RAPID7

SOLUTION BRIEF

SUPPORTING NIS 2 COMPLIANCE WITH RAPID7

+ NIS 2 DIRECTIVE

As governments, public services, private enterprises and citizens become more reliant on IT infrastructure, the availability and security of that infrastructure becomes ever more critical. Embedded into the fabric of our everyday lives, the availability and uptime of IT networks aren't just commercial issues for businesses; they are now also a national security issue as well.

In recent months there have been a series of significant tech outages impacting companies across all market segments. These interruptions have affected businesses on a global scale, causing billions in lost revenues and productivity. The vulnerability of our IT dependent world has become more apparent than ever. In our hyperconnected world, cybersecurity has never been more essential.

Addressing these pervasive challenges is the driving force behind the NIS 2 Directive (Directive (EU) 2022/2555), a legislative act aimed at achieving a high common level of cybersecurity across the European Union. As an EU directive, all 27 EU member states are mandated to transpose NIS 2 into national law before October 17 2024, with enforcement starting from 18 October 2024. NIS 2 will exist alongside DORA (Digital Operational Resilience Act), an EU regulation that entered into force on 16 January 2023 and will apply from 17 January 2025. However, DORA focuses specifically on financial services companies and their suppliers, while NIS 2 applies to a broader range of organisations across the EU that are deemed critical to the economy.

Both NIS 2 and DORA focus on managing cybersecurity risk and include incident reporting and business continuity requirements, along with measures to address security of supply chains and supplier relationships. The NIS 2 directive requires that essential and important entities within the EU - or providing services for EU businesses - take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of network and information systems, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Together NIS 2 and DORA aim to create a more resilient and coordinated cybersecurity framework across the EU, ensuring that both public and private sector organisations are better prepared to handle and respond to future cybersecurity challenges.

WHO DOES NIS 2 APPLY TO?

Essential Entities (EE)

Size threshold: varies by sector, but generally 250 employees, annual turnover of € 50 million or balance sheet of € 43 million

Energy
Transport
Finance
Public Administration
Health
Space
Water supply (drinking & wastewater)
Digital Infrastructure
e.g. cloud computing service providers and ICT management

Important Entities (IE)

Size threshold: varies by sector, but generally 50 employees, annual turnover of € 10 million or balance sheet of € 10 million

Postal Services
Waste Management
Chemicals
Research
Foods
Manufacturing
e.g. medical devices and other equipment
Digital Providers
e.g. social networks, search engines, online marketplaces

Plus all sectors under "essential entities" and within the size threshold of "important entities"

More details on organisations impacted by the NIS 2 directive can be found here.

The NIS 2 Pillars

The NIS 2 directive is built on three main pillars:

Improved Cybersecurity Measures

- **Risk Management and Security Policies:** Organisations are required to implement comprehensive risk management practices and cybersecurity measures. This includes having robust security policies, conducting regular risk assessments, and ensuring the security of their network and information systems.
- **Incident Prevention and Detection:** Enhanced requirements for detecting, managing, and mitigating cybersecurity incidents. Organizations must have measures in place to prevent, detect, and respond to cyber threats and vulnerabilities.

Enhanced Reporting and Information Sharing

- **Incident Reporting:** Organisations must report significant cybersecurity incidents to national authorities in a timely manner. This includes providing detailed information about the nature of the incident, its impact, and the response measures taken.
- **Information Sharing:** Improved mechanisms for sharing cybersecurity information and best practices among EU member states. This pillar emphasises the importance of cooperation and exchange of information to effectively tackle cross-border threats and vulnerabilities.

Strengthened Governance and Enforcement

- **National Competent Authorities:** Member states are required to designate or strengthen national cybersecurity authorities responsible for overseeing compliance with NIS 2. These authorities have the power to monitor, investigate, and enforce the directive's requirements.
- **Sanctions and Penalties:** The directive introduces stricter penalties for non-compliance. Organisations that fail to meet the requirements of NIS 2 can face substantial fines and other sanctions, ensuring that there are strong incentives for adherence to cybersecurity standards.

How Rapid7 Supports NIS 2 Compliance

As per EU GDPR compliance, it is likely that multiple cybersecurity and other solutions will be required to support an organisation's overall compliance with the NIS 2 directive. At Rapid7, our solutions are designed to support compliance with the first pillar of NIS 2, focused on cybersecurity and risk management.

Under this pillar and as highlighted in Chapter IV, Article 21 of the NIS 2 legislation, organisations are expected to fulfil as a minimum a number of requirements outlined in the table below. The table illustrates how the Rapid7 Command Platform can support your NIS 2 compliance.

NIS 2 Requirement	Rapid7 Solution
Risk analysis & information system security	• Surface Command • Exposure Command • Managed Threat Complete
Incident handling	• Managed Threat Complete
Business continuity measures (back-ups, disaster recovery, crisis management)	• Managed Threat Complete
Supply Chain Security	Partner
Security in system acquisition, development and maintenance, including vulnerability handling and disclosure	• Surface Command • Exposure Command

At Rapid7, our solutions are designed to support compliance with the first pillar of NIS 2, focused on cybersecurity and risk management.

Policies and procedures to assess the effectiveness of cybersecurity risk management measures	• Surface Command • Exposure Command
Basic cyber hygiene practices and cybersecurity training	Partner
Policies on appropriate use of cryptography and encryption	• Surface Command • Exposure Command
Human resources security, access control policies and asset management	• Surface Command • Exposure Command
Use of multi-factor, secured voice/video/text comm & secured emergency communication	• Surface Command • Exposure Command

Next Steps

NIS 2 compliance within the EU and for suppliers to EU based organisations is no longer discretionary but mandatory, with significant financial penalties for non-compliance. As an organisation, Rapid7 continues to monitor and contribute to the development of emerging industry and regulatory cybersecurity standards and requirements. Within our portfolio of products we offer and continue to extend our compliance packs that either map to or partially support standards and emerging regulatory requirements. These compliance packs can speed up both regulatory compliance and ROI for our customers.

If you would like to find out more on how Rapid7 can support your NIS 2 compliance please visit: https://www.rapid7.com/products/command/exposure-management/ or contact your local Rapid7 representative or partner.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit:
rapid7.com/try/insight