# NIS2 Directive:
# A strategic compliance guide for business leaders and security executives

## Directive (EU) 2022/2555 (NIS2) – Implementation, strategic impact and compliance roadmap

**Authors:**

Sławek Pijanowski,
*Global GRC Practice Leader – Cybersecurity Advisory*

**Editorial Team:**

Srikanth Raju,
*Global Head of Marketing for Cybersecurity Services*

Elisabeth Samadinger-Regner,
*Global Marketing Lead for Cybersecurity Consulting*

# Executive summary

**The digital landscape of the European Union has undergone a seismic shift with the enforcement of the Network and Information Systems Directive 2 (NIS2). Replacing the original 2016 NIS Directive, NIS2 is not merely an update; it is a fundamental restructuring of how Europe approaches cybersecurity. For business leaders, the era of treating cybersecurity as solely an IT operational task is over. NIS2 elevates cyber resilience to a board-level responsibility, introducing personal liability for executives and significant financial penalties for non-compliance.**

**This whitepaper serves as a strategic guide for organizations navigating this new regulatory environment. It simplifies the complex legal language of the directive into actionable business intelligence. We analyze the expanded scope which now impacts approximately 160,000 entities across 18 critical sectors and detail the rigorous risk management measures required under Article 21.**

## Key takeaways for executive leadership include:

**Expanded scope**

If you operate in energy, transport, health, digital infrastructure, manufacturing or supply chain services, you are likely in scope.

**Personal accountability**

C-suite executives and board members can be held personally liable for gross negligence in cybersecurity governance.

**Stricter penalties**

Fines can reach up to €10 million or 2% of global annual turnover for Essential Entities.

**Rapid reporting**

Significant incidents must be reported within 24 hours—a timeline that demands mature detection and response capabilities.

## Introduction: The new era of cyber resilience

### From NIS1 to NIS2

The original NIS Directive (NIS1), adopted in 2016, was the first piece of EU-wide legislation on cybersecurity. While it laid the groundwork, it suffered from fragmentation; member states implemented it differently, leading to inconsistent levels of security and gaps in cross-border cooperation. Compounding these issues, the threat landscape has evolved dramatically. Ransomware has industrialized, supply chain attacks have crippled critical infrastructure and geopolitical tensions have turned the digital domain into a contested space.

### NIS2 (Directive (EU) 2022/2555) addresses these shortcomings by:

- **Harmonizing rules:** Establishing a unified baseline for cybersecurity management and reporting across all 27 Member States.
- **Expanding coverage:** Moving beyond “operators of essential services” to a broader definition of “Essential” and “Important” entities.
- **Strengthening enforcement:** Giving national authorities real teeth, including the power to conduct on-site inspections and suspend executives.

### The “all-hazards” approach

A critical philosophical shift in NIS2 is the mandate for an “all-hazards approach.” This means organizations cannot just focus on malicious cyberattacks (like hackers or malware). They must also build resilience against physical events (fires, floods), human error, system failures and supply chain disruptions.

> “Compliance requires an integrated view of security where physical and digital risks are managed holistically.”

## Decoding applicability: Are you in scope?

One of the most immediate challenges for business leaders is determining whether their organization falls under the directive. NIS2 moves away from the reliance on national identification (where states told you if you were critical) to a size-cap rule.

**The general rule:** If you provide a service in one of the critical sectors listed below and are a Large enterprise (≥50 employees or ≥€10m turnover), you are automatically in scope.

EU Member States have the right to include additional sectors or subsectors, regardless of company size, if this is critical for a given country's resilience.

### The two categories of entities

NIS2 classifies organizations into two categories with differing supervisory regimes but largely identical security obligations.

#### A. Essential entities (EE)

- **Sectors (Annex I):** Energy, Transport, Banking, Financial Market Infrastructures, Health, Drinking Water, Waste Water, Digital Infrastructure (Cloud, Data Centers, DNS, TLDs), ICT Service Management (B2B including ICT Managed Security Services), Public Administration, Space.
- **Supervision: Ex-ante** (proactive). Authorities will monitor compliance regularly, not just after an incident.
- **Penalties:** Higher fines (up to €10M or 2% of global turnover[1]).

