



WHITE PAPER

NIS 2: A guide to navigating Europe's confusing yet powerful directive



Introduction: Why managing NIS 2 presents unique challenges

NIS 2 is complex. For example, although it took effect at the European Union (EU) level in January 2023, it's still not in place throughout the EU. That's because individual countries enforce its requirements through national laws, and while some countries have written NIS 2 into law, others haven't.

That doesn't mean organizations can just ignore NIS 2. Failure to comply can lead to heavy fines in countries that have adopted NIS 2 as law. And despite its relative youth as a directive, NIS 2 is poised for major change. Navigating the directive presents both operational and compliance challenges. Organizations can't afford to ignore it, but they also need to be ready to quickly adapt to shifts in NIS 2 requirements.

A key point to understand about NIS 2 is that it is a directive — not a regulation. That sets it apart from the better-known GDPR, or General Data Protection

Regulation. GDPR, as its name suggests, is a regulation applicable uniformly across all EU member states. Nations can't opt out of or decide not to implement GDPR.

That's not the case for NIS 2. Each EU member state must pass the directive into law separately before it applies in that nation. As of March 2026, transposition across the EU remained uneven. France, Ireland, Luxembourg, Netherlands and Spain had not yet fully completed transposition, with Spain the only country that had not yet submitted a draft law to parliament.

Current NIS 2 vs. proposed amendments

Although it is in flux in much of Europe, NIS 2 is unlikely to remain static. In January 2026, the European Commission (EC) proposed changes to the EU Cybersecurity Act, which, if adopted, would lead to changes in NIS 2. With the proposed changes, offered as formal amendments to the directive, the EC seeks to strengthen NIS 2 as well as to speed transposition in member countries.

Even before full adoption across Europe, NIS 2 may undergo significant changes. Organizations would have to adapt their NIS 2 strategies as a result. However, the proposed changes may simplify compliance for many organizations.

Waiting for European harmony on NIS 2 is not an option

As of early 2026, 21 of 27 EU Member States had written NIS 2 into national law, despite the EU's deadline for transposing the law having passed in October 2024.¹ Requirements are not uniform: Obligations, supervisory expectations and enforcement readiness vary by country.² And the picture gets even more confusing: Some non-EU countries, including Serbia, North Macedonia and Albania, have adopted or are developing NIS 2-aligned cybersecurity laws. Every EU state except Spain that hasn't transposed the law has a pending draft law.³ But if and when they'll pass, and what they'll look like, is still unclear.

NIS 2, which replaced a predecessor directive, NIS D, has reshaped cybersecurity expectations across the EU by widening scope, tightening governance and accelerating incident reporting.

The directive will likely undergo significant change as the EC seeks to implement proposed changes to the EU Cybersecurity Act and, by extension, to NIS 2.⁴ Fortunately for organizations, those amendments could lead to a simpler pathway to compliance, especially for multicountry entities.

So, what can businesses and other organizations do to avoid trouble in such a swirl of confusion? The short answer is act now. Waiting for full harmonization of NIS 2 across the EU and beyond is not a sound strategy. Some countries that have transposed the law are already enforcing it, and penalties can be severe. Plus, the operational impact of noncompliance can be worse than the fine itself, including binding remediation orders, heightened government supervision and potential restrictions on operating activities in high-impact scenarios.

The EC has proposed targeted amendments that, if adopted, could materially affect how NIS 2 is interpreted and applied across the EU.



¹ European Cyber Security Organisation (ECSO), NIS 2 Directive Transposition Tracker, updated 2026, accessed March 3, 2026, <https://ecs-org.eu/activities/nis2-directive-transposition-tracker>.

² Ibid.

³ Cullen International, How are EU member states transposing NIS 2?, March 9, 2026, accessed March 3, 2026, <https://www.cullen-international.com/news/2026/03/How-are-EU-member-states-transposing-NIS2-.html>.

⁴ European Commission, Proposal for a Directive as Regards Simplification Measures and Alignment with the Cybersecurity Act, January 20, 2026, accessed March 3, 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act>.

