medium sized companies	Small and micro enterprises
Highly critical industries				
Energy	19 types of subjects	Essential	Important*	Out of scope**
Transport	10 types of subjects			
Banking sector	DORA Lex specialis			
Financial market infrastructures				
Healthcare	5 types of subjects			
Drinking water	1 type of subject			
Wastewater	1 type of subject			
Digital infrastructures	9 types of subjects			
Management of ITC services (b2b)	2 types of subjects		Important*	Out of scope**
Space	1 type of subject			

Figure 1 – Breakdown of highly critical industries into essential and important entities [10]

Critical industries			
Post and courier services	1 type of subject	Important*	Out of scope**
Waste management	1 type of subject		
Manufacturing, production and distribution of chemicals	1 type of subject		
Production, processing and distribution of food	1 type of subject		
Manufacturing	6 types of subjects		
Digital service providers	4 types of subjects		
Research	2 types of subjects	Important*	Out of scope**

Figure 2 – List of critical industries [11]



Additional types of subjects		
Central Public Administration	4 categories of PA	Essential
Regional and local Public Administration	11 categories of PA	Important *
Additional types of subjects	4 type of subjects	Authority identification

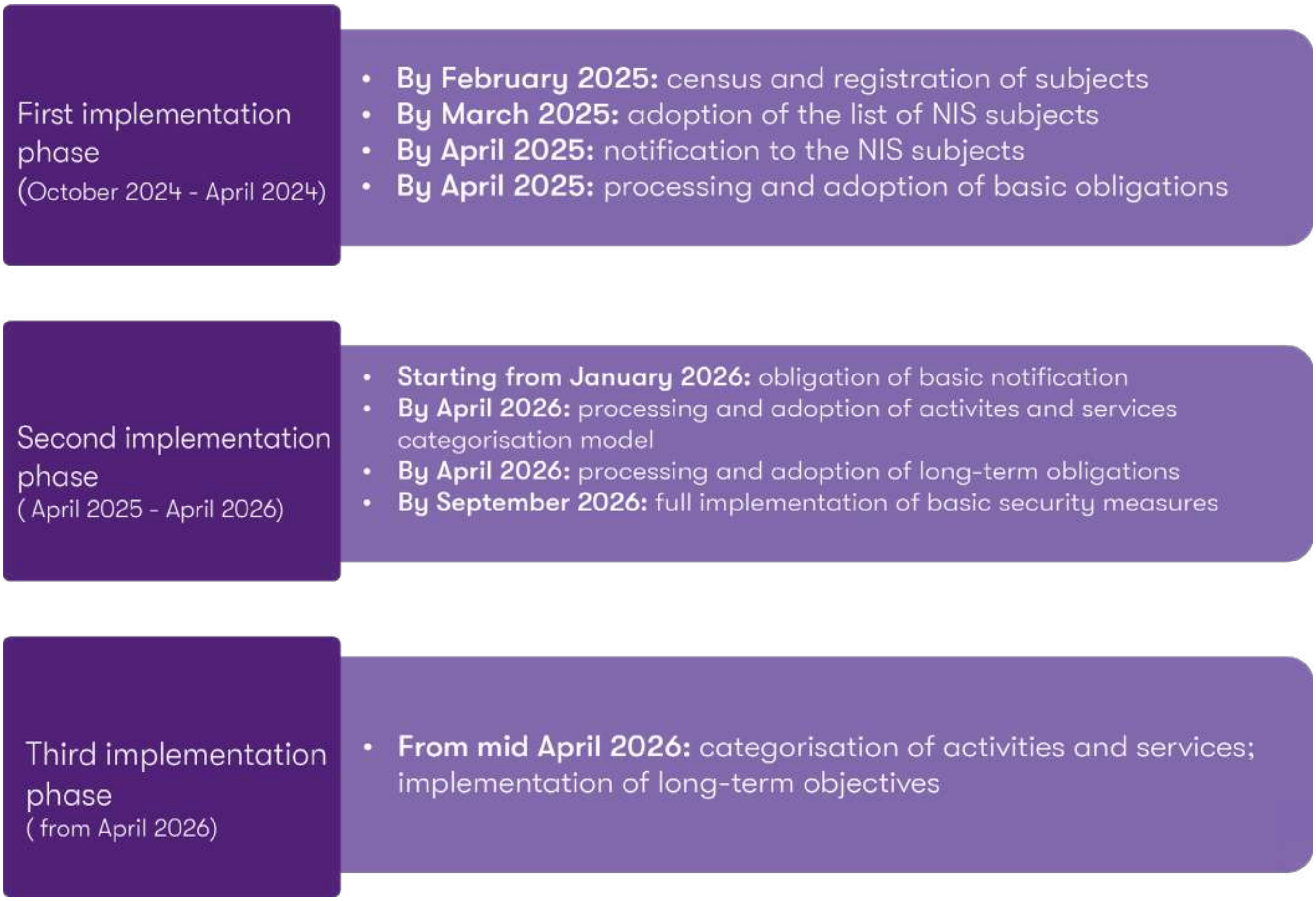
Figure 3 – Breakdown of additional types of subjects into essential and important entities [12]