#### B. Important entities (IE)

- **Sectors (Annex II):** Postal and Courier Services, Waste Management, Chemicals (Production/Distribution), Food (Production/Processing/Distribution), Manufacturing (Medical devices, Computers, Electronics, Machinery, Vehicles), Digital Providers (Search engines, Marketplaces, Social networks), Research Organizations.
- **Supervision: Ex-post** (reactive). Authorities act only if they receive evidence of non-compliance or after a significant incident.
- **Penalties:** Slightly lower fines (up to €7M or 1.4% of global turnover[2]).

### Critical nuances in scoping

Leaders must be aware of exceptions where size does not matter. You may be in scope regardless of size if:

- You are a **sole provider** of a service essential for societal or economic activities.
- Disruption of your service would have a **significant systemic impact** on public safety or health.
- You are a **Trust Service Provider**, TLD name registry, or DNS service provider.
- You are a public administration entity defined by national law.

**Jurisdiction:** Unlike GDPR, where the "One-Stop-Shop" often applies, NIS2 jurisdiction is generally based on where the entity is *established*. However, for Digital Infrastructure providers (Cloud, Data Centers) offering services across borders, jurisdiction is often where their **main** *establishment* in the EU is located. This requires careful legal analysis especially for multinational corporations.

[1] EU Member States may decide on local adoption of above parameters of those penalties.

[2] As in previous footnote / reference.

## The board’s responsibility: Governance and accountability (Article 20)

NIS2 fundamentally changes the role of the C-suite and Board of Directors regarding cybersecurity. It explicitly prevents the transfer of accountability.

### Personal liability

For the first time in EU cybersecurity law, “management bodies” (boards, CEOs, executive committees) can be held personally liable for non-compliance.

- **Suspension:** In the case of Essential Entities, competent authorities have the power to temporarily suspend certification or authorization concerning part or all of the relevant services provided. Crucially, they can also request the temporary prohibition of any person discharging managerial responsibilities at the CEO or legal representative level from exercising managerial functions.
- **Public naming:** Authorities can order organizations to make their non-compliance public, identifying the legal and natural persons responsible.

> **“For business leaders, the era of treating cybersecurity as solely an IT operational task is over. NIS2 elevates cyber resilience to a board-level responsibility.”**

> **“You can outsource your IT security operations, but you cannot outsource your liability.”**

### Mandatory training

To avoid “gross negligence” claims, board members must be literate in cyber risk. Article 20 mandates that members of management bodies follow specific training to gain sufficient knowledge and skills to identify risks and assess cybersecurity management practices. Furthermore, they must encourage similar training for employees.

### Active oversight

The board is required to:

1. **Approve** the cybersecurity risk management measures.
2. **Oversee** their implementation.
3. Be Accountable for any rigorous failures. This means cybersecurity must be a standing agenda item, not an annual update. Boards must demand clear, non-technical metrics on cyber resilience (e.g., Mean Time to Respond, Patching Status, Supply Chain Risk) to make informed decisions.

# Not only a CISO mandate: Risk management measures (Article 21)

## (CISO, BCM, CSO, IT and Procurement...)

Article 21 is the operational heart of NIS2. It lists 10 baseline security measures that every Essential and Important entity must implement. These are not optional; they are the legal minimum standard for "due diligence."

## The 10 pillars of article 21

### 1. Policies on risk analysis & information system security

- **Requirement:** Organizations must have a formalized framework for identifying, analyzing and evaluating cyber risks. This isn't a one-time audit; it must be continuous.
- **Action:** Transition from ad-hoc risk assessments to a structured Enterprise Risk Management (ERM) model that includes cyber risk.