Why NIS 2 is chaotic for regulated organizations

NIS 2 sets minimum compliance requirements but allows local variations across EU nations. That creates challenges for businesses operating across borders, and complexity is likely to increase. As transposition advances, organizations will face a shifting landscape of national registration rules, reporting portals, competent authorities and supervisory practices.

Compliance programs built solely around the directive's general text may fail to meet country-specific legal requirements. An organization might be compliant in one country and noncompliant

in another due to differences in registration deadlines, reporting mechanics, audit expectations or the interpretation of scope:

- Where national laws are in force, enforcement risk is real now.
- Where national laws are not yet in force, planning risk is high because requirements can change rapidly once adopted.
- For multicountry businesses, both risks apply at the same time.
- The EC is proposing changes to the general directive, which could shift everything.

Why regulators are tightening frameworks

The EC isn't proposing changes just to increase complexity. A rapidly evolving threat landscape has led Commission experts to reconsider NIS 2's requirements despite the fact that the directive isn't even two years old. The changes proposed in January 2026 provide a response to the increasing severity of threats.

Several recent incidents illustrate why the EC developed NIS 2 and introduced formal amendments in January 2026 to strengthen it:

Satellite communications disruption with downstream infrastructure impact. On February 24, 2022, a cyberattack disrupted broadband satellite services via Viasat's KA-SAT network. Public case analyses describe effects across Ukraine and Europe, with reported disruption to remote communications for thousands of wind turbines in Germany.⁵

Water infrastructure attack leaves Danish homes without water. In late 2025, an incident affecting a waterworks near Copenhagen resulted in water service disruption for hundreds of homes.⁶

Attempts and disruptions targeting hospitals and water systems in Eastern Europe. Attackers in 2025 targeted hospitals and city water supply systems in Poland in another example of why public services and critical operators face pressure to secure their operations.⁷

The common thread in all those attacks is operational disruption, not just data loss. Preventing operational disruption is a primary driver of the EC's proposals to strengthen NIS 2 requirements as well as of proposed revisions to a complementary piece of legislation, the EU Cybersecurity Act.

⁵ CyberPeace Institute, Case Study: Viasat Attack, CyberConflicts — Law & Policy, June 2022, accessed March 3, 2026, <https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat>.

⁶ Denmark Blames Russia for Cyberattacks on Water Utility That Left Houses Without Water, The Toronto Star, January 22, 2026, accessed March 3, 2026, https://www.thestar.com/news/world/europe/denmark-blames-russia-for-cyberattacks-on-water-utility-that-left-houses-without-water/article_eba3efbe-9fad-5754-84ff-101e9a79fbba.html.

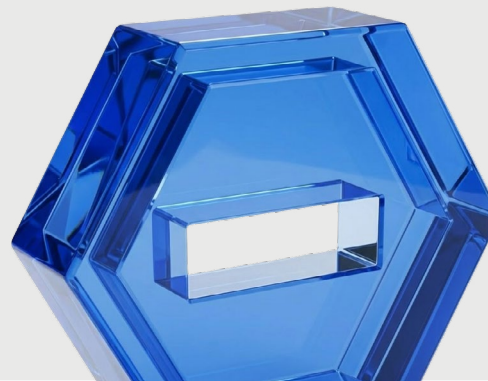
⁷ Industrial Cyber, Poland Faces Record Wave of Russian Cyber Sabotage, Sets €1 Billion Defense Budget, September 17, 2025, accessed March 3, 2026, <https://industrialcyber.co/critical-infrastructure/poland-faces-record-wave-of-russian-cyber-sabotage-sets-e1-billion-defense-budget/>.

NIS 2 penalties: Noncompliance is not an option

Although NIS 2 provides some guidance and limits, since NIS 2 is a directive and not a regulation, nations inside and outside the EU can choose to employ their own enforcement measures that go beyond monetary penalties.

This is important because, for many organizations, the largest impacts arise not from fines but from operational consequences. They come from other factors, including forced remediation work mandated country by country, as well as from the usual significant consequences of security breaches, such as disrupted operations, reputational impact, negative procurement consequences and leadership liability exposure.

Individual EU nations determine how to penalize organizations that don't comply with the NIS 2 directive.



EU-level fine ceilings and broader consequences

NIS 2 defines the overall EU framework for Essential and Important entities, while national authorities identify which organizations fall within scope under local implementation.



