CyberGrant
SECURITY MADE EASY

WHITE PAPER

NIS2: is your business at risk?

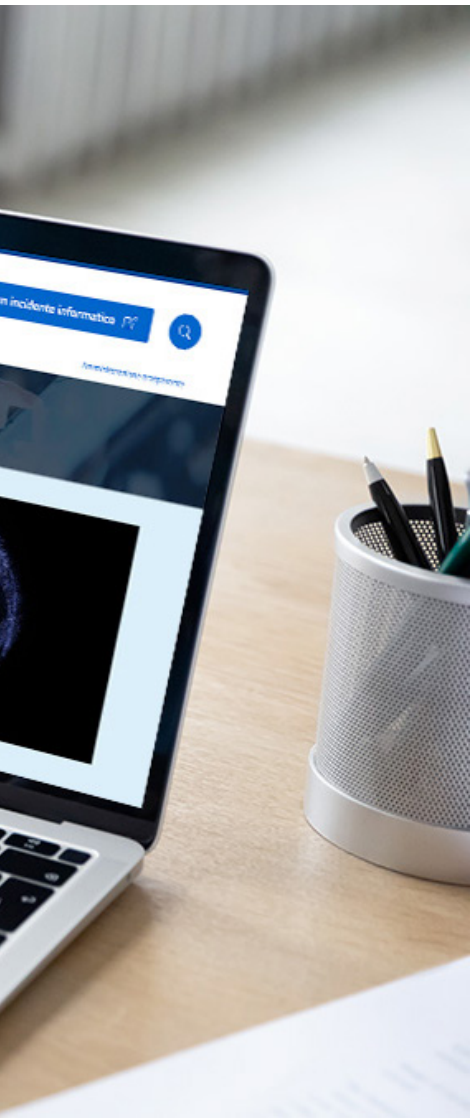
How to avoid penalties and strengthen your cybersecurity posture

Everything CEOs, CFOs, CISOs, and board members need to know to ensure compliance and protect the business

NIS2 compliance: what it means today

The NIS2 Directive was officially transposed into Italian law in October 2024. Yet many organizations are still assessing whether they fall within its scope and what specific requirements they must meet. A key difference from the earlier NIS1 is that top management - including legal representatives and corporate governance bodies - now bear direct accountability for cybersecurity oversight.

Index



Introduction

What changes with NIS2

The EU Directive 2022/2555, widely known as NIS2 (Network and Information Security Directive), marks a significant milestone in the European cybersecurity regulatory framework. It addresses the increasing volume and sophistication of cyber threats and imposes stricter obligations on organizations operating across the EU.

NIS2 introduces mandatory requirements in governance, risk management, and incident reporting. It expands the scope of covered entities compared to its predecessor (NIS1) and **places substantial compliance responsibilities on executive leadership** - including mandatory training and direct oversight of corporate cybersecurity strategies.

Failure to comply **could result in severe sanctions**, including removal from executive functions.

Let's break it down.

NIS2 is here: what you need to know

Although the EU's deadline for implementing NIS2 was **October 17, 2024,** many Member States have yet to complete local enforcement. The map below shows the implementation status across Europe as of April 30, 2025.

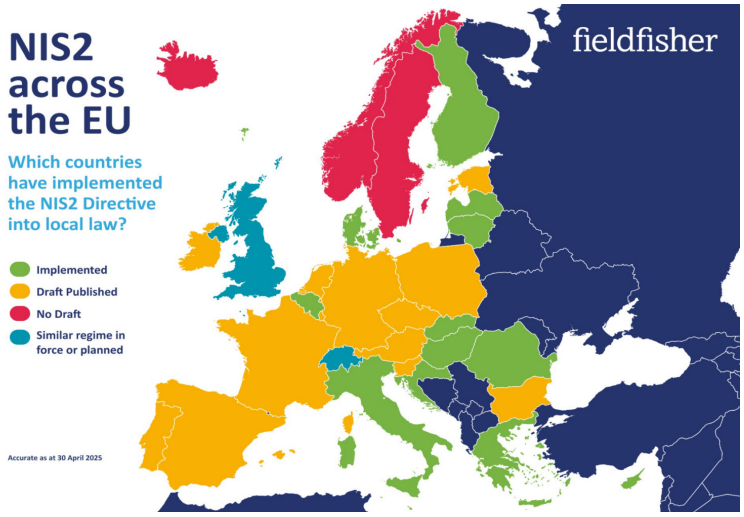


Image source: Fieldfisher, 2025. NIS2 across the EU -summary.