### 2. Incident handling

- **Requirement:** Procedures for the detection, analysis, containment and response to incidents.
- **Action:** Move beyond simple IT ticketing. Implement a dedicated Incident Response Plan (IRP) that is tested regularly via tabletop exercises.

### 3. Business continuity & crisis management

- **Requirement:** Backup management, disaster recovery and crisis management.
- **Action:** Ensure backups are immutable (ransomware-proof) and tested. Differentiate between IT recovery (getting servers up) and Business Continuity (keeping the business running during an outage).

### 4. Supply chain security

- **Requirement:** Managing security aspects concerning the relationships between the entity and its direct suppliers or service providers.
- **Action:** This is one of the hardest requirements. You must assess the security posture of your software, hardware or IT infrastructure vendors, managed service providers (MSPs), data centers and any suppliers of product's components with digital elements.

### 5. Security in network & information systems acquisition

- **Requirement:** Handling security during the development and maintenance lifecycle, including vulnerability disclosure.
- **Action:** Adopt a "Secure by Design" approach. Implement rigorous testing before new systems go live. Establish a Coordinated Vulnerability Disclosure (CVD) policy to receive reports from ethical hackers.

### 6. Effectiveness assessment

- **Requirement:** Policies and procedures to assess the effectiveness of cybersecurity risk management measures.
- **Action:** Regular auditing and testing. Don't just assume controls work; prove it through penetration testing, independent reviews and KPI monitoring.

### 7. Cyber hygiene & training

- **Requirement:** Basic cyber hygiene practices and training for staff.
- **Action:** Implement zero-trust principles, regular software updates, device management and mandatory awareness training (phishing simulations, etc.) for all staff.

### 8. Cryptography & encryption

- **Requirement:** Policies regarding the use of cryptography and, where appropriate, encryption.
- **Action:** Encrypt data at rest and in transit. Manage cryptographic keys securely.

### 9. Human resources security

- **Requirement:** Access control policies and asset management.
- **Action:** Implement robust Onboarding/Offboarding processes. Ensure strict Role-Based Access Control (RBAC)—employees should only access data necessary for their role.

### 10. Multi-factor authentication (MFA)

- **Requirement:** Use of MFA, continuous authentication and secure communications.
- **Action:** MFA should be mandatory for all remote access and privileged accounts. No exceptions.

# The Speed of Transparency: Reporting Obligations (Article 23)

One of the most significant operational shifts in NIS2 is the stringent timeline for incident reporting. The directive aims to provide national authorities with near-real-time visibility into threats to prevent cascading effects across borders.

## What is a "Significant Incident"?

An incident is considered significant if:

1. It causes (or is capable of causing) severe operational disruption or financial loss. Also those incidents which happened twice or more due to the same cause in 6 months if cumulatively exceed required threshold for reporting
2. It affects other persons (natural or legal) by causing considerable material or non-material damage.

## The "24-72-1" Timeline

Entities must adhere to a three-stage reporting process:

**Early Warning (Within 24 Hours):**

- **Trigger:** Becoming aware of the significant incident.
- **Content:** Minimal information indicating whether the incident is suspected to be malicious and if it has cross-border impact.
- **Goal:** To alert the respective industry or governmental CSIRT (Computer Security Incident Response Team) so they can warn others or offer assistance.

**Incident Notification (Within 72 Hours):**

- **Content:** An update to the early warning. It must include an initial assessment of severity, impact and "Indicators of Compromise" (IoCs).
- **Goal:** To provide technical details that help containment.

**Final Report (Within 1 Month):**

- **Content:** A detailed description of the incident, including the root cause, mitigation measures applied and the final impact assessment.
- **Goal:** Lessons learned and regulatory closure.

**Intermediate Reports:** In some cases, the CSIRT may request status updates between the 72-hour and 1-month window.

## The cost of non-compliance: penalties and enforcement

NIS2 aligns its penalty structure closely with GDPR to ensure fines are "effective, proportionate and dissuasive."

