Mandiant

Google Cloud
Security

From Reactive to Proactive

Transforming Your Strategic Roadmap for NIS2 Compliance

Executive Summary

The Network and Information Security 2 (NIS2) Directive elevates cybersecurity requirements for critical sectors in the European Union (EU), mandating a proactive approach to risk management and security. Mandiant, part of Google Cloud, offers a Security Program Assessment (SPA) that provides a proven framework for organizations to assess their cybersecurity posture, identify vulnerabilities, and implement a roadmap for continuous improvement.

This white paper delves into how the Mandiant SPA aligns with NIS2's core tenets, empowering organizations to not only achieve compliance, but also enhance their overall security resilience, mitigate cyber risks, and safeguard critical assets in an evolving threat landscape.

Authors: Meet Patel, Camille Felx Leduc, Georges Badro, Nathan Martz, Chris Sistrunk

Introduction

What is NIS2?

The NIS2 Directive, adopted on December 27, 2022, marks a significant evolution in the EU's approach to cybersecurity. Building upon the foundations laid by the original NIS Directive in 2016, NIS2 addresses the rapidly evolving threat landscape, where cyber-attacks have become more sophisticated, targeted, and impactful, establishing a more stringent and comprehensive cybersecurity framework for critical sectors across the EU. By raising the bar for cybersecurity preparedness and response, NIS2 aims to bolster the resilience of critical infrastructure and services, safeguarding the digital economy and society.

The directive acknowledges that cyber threats do not respect borders and that a coordinated, EU-wide approach is essential for effective mitigation. While the original directive focused on essential services in sectors like energy, transportation, and healthcare, NIS2 broadens its scope to include a wider array of industries deemed "essential" or "important," including digital infrastructure, public administration, and more. This expansion, particularly into sectors like ICT service management and digital providers, underscores the increasing interconnectedness of critical infrastructure and the need for a holistic cybersecurity strategy that encompasses risk assessment, threat intelligence sharing, and coordinated incident response across sectors.

Key Objectives

How We Can Help

The Mandiant SPA Framework is an advanced, proprietary, and proven framework for evaluating cyber posture that was developed to provide a highly detailed understanding of the maturity of any cyber program.

SPA		NIS2 Coverage	
SPA Function	**Themes Covered**	**New Requirements**	**Minimum Requirements**
Security Governance	• Security Governance and Strategy • Security Awareness Training & Compliance Requirements	• Reporting Obligations • Corporate Accountability	• Security Policies • Security Measure Effectiveness • Cybersecurity Training & Hygiene
Security Risk Management	• Asset and Vulnerability Management • Data Protection • Risk Management • Third-Party/Vendor Management • Business Continuity and Disaster Recovery	• Risk Management • Business Continuity	• Asset Management • Business Continuity Plan • Supply Chain Security Management • Secure System procurement & Development
Security Architecture Review	• Identity and Access Management • Network Architecture and Security • Endpoint Security • Cloud Architecture and Security • Secure Software Development Lifecycle (SDLC)	• Risk Management • Business Continuity	• Cryptography & Encryption • Access Control & Management • Advanced Authentication & Encryption
Cyber Defense	• Threat Detection, Automation, and Orchestration • Incident Response and Crisis Management • Cyber Threat Intelligence	• Reporting Obligations	• Incident Handling

How Is It Different From NIS?

- **Expanded Scope:** According to the European Commission's impact assessment accompanying the proposal for the NIS2 Directive: “The new rules would apply to around 160,000 entities, which is about ten times more than under the current NIS Directive."
- **Additional Requirements:** Businesses must implement a comprehensive risk management framework to address cybersecurity concerns related to incident handling, supply chain security, network protection, access controls, and encryption.
- **Stronger Supervisory Control Measures and Sanctions:** NIS2 strengthens cybersecurity through stricter supervision, including audits and incident reporting, and promotes information sharing. Non-compliance faces hefty fines of up to €10 million or 2% of turnover, and potential operational bans, emphasizing adherence to regulations.
- **Increased Focus on Management Bodies:** NIS2 introduces a paradigm shift in the EU's approach to cybersecurity by holding company leaders accountable for cybersecurity. This unprecedented level of accountability requires them to oversee plans, undergo training, and face potential penalties, including removal from leadership roles, in the event of breaches.
- **Enhanced Cooperation and Information Sharing:** Enhanced cooperation and information sharing among EU member states is called for, to improve overall cybersecurity through a framework for regular exchange and coordination, including sharing threat intelligence, vulnerabilities, incidents, and best practices.