NIS2 significantly broadens the scope of the original directive. It brings more sectors under regulation, requires enhanced security controls, and enforces more rigorous incident reporting protocols. As a result, organizations previously excluded may now be required to deploy entirely new cybersecurity systems and practices.

Entities already regulated under NIS1 may need to reassess and upgrade their cybersecurity posture to meet new compliance thresholds.

Sectors covered

“Essential” sectors and “important” sectors

NIS2 **classifies entities as either “essential” or “important”** and expands coverage across numerous industries.

It also introduces **size-based thresholds**, extending applicability to relevant suppliers and service providers.

ESSENTIAL SERVICES

- Energy
- Transport
- Banking
- Financial market infrastructure
- Healthcare and health services
- Drinking water
- Wastewater
- Telecommunications infrastructure
- Public administration
- Space

IMPORTANT SERVICES

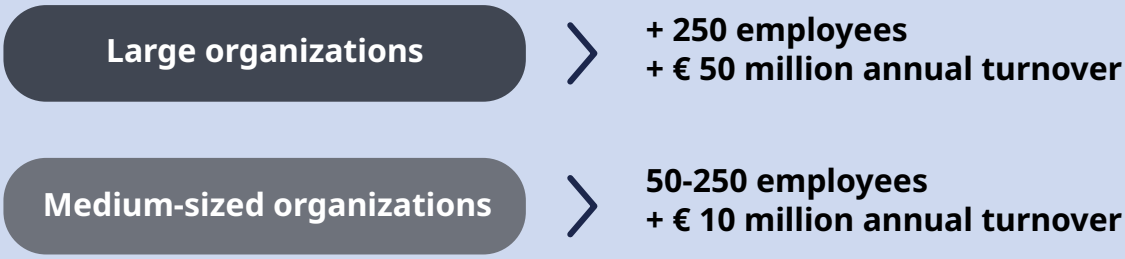
- Postal and courier services
- Waste management/treatment
- Chemical sector: production and distribution
- Food sector: production, processing, and distribution of food, i.e. including large-scale distribution
- Technology and engineering industries
- Digital services
- Research

+

SUPPLIERS & SERVICE PROVIDERS

of:

- Essential Services
- Important Services



Size of the companies involved

Exemptions apply to organizations with:

< 50 employees

< € 10 million in annual turnover

However, these thresholds don't apply if the organization:

- Operates public electronic communication networks or trust services (e.g., DNS, TLD registries)
- Is a public entity whose service disruption could significantly impact economic or social activities
- Is the sole provider of a critical service in a Member State
- Offers services whose interruption could affect public safety or health
- Could trigger systemic risks, especially in cross-border sectors
- Is deemed critical under Directive (EU) 2022/2557 on the resilience of critical entities (CER)

Importantly, any entity delivering critical services within the EU is subject to NIS2 - even if headquartered outside the EU and lacking a physical EU presence.

Penalties

Non-compliance with NIS2 may lead to serious penalties:

Essential entities	Important entities
Up to **€10 million or 2%** of global annual revenue	Up to **€7 million or 1.4%** of global annual revenue

Executive accountability

One of the most groundbreaking changes is the **direct accountability of C-level executives and board members**.

These individuals are responsible for:

- Leading compliance initiatives
- Overseeing security governance and risk management
- Promoting cybersecurity training across the organization
- Personally ensuring the adequacy of cybersecurity strategies

Penalties for non-compliance may include disqualification from executive roles.

Leadership must actively foster a cybersecurity-first culture - not just delegate responsibility. This includes mandatory internal training programs to strengthen organizational resilience.

Incident reporting obligations

NIS2 enforces strict incident notification timelines:

- **Within 24 hours –** Initial notification to the competent authority or CSIRT, indicating suspected malicious origin or potential cross-border impact
- **Within 72 hours –** Follow-up with incident assessment, impact details, and indicators of compromise
- **Upon request –** Progress reports during incident resolution
- **Within 1 month –** Final report detailing root cause, overall impact, mitigation efforts, and current status (if not fully resolved)

Authorities will assess not only whether a company suffered an incident but how effectively it responded.

