eBook

NIS2

Everything You Need to Know to Stay Compliant

Balbix®

The NIS2 Directive establishes a new standard for enhancing cybersecurity throughout the European Union, mandating that organizations implement advanced tools and platforms to comply with its stipulations or risk significant penalties. Balbix provides a robust array of capabilities that enables organizations in critical industries to not only meet the directive's requirements but also bolster their overall cybersecurity posture.

For international companies operating in Europe, particularly in key sectors, the NIS2 Directive (Network and Information Systems) marks a significant update to cybersecurity regulations. This directive is pivotal in strengthening cybersecurity across the European Union, so compliance is not optional. The stakes are high: companies that fail to adhere to these new cybersecurity requirements face substantial penalties. It's a critical moment for European businesses, as the EU takes decisive action to enhance its digital security landscape. Ensuring compliance with the NIS2 Directive is not just about avoiding fines; it's about contributing to a more secure digital environment across the continent.

NIS vs. NIS2: More Consistency, Stronger Controls

The difference between NIS, with which you are no doubt familiar, and NIS2 is that the option to tailor adherence to directive requirements was eliminated since there was too much flexibility under the original NIS, which led to vulnerabilities. In addition, NIS2 applies consistently across the EU and specifies the rules everyone must follow. These new requirements and obligations fall into four overarching areas: risk management, corporate accountability, reporting obligations, and business continuity. They demand that entities adopt adequate technical, operational and organizational measures to manage network and information systems risks.

NIS 1		NIS 2
30 types of entities	**Expanded Sectoral Scope**	• 67 types of entities • Includes SMEs in some cases • Includes supply chain
Risk-based with no obligation of prior compliance to the directive	**Strengthened Security Requirements**	• Ex-ante audits • 24 hour incident notification • Detailed report in 72 hours • Responsibility matrix across supply chain • Risk management TOMs
Sanctions determined by member states	**Expanded, Standardized Sanctions**	• Standard fines • Suspension of certifications • Criminal sanctions • Temporary bans on management positions
	Enhanced EU Cyber Risk Cooperation	• Creation of the Cyber Crisis Liason Organization Network — **EU-CyCLONe**

While NIS2 can be complex, Balbix can help address NIS2 Directive's requirements and mitigate the risk of non-compliance.

NIS2 & DORA: Overlap or Complement?

It is important to note that, when you make cyber security investments, consider **NIS2** and **DORA** together since there is quite a bit of overlap between the two directives. Both DORA and NIS2 :

- Emphasize the importance of operational resilience and ICT risk management.
- Mandate timely reporting of significant cyber incidents to relevant national or EU authorities.
- Highlight the need for stringent oversight and management of third-party and ICT service providers.
- Call for regular testing and audits to assess the effectiveness of cybersecurity measures and operational resilience frameworks.

DORA and NIS2 also serve complementary objectives. DORA is more focused on the financial sector's operational resilience, addressing the need for a financial system that remains stable and functional despite ICT-related disruptions. NIS2, on the other hand, aims at a broader enhancement of cybersecurity practices across key sectors vital to the economy and society, recognizing the interconnected risks that span across different industries.

Together, DORA and NIS2 represent a comprehensive approach to improving the cybersecurity posture and operational resilience of critical sectors in the EU, ensuring that both financial and non-financial entities are equipped to handle and recover from cyber threats and incidents.

A NIS2 Compliance Checklist

This checklist provides a starting point for organizations aiming to comply with the NIS2 directive, emphasizing incident management, risk assessment, resilience and governance in line with the directive's requirements.

Incident Handling and Reporting

- **Incident Detection and Reporting Mechanism:** Organizations must have effective mechanisms to detect and report significant cybersecurity incidents to the relevant authorities within the time frames specified by NIS2.
- I**mpact Assessment of Incidents:** Organizations must evaluate the impact of cybersecurity incidents on the continuity of essential services, guiding reporting and response efforts.
- **Provisional Reporting:** In cases where complete information about an incident is not available, organizations must provide provisional reports and follow up with detailed reports as more information becomes available.

