BITSIGHT

SOLUTION BRIEF

Enabling NIS 2 Compliance with Bitsight

NIS 2 - or Directive (UE) 2022/2555 - has replaced the original Directive 2016/1148/EC to strengthen security across critical sectors in the EU government and companies that operate in or within the European Union. The new version of NIS enhances cybersecurity capabilities and promotes resilience in critical infrastructure and digital services —and applies to all companies, suppliers, and organisations ("entities") that deliver essential or important services for the European economy and society.

The NIS 2 Directive will enter into force within EU Member States before the end of 2024. Failure to comply with NIS 2 can result in reputational damage and sanctions imposed by national authorities, including financial penalties and operational limitations. Organisations must prioritise NIS 2 compliance to avoid such consequences.

What changes in NIS 2 over the original version?

EXPANDED SCOPE

NIS 2 broadens its applicability to include a more extensive range of companies and sectors, recognising the diverse nature of cyber threats across industries—including transport, energy, banking and financial market infrastructure, digital infrastructure, ICT service management, healthcare, water supply, waste management public administration (central and regional levels), postal and courier services.

ENHANCED COOPERATION

NIS 2 emphasises cross-border cooperation and collaboration between Member States, enabling more effective incident response and threat mitigation.

UPDATED INCIDENT REPORTING

NIS 2 imposes stricter incident reporting obligations on organisations, ensuring prompt response and mitigation of cyber incidents.

How Bitsight supports NIS 2 main pillars

Bitsight empowers organisations to achieve compliance with NIS 2, as part of their overall compliance programme, while enhancing operational resilience. Through its comprehensive cybersecurity ratings, continuous monitoring capabilities, third-party risk management solutions, and incident response planning features, Bitsight assists organisations in meeting the main pillars of NIS 2.

Security Program

Continuous Monitoring	• Bitsight provides real-time insights into an organisation's cybersecurity posture, enabling continuous monitoring and proactive risk management.
Cybersecurity Ratings	• Bitsight's comprehensive cybersecurity ratings evaluate an organisation's security controls and help measure compliance with NIS 2 requirements.

Risk Assessment

External Threat Intelligence	• Bitsight leverages external threat intelligence to identify emerging risks and vulnerabilities, enabling organisations to prioritise risk mitigation efforts effectively.
Third-Party Risk Management	• Bitsight assesses the cybersecurity posture of vendors and business partners, ensuring supply chain security and compliance with NIS 2 standards.

Security Safeguards

Identifying System Vulnerabilities	• Bitsight enables comprehensive cyber security vulnerability assessments by providing external verification and continuous insight into risk, helping organisations identify and address system vulnerabilities in line with NIS 2 requirements.
Incident Detection and Response	• Bitsight offers incident response planning capabilities, assisting organisations in promptly detecting and mitigating cyber incidents to minimise their impact.

Supply Chain

Vendor Risk Assessment	• Bitsight enables organisations to assess the cybersecurity posture of third-party vendors, ensuring compliance across the entire supply chain and mitigating potential vulnerabilities.

Incident Reporting

Actionable Insights	• Bitsight provides actionable insights and recommendations for incident response planning, helping organisations effectively meet NIS 2 incident reporting obligations.

Recommendations for NIS 2 compliance

The next steps and actions organisations need to consider include:

- Assess the current cybersecurity posture and identify gaps.
- Conduct comprehensive risk assessments and prioritise remediation efforts.
- Evaluate the cybersecurity posture of third-party vendors and business partners.
- Establish incident response plans and reporting processes.
- Implement robust security programs aligned with NIS 2 requirements.
- Continuously monitor and evaluate security controls to maintain compliance.

NIS 2 compliance with Bitsight

Bitsight enables organisations to systematically lower cyber risk by supporting critical workflows across risk, performance, and exposure. Security leaders can continuously measure the effectiveness of controls recommended by best practice frameworks and map risk vector data to control frameworks and questionnaire-based assessments—allowing them to trust but verify vendor responses and improve visibility over risk.

With increased reliance on the cloud and service providers, managing third-party risk has become increasingly challenging. But based on history in an industry we created in 2011, Bitsight gives leaders the confidence to make faster, more strategic cyber risk management decisions. To assess performance, qualify vendors, prioritise investments, and minimise financial loss. At scale.

By actively monitoring over 40 million organisations worldwide, Bitsight empowers security teams to establish a universal understanding of cyber risk, going beyond ratings to provide financial and business context. And we ensure organisations collectively reduce risk to foster digital operational resilience.

Partner with Bitsight in your journey to compliance →