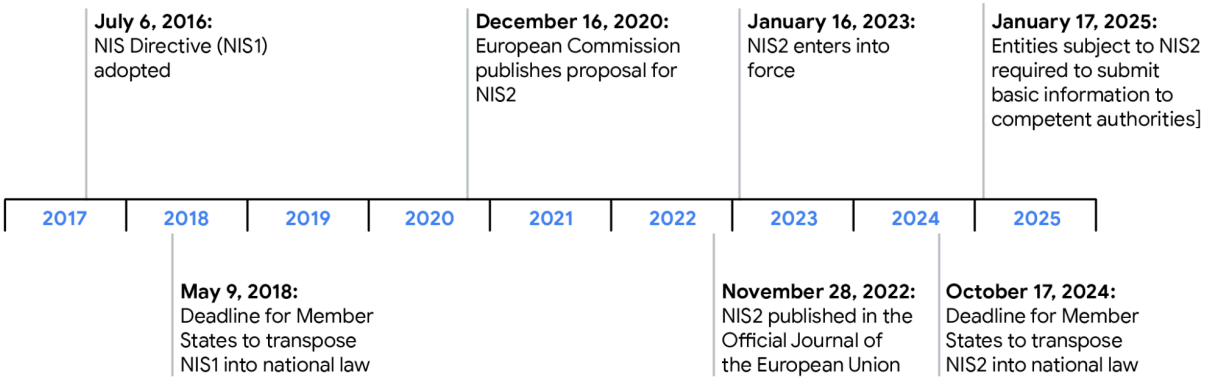
Key Provisions

1. **Risk Management:** The directive mandates organizations to adopt a risk-based approach to cybersecurity and to implement proportional measures based on identified risk. Emphasis is placed on conducting ongoing risk assessments and updating security measures.
2. **Incident Reporting/Reporting Obligations:** The directive mandates that essential and important entities report any incident significantly impacting their services to their Computer Security Incident Response Team (CSIRT) or to their competent national authority without undue delay:
    - **Early warning:** An early warning must be submitted within 24 hours of becoming aware of the incident, indicating if it is suspected to be unlawful, malicious, or have a cross-border impact.
    - **Incident notification:** A more detailed incident notification must be submitted within 72 hours, including an initial assessment of the incident’s severity, impact, and indicators of compromise.
    - **Final report:** A final report is due one month after the initial notification. This report details the incident, its impact, the likely cause, mitigation measures, and

any cross-border effects. If the incident is ongoing, a progress report is submitted, with the final report due one month after the incident is handled.

3. **Supply Chain Security:** NIS2 mandates that organizations assess and manage the cybersecurity risks within their supply chain. This involves evaluating the security practices of supplier and service providers to ensure they meet the directive's standards, fostering transparency and accountability throughout the supply chain.
4. **Cooperation and Information Sharing:** The directive encourages cooperation and information sharing among EU member states, competent authorities, and relevant stakeholders. By fostering collaboration and exchanging threat intelligence, NIS2 aims to enhance overall cybersecurity resilience across the EU.
5. **Supervisory Measures:** The directive introduces stricter supervisory measures and enforcement mechanisms, including harsher penalties for non-compliance. Sanctions are harmonized across EU member states to ensure consistent enforcement, holding management bodies accountable for their organizations.
6. **Management Bodies Accountability:** The NIS2 Directive holds management bodies directly accountable for cybersecurity risk management. They must approve and oversee the implementation of security measures, ensuring adequate resources are allocated and incident response plans are effective. Management is also expected to undergo cybersecurity training and foster a security-conscious culture.
   Non-compliance can result in personal liability for individual members, including fines and temporary bans from managerial positions.
7. **Baseline Security Measures:** NIS2 establishes a set of minimum security measures that organizations must implement.
   - https://eur-lex.europa.eu/eli/dir/2022/2555
   - https://nis2directive.eu/nis2-requirements/