Risk Management and Resilience

- **Comprehensive Risk Analysis:** Organizations must perform thorough risk assessments to identify and understand the cybersecurity risks they face, including those from supply chains and third-party services.
- **Resilience Building and Testing:** Organizations must establish and test resilience measures to ensure continuity of services in the event of a cybersecurity incident.
- **Supply Chain and Third-party Service Provider Security:** Organizations need to ensure that their supply chains and third-party service providers adhere to the same cybersecurity standards as required for NIS2 compliance.

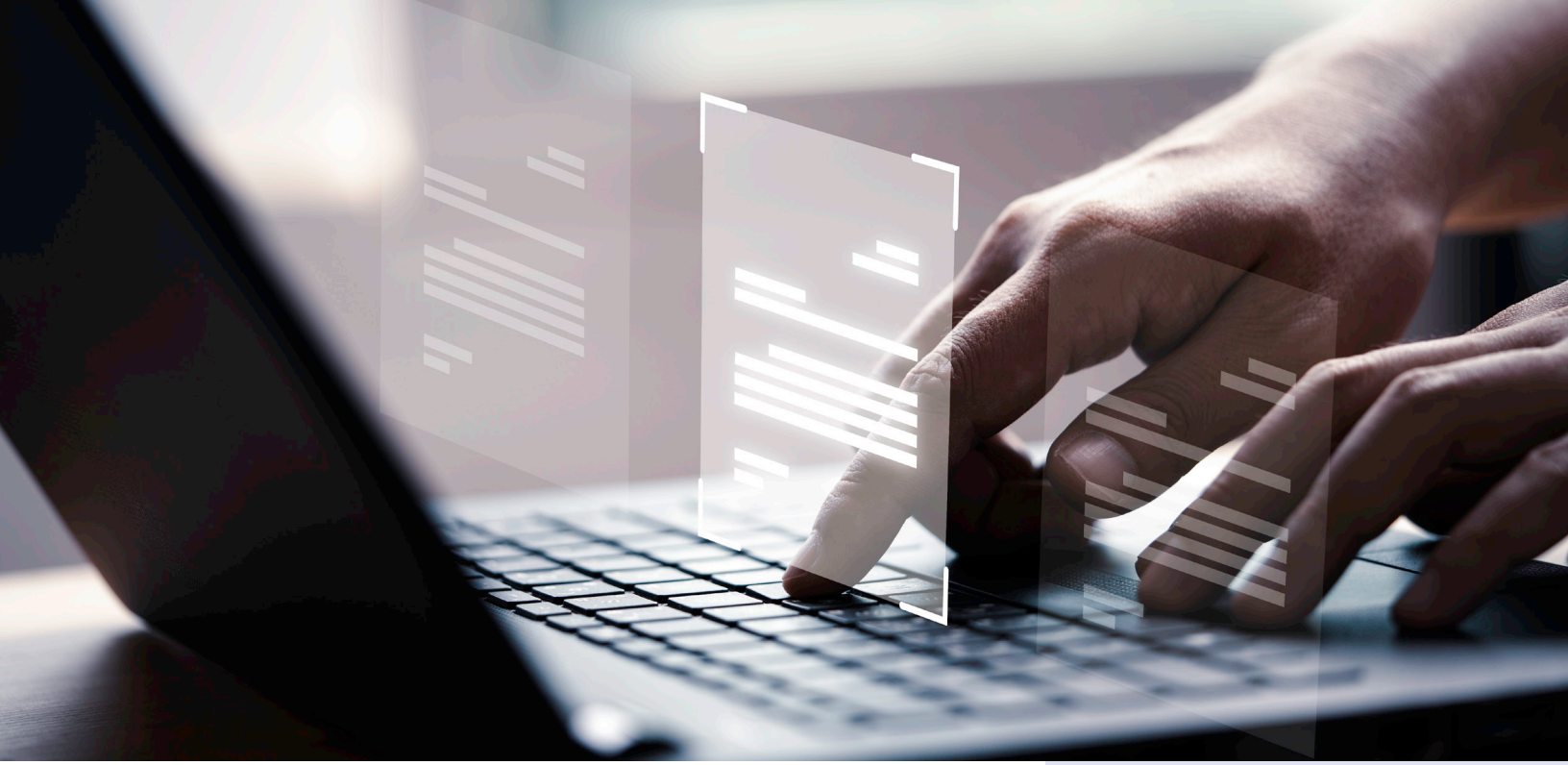
Governance and Compliance

- **Cybersecurity Governance Framework:** Establish a governance framework that includes policies, procedures, and measures to manage cybersecurity risks and comply with NIS2 requirements.
- **Integration with Business Processes:** Cybersecurity management practices should be integrated into the core business processes to ensure continuous compliance and resilience against cyber threats.