Essential entities (including organizations in fields such as energy, transport, health and financial services):

Up to at least €10 million or up to at least 2% of global annual turnover, whichever is higher.



Important entities (including organizations involved in fields such as manufacturing, food, chemicals and courier services):

Up to at least €7 million or up to at least 1.4% of global annual turnover, whichever is higher.

But that's not where the potential financial penalties for noncompliance end. Individual national authorities can also apply measures such as orders to remedy deficiencies, increased supervisory scrutiny and, in some implementations, restrictions that affect an entity's ability to operate or provide services.

Some countries are actively punishing noncompliance

In fact, the most useful way to understand risk is to look at specific national law examples. They reveal how “theoretical” penalties translate into real enforcement. They also demonstrate how enforcement varies from one country to another.



Germany: NIS 2 fine ceilings and enforcement posture are aligned to EU thresholds

Germany's NIS 2 implementation framework reflects the directive's fine ceilings, including up to €10 million or 2% of annual global turnover for Essential entities and up to €7 million or 1.4% for Important entities.

The financial risk can be material, but the practical risk is that failure to implement risk management controls or failure to report incidents can escalate into intensified supervision and remediation actions, which can lead to organizations spending resources on fixing compliance problems rather than focusing on other areas of their operations.⁸



Belgium: Failure to complete mandatory registration is a potential red flag

Belgium's NIS 2 law includes mandatory registration on fixed deadlines tied to the law's entry into force. Entities in certain digital sectors had to register by mid-December 2024, while all other in-scope entities had until mid-March 2025.⁹ It also outlines enforcement mechanisms available to the competent authority, including investigations, binding measures and administrative fines. Belgium holds to the same fine ceilings as Germany, in line with the directive's thresholds.

However, registration failure in Belgium can become a fast path into enforcement attention. It is also a common trigger for procurement and customer trust issues because registration is increasingly treated as a proxy signal for governance maturity.

⁸ Morrison & Foerster, Flipping the NIS 2 Switch: What Germany's Implementation Means for Regulated Entities, December 8, 2025, accessed March 3, 2026, <https://www.mofo.com/resources/insights/251208-flipping-the-nis2-switch-what-germanys-implementation>.

⁹ Centre for Cybersecurity Belgium (CCB), The NIS 2 law, Safeonweb@Work, accessed March 3, 2026, <https://atwork.safeonweb.be/nis2>.



Italy: Financial penalties can come with leadership-level consequences

Italy's NIS 2 implementation specifies administrative fines that reach the directive-level ceilings for both essential and important entities, and it also includes measures that can affect leadership roles. Italian NIS 2 law includes the possibility of temporary disqualification from management roles for individuals responsible for noncompliance.

Italy illustrates a point that many leadership teams underestimate: NIS 2 enforcement can become personal, not just corporate. That reality changes board-level risk calculus, especially for regulated entities that have had historically light cyber oversight.¹⁰



Croatia: Penalties include both entity-level and personal fines

Croatia's Cybersecurity Act imposes fines that track to the directive model's ceilings but also includes separate penalties for individuals responsible for noncompliance.

It's clear from the Croatian example that even where top-line fine ceilings match the NIS 2 ceilings, individual national laws can create additional pressure via personal fines or role-specific accountability structures.¹¹



¹⁰ CoPLA, NIS 2 Directive Regulations and Implementation in Italy, accessed March 3, 2026, <https://copla.com/blog/compliance-regulations/nis2-directive-regulations-and-implementation-in-italy>.

¹¹ OpenKritis, EU NIS-2 Croatia: NIS 2 Compliance and Implementation Overview, accessed March 3, 2026, <https://www.openkritis.de/eu/eu-nis-2-croatia.html>.

Consequences beyond fines: Being “almost compliant” has a hidden cost

No matter where fines are set in a given country, noncompliance can produce other costly knock-on effects:

Regulatory escalation and operational drag

Once a national authority identifies a compliance gap, follow up typically becomes recurring, with evidence requests, timelines, documentation demands and audits required on a grindingly regular schedule. As such, security work becomes a regulatory delivery program closely overseen by a government entity, with more potential penalties possible for noncompliance. The opportunity cost of dealing with regulators rather than focusing on other operations can be substantial.