**Administrative fines**

| Entity Category | Supervision Model (Risk of Audit) | Maximum Financial Penalty |
|---|---|---|
| Essential Entities (EE) | **Proactive (Ex-ante):** Regular audits, on-site inspections and systematic oversight. | **€10,000,000** or **2%** of global annual turnover (whichever is higher). |
| Important Entities (IE) | **Reactive (Ex-post):** Regulatory action triggered only by incidents or evidence of non-compliance. | **€7,000,000** or **1.4%** of global annual turnover (whichever is higher). |

Note: These are maximums. Member states will determine the exact fine based on the severity of the breach, the duration and previous infringements.

## Non-financial enforcement

Often more damaging than fines are the administrative powers granted to regulators:

- **On-site inspections:** For Essential Entities, regulators can walk in proactively.
- **Security audits:** Authorities can mandate regular security audits at the entity's expense.
- **Scanning:** Regulators can conduct security scans of your public-facing infrastructure.
- **Warnings and orders:** Binding instructions to remedy deficiencies by a set deadline.

“Operational Challenge: Meeting a 24-hour deadline requires 24/7 monitoring capabilities. Organizations relying on ‘business hours’ security teams will likely fail to meet this requirement.”

# Strategic implementation roadmap

**For Business Leaders like: CISOs, CSO, CIO, COOs / BCM Managers, Procurement and organization's management bodies accountable for NIS2 Supervision and implementation the path to NIS2 compliance can be daunting. We recommend a phased approach, moving from assessment to remediation and continuous improvement.**

## Phase 1: Scoping and awareness (Weeks 1-4)

- **Legal assessment:** Consult legal and compliance teams to determine definitively if you are an Essential or Important entity. Check national transposition laws in every EU country where you operate, as small variations exist.
- **Board buy-in:** Present the "Board's Burden" (Section 4) to executive leadership. Secure budget for the compliance program.
- **Identify critical assets:** Map the specific systems and services that are critical to the economy/society. Not every server in your company is subject to NIS2—only those supporting the essential service.

## Phase 2: Gap analysis & risk assessment (Weeks 5-12)

- **Maturity assessment:** Map your current security controls against the 10 Pillars of Article 21. Use frameworks like ISO 27001 or NIST CSF 2.0 as a baseline.
- **Supply chain audit:** Identify your critical vendors. Send out questionnaires or review their security certifications.
- **Gap report:** Create a prioritized list of deficiencies (e.g., "We have MFA, but not on legacy systems," or "Our incident response plan is outdated").

## Phase 3: Remediation (Months 3-9)

- **Quick wins:** Implement "Cyber Hygiene" basics immediately (MFA, Patching, Backups).
- **Policy overhaul:** Rewrite Incident Response Plans to accommodate the 24-hour notification rule. Update governance policies to include board oversight mechanisms.
- **Technical implementation:** Deploy necessary technologies (SIEM for detection, Encryption tools, Identity Management systems).

## Phase 4: Operationalization (Ongoing)

- **Training:** Roll out cyber awareness training to all staff and specific "Crisis Management" training for the Board.
- **Drills:** Conduct a cyber crisis tabletop exercise simulating a ransomware attack to test the 24-hour reporting flow or other relevant scenarios.
- **Evidence collection:** Start documenting everything.

> **"In an audit,
> if it isn't documented,
> it didn't happen."**

# Focus area: Supply chain security

**Supply chain security (Article 21.2.d) is arguably the most complex requirement of NIS2. The directive recognizes that many recent major attacks (e.g., SolarWinds, Kaseya) originated not in the target organization, but in their software providers.**

## The “trickle-down” effect

Essential Entities are legally required to assess the security of their suppliers.

- **Contractual clauses:** Expect your customers (Essential Entities) to demand right-to-audit clauses and strict security SLAs in your contracts.
- **Software bill of materials (SBOM):** You may be asked to provide transparency on the software components you use.

