NIS2 compliance beyond the April 2026 deadline

BY ELEANOR BARLOW · MAY 12, 2026

The April NIS2 compliance deadline has come and gone, but where does your company stand?

The European Union, via the NIS2 Directive, sets the overall framework and timelines. Member States are responsible for transposing these into national law.

The deadline for Member States to transpose the NIS2 Directive into their national law was October 17, 2024. The April 18 deadline is for Member States to identify and list the entities.

The expectation is that listed entities will need to demonstrate compliance with the new national regulations.

A quick recap: what is NIS2?

The NIS2 Directive stands for Network and Information Security Directive 2 and is the EU-wide legislation on cybersecurity.

NIS2 was translated into national law and became effective as of 18 October 2024, to provide legal measures to boost the overall level of cybersecurity across the European Union and improve resilience and incident response capabilities and capacities.

Rules were first introduced back in 2016, with NIS1. In 2023, NIS2 was implemented to modernize and expand the scope of the existing legal framework to keep up with increased digitalization and the evolving threat landscape.

> **"The NIS2 Directive has driven improvements in vulnerability management across Europe, shifting more organizations from a reactive posture toward a more proactive security posture."**
>
> **Ed Parsons, Chief Operations Officer, Intigriti**

For expert insights regarding the progress European organizations have made toward NIS2 compliance, view this video.

Are you impacted? Which entities apply?

NIS2 outlines two categories for entities in scope: 'important' and 'essential'. These include sectors such as healthcare, energy, transport, banking, public administration, and digital providers. The directive sets out the minimum requirements, but national NIS2 laws determine which specific requirements these types of entities must meet. As a rule, large and medium entities are in scope. But smaller companies are not excluded, and EU members can make exceptions.

If you're new to NIS2, start by familiarizing yourself with our full guide for in-scope entities. This covers the fundamentals you'll need before diving into April requirements.

What was expected by the April Deadline?

Companies across Europe must have met their NIS2 requirements by April 18th. Although specific regulations will vary by member state, national authorities are providing guidance; in Belgium, for example, the Centre for Cybersecurity has outlined three key actions for entities to complete before the deadline.

1. **CyberFundamentals (CyFun®):** Obtain, or be actively in the process of obtaining, at least a Basic or Important verification, or hold a signed agreement with an accredited assessment body. **It is important to clarify** that important entities do not have any specific formalities to complete. The deadline for achieving a CyFun label is for essential entities.

2. **ISO/IEC 27001:** Submit the certification scope, Statement of Applicability (SoA), and the most recent internal audit report, with full certification to be completed by April 2027.

3. **Direct inspection:** Provide a self-assessment **and** relevant supporting documentation and formally request an inspection (noting that this pathway may lead directly to supervisory measures).

What's the risk of noncompliance or missed deadlines?

Companies that do not meet NIS2 requirements and/or deadlines face penalties of up to 10,000,000 euros, 2% of global revenue, dismissal, and/or disqualification for management.

The shift from preparation to demonstration

Now that the April 2026 deadline is behind us, the question has shifted from 'Are you preparing?' to 'Are you fully compliant, and can you prove it?' For many, the answer isn't as clear-cut as it should be.

Below, we break down the key requirements and next steps to support your organization's NIS2 compliance journey.

NIS2 entity requirements

There are four main requirements categories outlined on the NIS2 Directive website.

> **"The regulation put more emphasis on asset discovery and the need for a deeper understanding of the full attack surface, including previously unknown or unmanaged systems related to shadow IT."**
>
> **Ed Parsons**

You can view all the details here, but the requirements boil down to these four critical actions.

- **Risk Management:** Including incident management, stronger supply chain security, enhanced network security, better access control, and encryption.

- **Corporate Accountability:** Corporate management to oversee, approve, and be trained on the entity's cybersecurity measures and to address cyber risks.
- **Reporting Obligations:** Processes in place for prompt reporting of security incidents, meeting specific deadlines, such as a 24-hour “early warning” to authorities.
- **Business Continuity**: Plans set out to ensure business continuity in the case of a major cyber incident, considering system recovery, emergency procedures, and crisis response.