As for the operational obligations, the Directive provides for the adoption of adequate and documented risk management measures, the implementation of procedures for a timely notification of incidents, to be reported to the national authorities within 24 hours from their discovery (compared to the 72 hours provided by the previous regulation), the introduction of control mechanisms on supply chain security, which require organisations to evaluate and monitor risks related to their external suppliers and partners, particularly those managing IT services, infrastructures or confidential information, the definition of business continuity and crisis management plans, the accountability of the top management, which may be directly sanctioned in case of serious breaches.

A distinctive feature of the NIS2 Directive is the introduction of a strengthened penalty system. In particular, essential entities can be fined up to 10 million euros or for an amount up to 2% of their total worldwide average turnover (whichever the higher), whereas for important entities the maximum penalty is equal to 7 million euros or 1.4% of the turnover.

Besides fines, the Directive also introduces additional forms of direct accountability for the top management. In case of significant non-compliance, managers may be subject to specific measures by the competent authority, including temporary withdrawal of decision-making functions as for security and training obligations. This implies that cybersecurity governance cannot be entirely delegated to operating or technical structures: it is up to the Board of Directors, together with the top management, to guarantee strategic monitoring and compliance with the regulation. Thus, the penalty system provided by the NIS2 Directive, is not limited to hitting the organisation as a whole, but directly involves decision makers, in the logic of an increased accountability and transparency in the management of IT risk.

As far as Italy is concerned, the NIS2 Directive was implemented with Legislative Decree no. 138/2024. THe Decree assigns to the National Cybersecurity Agency (Agenzia per la Cybersicurezza Nazionale - ACN) a pivotal role in supervision and coordination, defines the methods of identification of the obliged entities and establishes the reference digital platform for the management of communications and notifications. The main operational deadlines for Italian entities are:



First implementation phase (October 2024 - April 2024)	• **By February 2025:** census and registration of subjects • **By March 2025:** adoption of the list of NIS subjects • **By April 2025:** notification to the NIS subjects • **By April 2025:** processing and adoption of basic obligations
Second implementation phase (April 2025 - April 2026)	• **Starting from January 2026:** obligation of basic notification • **By April 2026:** processing and adoption of activites and services categorisation model • **By April 2026:** processing and adoption of long-term obligations • **By September 2026:** full implementation of basic security measures
Third implementation phase (from April 2026)	• **From mid April 2026:** categorisation of activities and services; implementation of long-term objectives

With the NIS2 Directive, the European Union is making a qualitative leap in building a solid, integrated and prevention-oriented cybersecurity system. For the companies involved, this is a complex but necessary challenge, requiring investments, skills and a structured approach. But above all, it is a concrete opportunity to strengthen their resilience, stakeholder trust and competitiveness in the market.

[10] Source: *Agenzia per la Cybersicurezza Nazionale* (ACN) (National Cybersecurity Agency), *Ambito di applicazione NIS2*, n.d.
[11] Ibid.
[12] Ibid.

We can help you protect your future

Grant Thornton