**Strategy for compliance:**

1. **Categorize suppliers:** Not all suppliers are equal. The catering company is low risk; the Managed Service Provider (MSP) managing your firewall is critical.
2. **Risk-based due diligence:** Don’t send a 500-question Excel sheet to everyone. Tailor assessments to the risk. Leverage modern solution scanning continuously your suppliers’ cyber security posture.
3. **Collaborative security:** Work with key suppliers to improve their posture rather than just penalizing them. Their weakness is your weakness.

> **“Even if your company is not directly in scope of NIS2, if you sell to a company that is, you will be impacted.”**

# Conclusion: From compliance to advantage

The deadline for national transposition of NIS2 was **October 17, 2024** and the rules are now in effect across the EU. While the list of Essential and Important entities is being finalized by Member States (deadline April 2025), organizations cannot afford to wait.

NIS2 should not be viewed solely as a regulatory burden. The measures mandated by the directive—better governance, rigorous risk management and supply chain visibility—are the same measures required to survive in a hostile digital economy.

## Your final checklist:

1. **Confirm your status** (Essential vs Important).
2. **Brief the board** on their personal liability.
3. **Review your incident response Plan** against the 24-hour deadline.
4. **Audit your supply chain** for critical dependencies.
5. **Budget for resilience**, not just compliance.

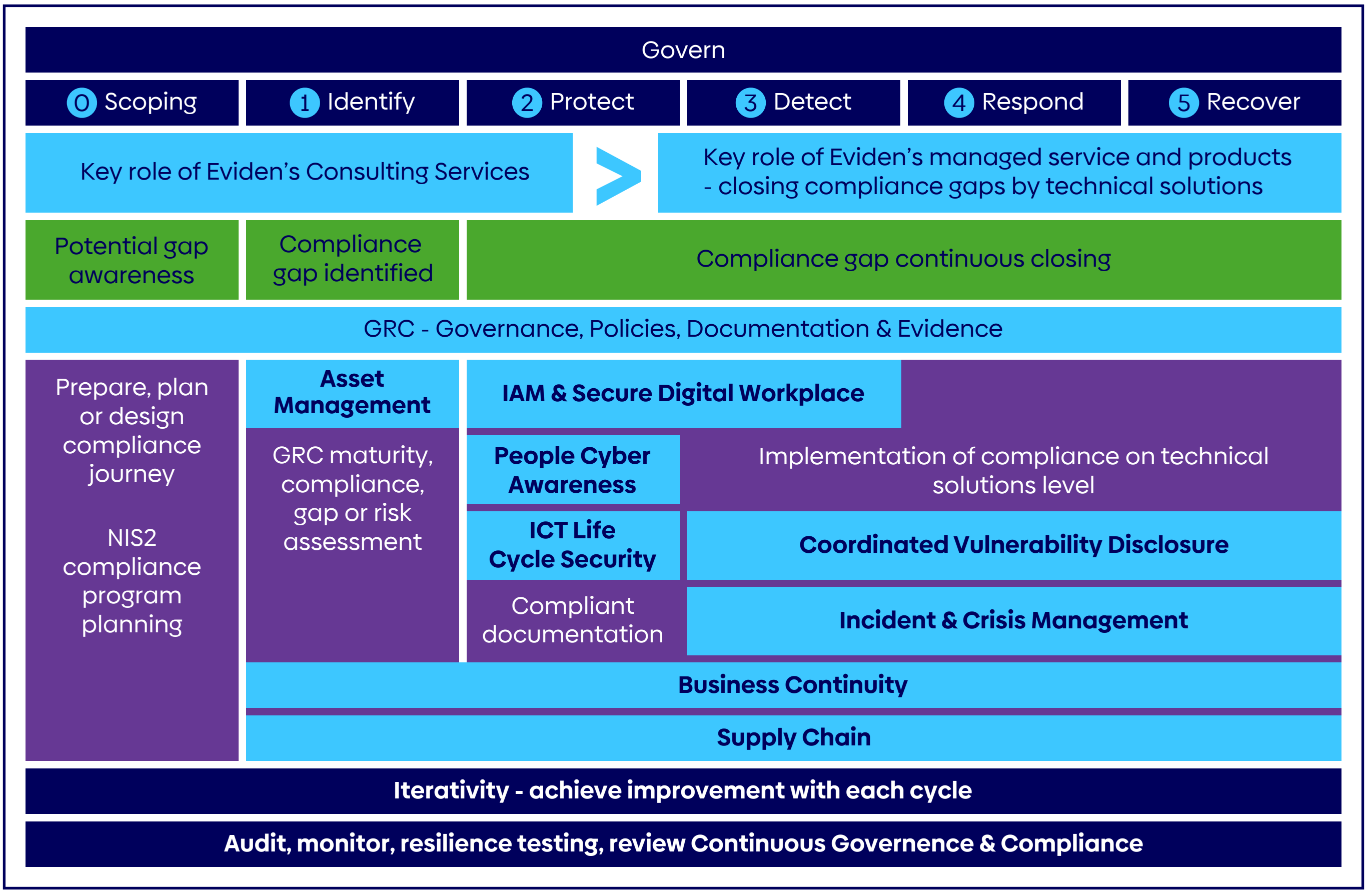
By proactively embracing NIS2, organizations signal to their customers, partners and investors that they are resilient, responsible and ready for the future.