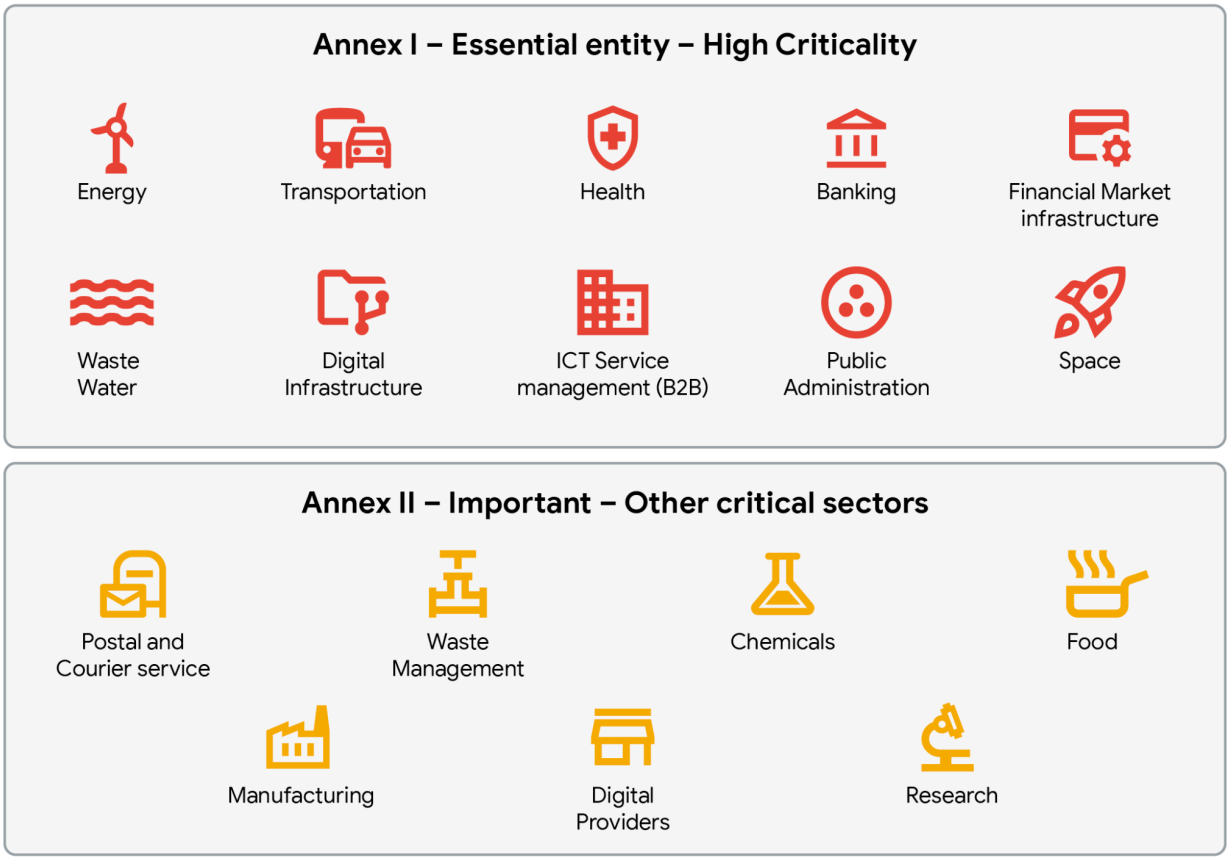
When Does It Go Into Effect?



The Expanded Scope

NIS2 broadens the reach of its regulations to encompass a broader spectrum of businesses, aiming for more uniform application across member states. This expansion attempts to create a level playing field, irrespective of enterprise size, and safeguards consumers from unfair commercial practices.

- **Larger Enterprises:** More than €50 M annual revenue, 250 + employees
- **Medium Enterprise:** More than €10 M annual revenue, 50+ employees
- **Member State Selected:** Any size, selected based on risk profile



Cybersecurity Risk Management Measures

Article 21 of the NIS2 Directive includes the following key language to describe the efforts that organizations are to take related to managing cybersecurity risk:

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(a) policies on risk analysis and information system security;

(b) incident handling;

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;

(g) basic cyber hygiene practices and cybersecurity training;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, access control policies and asset management;

(j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Challenges In Implementing

Implementing a robust cybersecurity framework poses several challenges. The vast scope and complexity of modern IT environments make it difficult to identify and protect all potential vulnerabilities. Incident response protocols must be carefully designed and tested to ensure effective handling of security breaches. Regulatory compliance adds an additional layer of complexity, as organizations must adhere to various laws and standards related to data protection. Moreover, the rapid evolution of technology and the shortage of skilled cybersecurity professionals further exacerbate these challenges, making it difficult for organizations to keep pace with the evolving threat landscape.

Regulatory Repercussions

Fines, temporary or permanent bans, public reprimands, and orders to comply are all potential consequences for non-compliance with NIS2. Essential entities face a maximum fine of at least EUR 10 million or 2% of their total worldwide annual turnover in the preceding financial year, whichever is higher. Important entities face a maximum fine of at least EUR 7 million or 1.4% of their worldwide annual turnover in the preceding financial year. Non-compliant organizations may also be publicly named and shamed, damaging their reputation. Finally, authorities can issue mandatory instructions to rectify non-compliance, with further penalties for failing to do so.

Conclusion

Considering accountability as a fundamental principle, the NIS2 Directive marks a substantial advancement in cybersecurity regulation within the European Union. Its expanded scope, stringent requirements, and emphasis on holding entities responsible reflect the critical need for proactive cybersecurity measures in today's interconnected digital landscape. Organizations that fall under the purview of NIS2 must not only comply with its provisions, but also view it as an opportunity to enhance their overall security posture. The Mandiant Security Program Assessment (SPA) Framework offers a structured and comprehensive approach to aligning with NIS2's core tenets. By leveraging the Mandiant SPA, organizations can effectively assess their cybersecurity maturity, identify vulnerabilities, and develop a strategic roadmap for continuous improvement. This not only furthers compliance, but it also strengthens their resilience against evolving cyber threats, safeguarding critical assets and contributing to a more secure digital landscape across the EU.

In the face of increasingly sophisticated cyberattacks, NIS2 compliance is not merely a “checkbox” exercise; it is a fundamental requirement for organizations entrusted with essential services and critical infrastructure. Mandiant is committed to supporting organizations in their NIS2 compliance journey, providing expert guidance and tailored solutions to navigate the complexities of the directive and achieve lasting cybersecurity resilience.