Key requirements of NIS2

NIS2 adopts a risk-based, multi-risk approach that extends beyond digital threats to include physical, environmental, and human-related risks. Compliance rests on four strategic pillars:

1. **Executive accountability –** top management must understand and own the risk management process
2. **Regulatory reporting** – clear procedures must be in place for incident reporting
3. **Risk management** – organizations must implement proactive security controls across systems, networks, supply chains, and access points
4. **Business continuity** – formal plans must exist for system recovery and crisis management during **severe cyber events**

Ten minimum cybersecurity measures required

Entities within NIS2's scope must implement and demonstrate the following minimum controls:

1. **Risk assessment & security policies –** frameworks to assess and mitigate cybersecurity risks
2. **Effectiveness testing –** procedures to assess the performance of security measures
3. **Encryption policies** – guidelines for applying encryption and data protection
4. **Incident response plan –** detailed playbooks for rapid response to security events
5. **Secure development lifecycle –** vulnerability handling throughout system lifecycle
6. **Employee training –** ongoing awareness programs to build a strong human firewall
7. **Sensitive data access controls –** strict access policies and resource inventories
8. **Business continuity & disaster recovery –** comprehensive BCDR plans with regular backups
9. **Human resource security –** MFA, secure communications, and access governance
10. **Supply chain security –** risk assessments, contractual controls, and supplier engagement

NIS2 compliance timeline (Italy)

Guidelines from ACN

The National Cybersecurity Agency (ACN) oversees implementation in Italy. Key milestones include:

- **From Dec 1, 2024 –** Voluntary registration opens on ACN's platform
- **By Jan 17, 2025 –** Registration deadline for cloud, data center, managed services, and online marketplaces
- **By Feb 28, 2025 –** Registration deadline for all other in-scope organizations
- **By April 15, 2025 –** ACN confirms scope inclusion and publishes required security measures
- **April 15–May 31, 2025 –** Entities must submit key operational data to ACN
- **May–June 2025 –** Entities must update service and activity listings
- **Jan 1, 2026 –** Entities must begin formal incident reporting and annual updates
- **By Oct 2026 –** Full implementation of baseline controls and supply chain security

EU-wide deadlines

- **By Apr 17, 2025** – Member States finalize lists of essential and important entities
- Every 2 years **from Apr 17, 2025** – Member States notify the Commission of covered entities
- **Every 36 months from Oct 17, 2027 – The Commission reviews the directive's effectiveness**

NIS2 and the CIA triad

NIS2 is grounded in the core principles of the CIA Triad:

Confidentiality

Ensures that sensitive information is only accessible to authorized individuals. Breaches may result from hacking, insider threats, misconfigured systems, or human error.

Recommended measures include:

- Access control
- Data classification
- MFA and Zero Trust architecture
- Employee training

Integrity

Protects data from unauthorized alteration. Techniques include:

- Hashing
- Encryption
- Digital signatures
- Non-repudiation controls

Availability

Ensures authorized users have timely access to data and systems. Threats include natural disasters, DDoS attacks, and infrastructure failures. Key safeguards:

- Redundant systems
- Regular backups
- Tested disaster recovery plans

NIS2 vs. U.S. regulations

Executive accountability

The EU's NIS2 establishes a harmonized cybersecurity framework for critical infrastructure. The U.S., by contrast, follows a decentralized, sector-specific approach.

However, the release of NIST's Cybersecurity Framework 2.0 (CSF2) in January 2024 introduces strong similarities. Both CSF2 and NIS2 share a risk-based structure and emphasize asset identification, threat mitigation, and continuous improvement.

The SEC's S-K regulation (effective December 2023) also aligns partially with NIS2 in requiring public companies to disclose cybersecurity governance and incident impact. But while S-K focuses on financial transparency and investor protection, NIS2 prioritizes operational resilience and cross-sectoral security standards.

How CyberGrant Inc. Supports NIS2 Compliance

CyberGrant Inc., headquartered in Menlo Park, California, offers two complementary solutions that support compliance with NIS2 requirements:

Risk management

- **FileGrant Enterprise** – Provides advanced encryption and access controls
- **RemoteGrant** – Delivers endpoint protection, vulnerability scanning, and patching

Threat monitoring and response

- **FileGrant Enterprise** – Real-time document access monitoring and revocation
- **RemoteGrant –** Logs unauthorized activities and detects threats via 75+ antivirus engines

Unauthorized access prevention

- **FileGrant Enterprise** – Role-based access, screen capture protection, and encryption
- **RemoteGrant** – MFA, IP whitelisting, and endpoint access restrictions

Incident reporting

- **FileGrant Enterprise** – Integrates with SIEMs for instant breach notifications
- **RemoteGrant** – Offers tiered logging and reporting for compliance-ready insights

Secure data sharing

- **FileGrant Enterprise** – Prevents unauthorized duplication with advanced encryption
- **RemoteGrant** – Blocks remote file transfers to prevent data exfiltration

CyberGrant is committed to helping organizations of all sizes turn regulatory compliance into a strategic advantage - empowering secure growth, operational resilience, and long-term trust in the digital ecosystem.

Edited by **Federica Maria Rita Livelli**

www.cybergrant.net