## Atos compliance journey and strategic Support

We offer a holistic NIS2 compliance framework aligned with NIST CSF 2.0 and other state-of-the art industry or domain-specific standards covering domains such as governance, incident management, business continuity, supply chain security, IAM and cyber awareness. The approach includes iterative assessments, gap analysis, planning, implementation and continuous improvement.

> “Compliance with NIS2 should not be viewed as a checkbox exercise but as an opportunity to build genuine resilience.”

### Holistic NIS 2 Compliance Program



Govern

0 Scoping | 1 Identify | 2 Protect | 3 Detect | 4 Respond | 5 Recover

Key role of Eviden's Consulting Services > Key role of Eviden's managed service and products - closing compliance gaps by technical solutions

Potential gap awareness | Compliance gap identified | Compliance gap continuous closing

GRC - Governance, Policies, Documentation & Evidence

Prepare, plan or design compliance journey

NIS2 compliance program planning

**Asset Management**

GRC maturity, compliance, gap or risk assessment

**IAM & Secure Digital Workplace**

**People Cyber Awareness**

Implementation of compliance on technical solutions level

**ICT Life Cycle Security**

**Coordinated Vulnerability Disclosure**

Compliant documentation

**Incident & Crisis Management**

**Business Continuity**

**Supply Chain**

**Iterativity - achieve improvement with each cycle**

**Audit, monitor, resilience testing, review Continuous Governence & Compliance**

Figure 1: Atos' NIS2 compliance program

## Our consulting services include:

- Quick Scan (2–3 weeks): Real Regulatory audit simulation, challenging readiness with strict timelines of your evidence collection process being basis to confirm your compliance- Risk-Based Assessment (7–12 weeks): Deep-dive with cyber risk prioritization including business impact scenarios
- Evidence-Based Assessment: ISO-aligned digital evidence collection

We map NIS2 requirements to over 100 international standards, including ISO/IEC 27001, 22301, 28000 and ISA 62443. Sector-specific mappings (e.g., TISAX, BSI) are also available. Organizations are advised to assess their classification, engage leadership, align documentation and plan remediation budgets.

Our cybersecurity services support end-to-end compliance, from diagnosis to managed services onboarding, with multilingual teams and global reach. The evidence-based methodology ensures organizations are audit-ready and resilient against evolving cyber threats.

## Resources & References

- Atos NIS2 Compliance Methodologies
- Directive (EU) 2022/2555 of the European Parliament and of the Council (NIS2 Directive)
- ENISA Technical Guidelines for Security Measures
- NIST Cybersecurity Framework 2.0

## About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let’s start a discussion together

251218 - CS + JG