Procurement and supply chain penalties

As NIS 2 drives supply chain scrutiny, customers

and prime contractors increasingly require proof of controls, incident readiness and sometimes third-party attestations. The Commission's proposals include guidelines to reduce chaotic supplier questionnaires, but these guidelines are not yet part of the directive. As a result, many suppliers face a heavy burden.

Incident cost amplification

A security incident under weak governance becomes more expensive due to delayed detection, slower containment and the resource diversion required to manage both the incident and the reporting obligations. NIS 2's reporting cadence can be demanding, including early warning within 24 hours and incident notification within 72 hours, followed by a final report within one month.

The January 2026 proposal: What could change and why it matters

On January 20, 2026, the Commission published a proposal that would amend NIS 2 as part of a broader package aligned with a proposed revision of the EU Cybersecurity Act.¹² The proposal is a response to challenges observed during NIS 2 implementation, including scope ambiguity, reporting friction and complexity of cross-border supervision.

Key themes in the proposal include:

More harmonization via implementing acts and limits on “gold-plating”

A central idea is to increase universal legal clarity across member states, including through what the EC calls a “maximum harmonization” effect across countries. Under the proposed change, the Commission would adopt acts based on technical and methodological requirements and advise member countries not to impose additional technical or methodological requirements.

Why it matters:

For multicountry organizations, the proposed revision could reduce the cost of maintaining multiple parallel control baselines.

¹² European Commission, Proposal Directive Regards Simplification Measures and Alignment with the Cybersecurity Act, Digital Strategy Library, January 20, 2026, accessed March 3, 2026, <https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act>.

Stronger, more structured ransomware reporting

The proposal introduces more standardized ransomware-related data collection, including details such as attack vector and whether mitigation measures were implemented.

Why it matters:

Even when organizations do not pay ransoms, those who fall victim to ransomware will need better telemetry, incident classification and post-incident documentation discipline.

Stronger cross-border supervision support for ENISA

The proposal gives ENISA, the EU's agency for cybersecurity, a stronger role supporting member states in supervising cross-border entities and facilitating mutual assistance.

Why it matters:

Cross-border companies should expect greater coordination among regulators over time, which will make consistent evidence, standardized reporting and unified security posture metrics more critical than before.

Post-quantum cryptography planning

The proposal includes requirements for EU countries to adopt policies for migration to post-quantum cryptography as part of national cybersecurity strategy.

Why it matters:

Even if the obligation is framed at a national rather than EU level, the downstream effect is that organizations operating under the NIS 2 directive will face increasing expectations to inventory cryptographic assets, plan migrations and prioritize critical use cases.

Certification as a future tool for demonstrating compliance

The Commission's January 2026 proposal points to certification as a potential tool for demonstrating compliance more efficiently across the EU. If adopted, a future cyber-posture certification scheme could give organizations a more consistent way to provide evidence of compliance and benefit from a presumption of conformity under NIS 2. The proposal also frames certification as a tool to help businesses reduce compliance costs and improve coherence across cybersecurity obligations in multiple nations.

That's important because certification could become a practical route to reducing duplicative assessments and supplier questionnaires, especially for organizations operating across multiple EU countries.

How to prepare now, even before certification rules are finalized

Certification-based compliance is not guaranteed, and details will evolve through the legislative process. Still, businesses can prepare without wasting effort:

Build an evidence-first compliance program

Start treating controls as "auditable objects." Policies, risk assessments, control implementation evidence and incident records should be easily retrievable and stored so different versions are readily available as needed.

Unify security operations and data protection

NIS 2 does not prescribe a specific technology architecture. Instead, it requires organizations to implement appropriate and proportionate cybersecurity risk-management measures across areas such as incident handling, business continuity, supply chain security, vulnerability handling, asset management and cryptography where appropriate. Acronis can help

organizations operationalize those requirements by bringing together capabilities such as backup and recovery, endpoint protection, endpoint detection and response (EDR), vulnerability assessment and patch management in a natively integrated platform with centralized visibility and management.

