RSA

## Buyer's Guide for CISOs:

# Achieving NIS2 Compliance

Meet NIS2 Identity Security Requirements

# Buyer's Guide for CISOs:
# Achieving NIS2 Compliance.

The CISO's (Chief Information Security Officer's) job of balancing business growth objectives and compliance requirements has always been delicate, and the pending European Union Network and Information Systems 2 (NIS2) compliance requirement will further stress that dynamic.

This EU directive imposes stricter cybersecurity requirements on businesses across various sectors and comes into effect October 17, 2024. CISOs must ensure their organizations comply with the relevant regulations and meet all applicable EU and member-state requirements.

This guide aims to help CISOs navigate NIS2 compliance and meet the requirement's identity security measures. Apart from accelerating compliance, prioritizing identity security will help CISOs prepare for the most frequent and highest-impact attacks.

# Understanding NIS2 from a CISO's Perspective.

## Expanded Scope

NIS2 applies to a wider range of organizations compared to the original NIS Directive. NIS2 now includes energy providers, waste management, wastewater, postal services, public transport operators, and additional infrastructure and services. There is also a 'size' component to NIS2. An organization may need to comply with the directive depending on its annual revenue or the size of its team. Third-party suppliers are also impacted as they will need to comply if they wish to maintain business relationships with identified entities that must meet NIS2 requirements. Familiarize yourself with the specific requirements applicable to your sector.

## Risk Management

NIS2 emphasizes a risk-based approach without being prescriptive. Every organization should identify the critical assets that adversaries are likeliest to target and prioritize efforts based on the potential impact of a cyberattack. Organizations should start by finding the risk management framework that works best for their organization or sector. Two frameworks that the EU recommends are the ISO 31000 risk management framework or ENISA's Interoperable EU Risk Management Framework, which shows interoperability and contrasts between several risk management frameworks.

# Key Focus Areas.

## Prioritize Incident Reporting

NIS2 mandates swifter incident reporting timelines than the previous NIS cybersecurity directive. Ensure your organization has established procedures for timely identification, investigation, and reporting of cybersecurity incidents to the relevant authorities. Cybersecurity tools can make this easier when metadata around the security domain is collected and reporting around the incident can be easily accessed.

## Cybersecurity Certification

NIS2 requires regular audits to ensure organizations have implemented state-of-the-art protections. Be sure to assess your tooling capabilities to guarantee your ability to gather information to provide efficient auditing.

## Invest in Threat Intelligence

NIS2 prioritizes proactive threat intelligence to anticipate and mitigate cyber threats. Implement solutions that provide real-time threat feeds and insights tailored to your industry.

## Secure Your Supply Chain

NIS2 emphasizes supply chain risk management. Evaluate the cybersecurity posture of your vendors and third-party partners. Contractual agreements should incorporate cybersecurity obligations such as joint exercises in analysis of cybersecurity postures and protection interoperability.

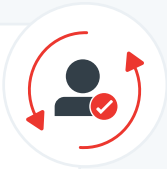
# The 5 Steps to Building a Compliant NIS2 Strategy.

Step 1

## Gap Analysis

Conduct a thorough assessment to identify gaps between your current cybersecurity posture and NIS2 requirements. Pay close attention to identity security measures, including access controls, user provisioning, and privileged account management.

Step 2



## Strengthen Identity Governance and Administration (IGA)

A robust IGA program is critical for NIS2 compliance. To comply with NIS2, IGA solutions should provide:

- **User Provisioning and Deprovisioning:** Streamline processes for granting and revoking access based on the principle of least privilege. Automate these processes where possible to minimize human error. Additionally, be sure to include processes that account for contingency planning, such as tiered approvals.
- **Access Controls:** Implement strong access controls such as multi-factor authentication (MFA) and role-based access control (RBAC) to restrict access to critical systems and data based on user roles and needs.
- **Identity and Access Management (IAM) Capabilities:** Consider implementing a centralized IAM system to manage user identities and access across your organization.

Step 3

## Policy and Procedure Review

Review and update existing policies and procedures to align with NIS2 mandates, including data breach notifications, incident response, auditing and risk management protocols, with a specific focus on identity security practices.

# The 5 Steps to Building a Compliant NIS2 Strategy.

**Step 4**

## Security Awareness Training

NIS2 emphasizes supply chain risk management. Evaluate the cybersecurity posture of your vendors and third-party partners. Contractual agreements should incorporate cybersecurity obligations such as joint exercises in analysis of cybersecurity postures and protection interoperability.

**Step 5**

## Technology Investments

Invest in security solutions that address NIS2 requirements and strengthen identity security. This may include:

- IAM systems
- MFA solutions
- Security information and event management (SIEM) systems for centralized logging and monitoring of user activity

**Complying with NIS2 requires a comprehensive and strategic approach that prioritizes identity security.**

By leveraging the insights from this guide, adopting a risk-based framework, and focusing on robust IGA practices, CISOs can ensure their organizations meet compliance standards and effectively manage cybersecurity risks.

# Meet NIS2 requirements with RSA Unified Identity Platform.

RSA provides the identity security components organisations need to prevent risks, detect threats, and meet NIS2 cybersecurity requirements. See for yourself: sign up for a free trial of RSA® ID Plus or contact our team to learn more.

## About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments. For additional information, visit our website to contact sales, find a partner, or learn more about RSA.