How Balbix Helps

By automating the identification, assessment, and mitigation of cyber risks, Balbix reduces the manual effort required, allowing organizations to focus on strategic initiatives rather than compliance alone. However, here's how Balbix can help with addressing the NIS2 Directive:

Balbix Capability	How It Addresses NIS2
Automated Risk Assessment & Governance	**ARTICLE 20** Balbix automates the risk assessment process, leveraging AI to provide real-time insights into an organization's cyber risk (i.e. risk of exposure or potential loss resulting from a cyber attack or data breach). This capability aligns with Article 20 of the NIS2 Directive, which mandates that entities' management bodies oversee and approve cybersecurity measures. Balbix identifies risks and offers actionable insights, enabling decision-makers to understand their cyber risk exposure and approve effective risk mitigation strategies.
Cybersecurity Risk Management Measures	**ARTICLE 21** Balbix helps you manage cybersecurity risks. This includes risk-based vulnerability management, comprehensive asset and software inventory, and cyber risk quantification. Balbix ensures that companies have comprehensive cybersecurity risk management measures in place, which is a core requirement for companies under the NIS2 Directive.
Reporting Obligations	**ARTICLE 23** The directive's emphasis on timely reporting is met with Balbix's capability to identify, prioritize for remediation, and report on critical assets at risk. Balbix provides real-time visibility into critical vulnerabilities and automated remediation, facilitating compliance with the reporting obligations outlined in Article 23.
Supply Chain Risk Assessments	**ARTICLE 22** Balbix's visibility into third-party vulnerabilities and risks supports the directive's requirements for critical supply chain risk assessments in Article 22. By providing deep insights into the cybersecurity practices of suppliers and service providers, Balbix enables organizations to assess and mitigate supply chain risks effectively.
Compliance with Cybersecurity Certification Schemes	**ARTICLE 24** As the NIS2 Directive encourages using certified information and communication technology (ICT) products and services in Article 24, Balbix aids organizations in assessing their ICT infrastructure against recognized cybersecurity standards. This support ensures that entities can demonstrate compliance with certification schemes, thereby adhering to the directive's requirements.



Essential vs. Important Entities

The NIS2 Directive categorizes entities as "Essential" and "Important" to ensure the resilience and security of network and information systems. Essential Entities operate within critical sectors such as healthcare, energy, transportation, banking, digital infrastructure, water supply and distribution. Disruptions of these Entities could have a major impact on national security, economic stability, or public safety.

Important Entities, while still significant, operate in sectors that are less critical but where an incident could still pose considerable risks to the public interest or societal functions.

Essential Entities must comply with NIS2, while Important Entities are subject to ex-post supervision, where penalties will only be levied if authorities receive evidence of non-compliance. Penalties for non-compliance are much higher for Essential Entities than for “important” ones.

The High Cost of Non-Compliance

The consequences of non-compliance with the NIS2 Directive are severe, with fines reaching up to €10 million or 2% of global annual revenue for Essential Entities and €7 million or 1.4% for Important Entities. NIS2 has teeth just like GDPR.

As the NIS2 Directive sets a new benchmark for cybersecurity in the EU, organizations must adopt sophisticated tools and platforms to meet its requirements. Balbix emerges as a powerful ally in this endeavor, offering a comprehensive suite of features that align with the directive's mandates. Through AI, automation, real-time insights and a holistic approach to cyber risk management, Balbix not only ensures compliance with the NIS2 Directive but also enhances an organization's overall cyber resilience. In the face of increasing cyber threats, the combination of Balbix and the NIS2 Directive represents a forward-thinking approach to cybersecurity. This approach prioritizes resilience, compliance, and the proactive management of cyber risks.

Request a demo to learn more about how Balbix enables organizations to meet NIS2 directive requirements

Balbix®