Pre-map controls to likely certification domains

Even without final scheme details, organizations can map their current security programs to risk management areas typically evaluated in EU-aligned frameworks: asset management, access control, vulnerability management, incident response, business continuity, supply chain security and governance.



Table: Current NIS 2 vs. proposed amendments

Note: The right-hand column reflects Commission proposals published in January 2026. As of March 2026, these amendments are not yet adopted and may change during the legislative process.

Topic	Current NIS 2 baseline	January 2026 Commission proposal (not yet adopted)
Transposition model	There is minimum harmonization with latitude among EU countries, enabling local divergence.	The EC wants more convergence, including constraints on some additional national requirements.
Cross-border supervision	One-stop-shop concepts exist for some digital services but multicounty supervision remains complex.	An expanded ENISA support role would help supervise cross-border entities and facilitate coordination.
Ransomware reporting	Organizations must report significant incidents under strict timelines, but ransomware data fields vary by country implementation.	Proposed changes would require more standardized ransomware data collection, including attack vector and mitigation measures, plus potential additional details on ransom demands and payments.
Supply chain burden	Supply chain security is required but often translated into heavy, inconsistent supplier questionnaires in practice.	Commission guidelines propose harmonizing supplier information requests and reducing undue burden.
Scope clarity	Scope and definitions can still be interpreted differently across member states.	Proposal includes clarifications to scope and a more universal definition of where organizations fit.
Technical requirements	Risk management measures are required but with local implementation differences.	The proposal would support further harmonization of technical and methodological requirements across member states.
Certification linkage	Certification is not a standard compliance route under NIS 2 itself.	Proposed changes would introduce a certification-based pathway, enabling proof of compliance through “cyber posture” certification under EU certification programs.
Future readiness	There is no direct directive-level push on post-quantum planning.	Member states would be required to adopt policies supporting migration to post-quantum cryptography, creating downstream expectations.

What businesses should do now: A pragmatic approach

Step 1: Determine scope

Start with a country-by-country scope assessment. Know how each nation defines essential and important entities, and make sure it's clear where to register, and which national supervisory authority is relevant in each country. Differences in national laws remain a major source of confusion for cross-border organizations.

Step 2: Implement controls that survive regulatory scrutiny

A practical starting point is implementing the core controls regulators prioritize: governance, asset inventory, vulnerability management and patching, backup and recovery, endpoint visibility, incident response and reporting readiness.

NIS 2 requires organizations to implement appropriate cybersecurity risk-management measures, including in areas such as incident handling, vulnerability management, business continuity and the use of cryptography where appropriate. In practice, organizations can support those objectives with capabilities such as automation, EDR and patch management.

This is where an integrated approach becomes essential. A natively integrated cyber protection platform that combines secure backup and recovery with anti-ransomware capability, EDR, vulnerability assessment and patch management is the foundation on which organizations should build their NIS 2 compliance strategies.

Step 3: Prepare for reporting under pressure

Reporting timelines can begin quickly. NIS 2's phased reporting framework can be demanding, including early warning within 24 hours and notification within 72 hours. Build incident playbooks that include evidence capture, decision logging and draft notification templates.

Step 4: Treat compliance as a business continuity program, not a checklist

The most painful failures have repercussions far beyond paperwork or even fines. They are preventable disruptions that spread into customer impact, contract risk and reputational damage.