Your top 10 tasks

As well as complying with these four elements, 10 security measures were also put in place. The following list comes directly from the NIS2 Directive.

1. Risk assessments and security policies for information systems.
2. Policies and procedures for evaluating the effectiveness of security measures.
3. Policies and procedures for the use of cryptography and, when relevant, encryption.
4. A plan for handling security incidents.
5. Security around the procurement of systems and the development and operation of systems. This means having policies for handling and reporting vulnerabilities.
6. Cybersecurity training and practice for basic computer hygiene.
7. Security procedures for employees with access to sensitive or important data, including policies for data access. Affected organizations must also have an overview of all relevant assets and ensure that they are properly utilized and handled.
8. A plan for managing business operations during and after a security incident. This means that backups must be up to date. There must also be a plan for ensuring access to IT systems and their operating functions during and after a security incident.
9. The use of multi-factor authentication, continuous authentication solutions, voice, video, and text encryption, and encrypted internal emergency communication, when appropriate.
10. Security around supply chains and the relationship between the company and direct supplier. Companies must choose security measures that fit the vulnerabilities of each direct supplier. And then companies must assess the overall security level for all suppliers.

How can crowdsourced security support your NIS2 journey?

Determine if you fall under the scope of NIS2, evaluate your security measures to meet NIS2 compliance, and highlight which security measures to incorporate to enhance your incident reporting, with crowdsourced security.

Bug bounty platforms have established processes for handling vulnerability reports and have procedures in place for responding to vulnerabilities quickly and efficiently. In relation to security testing, the NIS2

guidance supports bug bounty programs as a testing approach.

> **"Organizations are accelerating vulnerability discovery and Security Testing by engaging with crowdsourced security communities and ethical hackers, enabling them to identify weaknesses before they can be exploited."**
>
> **Ed Parsons**

There are several areas where crowdsourced security testing can increase compliance with NIS2.

First, all EU member states must ensure that anyone is able to report a vulnerability to the Computer Security Incident Response Team (CSIRT). Having your own Vulnerability Disclosure Program (VDP) or Bug Bounty (BB) Program increases the chance of vulnerabilities being reported to you as a company, rather than to the government. It also provides an easy way for these parties to assess the security maturity of suppliers.

The easiest way to do this is with a VDP.

Second, under the Belgian NIS2 national law, having a coordinated VDP is an explicit requirement for in-scope entities. Belgium has added this as an 11th requirement to the list, and other EU member states are expected to follow.

Third, regarding asset management, NIS2-compliance expects in-scope organizations to be able to showcase the status of all IT assets. This includes being able to identify all hardware and software in use and then being able to assess the associated risk levels. Crowdsourced security can help by providing continuous, real-world discovery of both known and unknown assets through the eyes of ethical hackers. As researchers probe your attack surface, they often uncover forgotten, misconfigured, or shadow IT assets, such as legacy servers or orphaned subdomains, that internal inventories typically miss. This ongoing external perspective helps organizations maintain an accurate, up-to-date asset inventory and better assess the true risk posture of their entire digital footprint, directly supporting the visibility and accountability NIS2 demands.

Fourth, in terms of risk identification, crowdsourced security provides continuous and proactive human-driven risk identification. This addresses the directive all-hazards re-evaluations regarding risk management and vulnerability handling. As stated in The NIS2 Directive, Updates, Compliance, the 'directive mandates an "all-hazards" approach, meaning that entities must be prepared to address a wide range of threats, from cyberattacks to physical disruptions, ensuring comprehensive protection and resilience in their operations.'

Prepare for next steps with Intigriti

Many companies view compliance as a tick-box exercise. What it really demands is a thorough analysis and evaluation of your organization.

The NIS2 Directive promotes a culture of transparency and collaboration. Intigriti embodies this by fostering open communication between organizations and the security research community.

We can help you determine if you fall under the scope of NIS2, evaluate your security measures to meet NIS2 compliance, and highlight which security measures to incorporate to enhance your incident reporting.

Interested in learning more? Take a look at the guidance from ENISA for technical guidance.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.