NIS2 Maturity Accelerator

PREPARE FOR NIS2 COMPLIANCE AND INCREASE CYBERSECURITY RESILIENCE

The Network and Information Security Directive 2 (NIS2) is a European Union (EU) directive aimed at enhancing the cybersecurity resilience of critical infrastructure and essential services across the EU. NIS2 significantly updates the EU's original NIS Directive by expanding its scope, enforcing stricter requirements, and promoting greater harmonization across Member States to address evolving risks.

The European Parliament voted to adopt NIS2 in May 2022 and the Council of the EU approved NIS2 in November 2022. NIS2 entered into force on January 16, 2023, requiring Member States to transpose it into national law by October 17, 2024. The deadline for in-scope entities to register their obligations with the supervisory authorities is either January 17, 2025, or April 17, 2025, depending on the types of services provided.

As part of NIS2, organizations will need to strengthen their governance, risk management measures, and incident reporting processes. This directive represents not only a regulatory obligation but also an opportunity for organizations to build more resilient, secure, and future-proof operations that minimize vulnerabilities and enhance customer trust.

The Trustwave NIS2 Maturity Accelerator provides you with a roadmap to prepare your security programs for NIS2 compliance. Trustwave will provide guidance and remediation planning to help you align with the NIS2 requirements.

Understanding NIS2

NIS2 is a directive established by the EU to enhance the cybersecurity resilience of critical infrastructure, improve risk management practices, and ensure more robust incident reporting across Member States. In general, NIS2 applies to medium- and large-sized public and private entities providing essential services or critical infrastructure within or to the EU. It broadens the scope of the original NIS Directive to include sectors such as energy, healthcare, transportation, digital infrastructure, and public administration.

The National Competent Authorities (NCAs) are empowered to impose substantial penalties on organizations that fail to comply with NIS2. This includes fines of up to EUR 10,000,000 or 2% of total annual worldwide turnover for essential entities, and may also include prohibition from managerial functions, cease and desist orders, and public disclosure of infringements.

NIS2's framework is bult around three key focus areas, each designed to strengthen different aspects of cybersecurity resilience:

1. **Governance:** Focuses on ensuring robust cybersecurity leadership within organizations by establishing clear roles, responsibilities, and strategic oversight at senior levels.
2. **Cybersecurity Risk Management Measures:** Focuses on achieving risk management outcomes using appropriate technical, operational, and organizational measures to secure network and information systems. This includes managing risks within supply chains and supplier relationships to ensure that both new and existing suppliers are resilient and that viable alternatives are available in case of disruptions.
3. **Reporting Obligations:** Focuses on enhancing the transparency of cybersecurity operations through the mandatory reporting of cybersecurity incidents and risks.

Benefits

- Access a team of Trustwave consultants with deep subject matter expertise in governance, risk, and compliance.
- Streamline compliance processes to align with NIS2 while optimizing resources.
- Assess supply chain risks and develop supplier oversight measures.
- Strengthen cybersecurity resilience with targeted risk management practices.
- Identify and address security weaknesses relating to NIS2 obligations.
- Establish robust incident reporting workflows.
- Ensure preparedness for audits and inspections by authorities.

The Approach

Trustwave produces a roadmap for you to prepare for NIS2 compliance and increase cybersecurity resilience, and can adopt a modular, focus area-based approach to address your specific requirements for NIS2 compliance:

1. **Requirements Gathering:** Trustwave works with you to outline the NIS2 requirements and identify the in-scope areas based on NIS2. This includes reviewing the NIS2 articles and requirements and defining the assessment scope to establish clear boundaries.
2. **Gap Analysis:** Trustwave conducts a gap analysis to identify weaknesses in your current in-scope security and resilience programs as they pertain to NIS2. This includes reviewing existing policies, procedures, and technical controls and identifying areas that need improvement.
3. **Roadmap Development:** Trustwave works with you to develop a prioritized roadmap tailored to your needs, based on findings from the gap analysis. This includes developing recommendations for addressing identified gaps and best-practice controls to meet NIS2 requirements.

Implementation Support: Trustwave can also help you implement changes to your security environment in alignment with NIS2 requirements. Implementation services may include implementing the corrective actions from the roadmap or any other activities that you are looking to achieve to increase your cybersecurity resilience, such as providing Trustwave Managed Vendor Risk Assessment or Trustwave Digital Forensics & Incident Response. Implementation services are not included in the Trustwave NIS2 Maturity Accelerator service but may be purchased separately.

Microsoft & NIS2

Trustwave is endorsed and validated by Microsoft as a leading cybersecurity partner.

Microsoft provides comprehensive security solutions to help organizations prepare for NIS2 by strengthening cybersecurity resilience, enabling regulatory compliance, and safeguarding critical infrastructure and services. This includes Microsoft Sentinel, Microsoft Defender XDR, Microsoft Defender Threat Intelligence, Microsoft Purview, and Microsoft Azure.

Trustwave can help you prepare for NIS2 with Microsoft Security via the Trustwave Accelerators for Microsoft Security service. This service provides you with a roadmap to accelerate value and security outcomes from Microsoft Security products.

Build, Test, & Run a Secure Organization

Trustwave's range of capabilities help you get the right service to suit your specific needs:

Cyber Advisory Services:

- Digital Forensics & Incident Response
- Threat Detection & Response
- Managed Vendor Risk Assessment
- Scenario-Based Crisis Simulation
- Data Protection
- Governance, Risk, & Compliance
- Security Colony
- Technology Partnerships
- Executive & Technical Training
- Threat Intelligence as a Service

Security Testing Services:

- Penetration Testing (Network, Application – Internal, External, Wireless)
- Vulnerability Scanning (Discovery, Network, Application, Database)
- Red/Purple Teaming
- Intrusion Detection & Prevention
- Database Security (DbProtect, AppDetectivePRO)
- Secure Email & Web Gateways
- Physical Assessments

Managed Security Services:

- Managed Threat Detection & Response
- Co-Managed SIEM/SOC
- Security Technology Management
- Managed Web Application Firewall
- Proactive Threat Hunting

Trustwave®

www.trustwave.com

Copyright © 2025 Trustwave Holdings, Inc.