How Acronis supports compliance with NIS 2

CIS Controls mapped with NIS 2	Security function	How Acronis can help
Establish and Maintain Detailed Enterprise Asset Inventory (1.1)	Identify	Acronis can share detailed asset data with your inventory solution through integration. This connection is easily enabled using Acronis CyberApp .
Establish and Maintain a Data Classification Scheme (3.7)	Identify	Acronis DLP classifies data according to labels, and/or applies labels to data.
Log Sensitive Data Access (3.14)	Detect	Acronis DLP can partially map to this control. Logs can be generated by Acronis DLP when data is accessed, including when it is being sent.
Establish and Maintain a Vulnerability Management Process (7.1)	Protect	Acronis RMM manages vulnerability management processes.
Establish and Maintain a Remediation Process (7.2)	Govern	Acronis RMM manages a remediation process.
Perform Automated Vulnerability Scans of Internal Enterprise Assets (7.5)	Identify	Acronis RMM has the ability to perform automated vulnerability scans of internal enterprise assets. e.g., a vulnerability scanning tool.
Remediate Detected Vulnerabilities (7.7)	Respond	Acronis RMM has the ability to coordinate and manage the remediation of detected vulnerabilities. e.g., a process management tool.
Conduct Audit Log Reviews (8.11)	Detect	Acronis EDR / XDR / MDR can conduct audit log reviews. e.g., log analytics and centralization tool. Has the ability to detect anomalies and abnormal events that could indicate a potential threat.
Deploy and Maintain Anti-Malware Software (10.1)	Protect	Acronis EDR / XDR / MDR is an anti-malware software on all enterprise assets.
Configure Automatic Anti-Malware Scanning of Removable Media (10.4)	Detect	Acronis XDR scans removable media for malware automatically. e.g., anti-malware software.
Establish and Maintain a Data Recovery Process (11.1)	Govern	Acronis Cyber Platform is not a process management solution. However, it strengthens and streamlines backup and recovery operations, ensuring greater efficiency and resilience.
Protect Recovery Data (11.3)	Protect	Acronis Backup and Acronis Disaster Recovery can protect recovered data with the same security controls and safeguards applied to the original data.
Establish and Maintain an Isolated Instance of Recovery Data (11.4)	Recover	Acronis Cyber Platform establishes a copy of the recovery data that is isolated (logically, virtually or physically separate, immutable).
Test Data Recovery (11.5)	Recover	Acronis Backup restores data from a sample of in-scope enterprise assets.
Establish and Maintain a Security Awareness Program (14.1)	Govern	Acronis Security Awareness Training (SAT) is capable of managing a security awareness program with the goal of educating the workforce on how to interact with assets and data in a secure manner.
Train Workforce Members on Recognizing and Reporting Security Incidents (14.6)	Protect	Acronis Security Awareness Training educates the workforce members on recognizing and reporting security incidents.
Conduct Role-Specific Security Awareness and Skills Training (14.9)	Protect	Acronis Security Awareness Training can facilitate role-specific security awareness and skills training.
Establish and Maintain Security Incident Thresholds (17.9)	Recover	Acronis EDR / XDR / MDR help maintain incident response readiness by enabling preparation, detection, and rapid response to attacks. For full incident response capabilities, integration with incident management and incident response planning tools is required.

NIS 2 compliance is not only about meeting existing requirements but also building a program that can withstand uneven national implementation, active enforcement in some countries and potential upcoming reforms that could change the nature of compliance.

Organizations that move now gain three primary advantages: reduced enforcement exposure, lower incident impact and a clearer path to adapting as the Commission's proposals progress through the legislative process.

Adopting the right technology platform is critical. Acronis helps organizations strengthen their readiness for NIS 2 compliance by providing an integrated cyber protection platform designed to support core requirements of the directive, including risk management, incident response and business continuity.

Acronis Cyber Platform combines cybersecurity capabilities such as anti-malware, anti-ransomware, EDR, vulnerability assessment and patch management with backup and disaster recovery in a natively integrated platform manageable by a single point of control.

This integrated approach enables organizations to detect threats, mitigate risks and recover quickly from incidents while maintaining operational continuity, all of which are key requirements under NIS 2. By simplifying security operations and providing centralized visibility into systems and vulnerabilities, Acronis helps organizations strengthen their defenses and demonstrate the structured security controls regulators expect from entities subject to NIS 2.

Improve and maintain compliance with NIS 2 and other regulatory obligations in the EU with the Acronis Cyber Platform for businesses and service providers.

Acronis Cyber Platform for Business

Acronis Cyber Platform for MSPs

About Acronis

Acronis is a global cyber protection company delivering the only natively integrated cybersecurity, data protection, and infrastructure management platform for managed service providers and IT departments. Acronis solutions are designed to identify, protect, detect, respond, recover and govern IT deployments, ensuring data integrity and business continuity.

A Swiss company founded in Singapore in 2003, Acronis has 15 offices worldwide and employees in 60+ countries. Acronis Cyber Platform is available in 26 languages in 150 countries and is used by over 21,000 service providers to protect over 750,000 businesses.