BITSIGHT

DATA SHEET

Enabling DORA Compliance with Bitsight

The Digital Operational Resilience Act (DORA) is raising the standard of operational resilience across the EU's digital banking ecosystem. Bitsight's cyber risk management solutions facilitate compliance by allowing organisations to minimise ICT risk exposure, manage governance, and implement robust cybersecurity best practices—across DORA's five pillars.

1. ICT Risk Management

Scope of Application	How Bitsight Helps	Enabling Capabilities
• Governance (accountable management body) • Risk management framework and associated activities (identification, protection and prevention, detection, response and recovery, learning and evolving, crisis communication)	**Ensuring governance principles around ICT risk**. This includes identifying an organisation's tolerance for ICT risk and disruptions, based on their overall risk appetite.	• Security Ratings to measure internal and third-party risk for financial service providers and their ICT vendor ecosystem, through an objective, consistent metric that is correlated with the likelihood of cybersecurity incidents. • Mapping risk categories to standard frameworks such as ISO 27001 and NIST in order to help firms gather evidence for compliance. • Providing data to allow for better assessment of received information—for both internal governance and assurance, but also third-party oversight and risk identification. • Quick identification of cybersecurity control gaps as seen from the external attack surface.

2. ICT Incident Reporting

Scope of Application	How Bitsight Helps	Enabling Capabilities
• Standardized incident classification • Compulsory and standardised reporting of major incidents Anonymized EU-wide reports	**Assessing incident classification based on a set of specific criteria** such as number of users affected, duration, geographical spread, data loss, severity of impact on ICT systems, criticality of services affected, and economic impact.	• Risk alerts based on business context and/or services, to understand potential risk changes that may be precursor to security incidents—such as botnet infections, new vulnerabilities or material control changes. • Data breach reporting and classification for third (and fourth) parties. • Risk hunting for more susceptible controls across the vendor ecosystem.

3. Digital Operational Resilience Testing

Scope of Application	How Bitsight Helps	Enabling Capabilities
• Comprehensive testing program, with a focus on • technical testing Large-scale, threat-led live tests performed by independent testers every three years	**Providing the cybersecurity performance data and insights** to systematically lower breach risk across the full ecosystem. Our offer spans into first, third, and fourth parties—and it further raises awareness on the importance of testing and measuring its effectiveness.	• Detection of malware, botnets, and external data on compromised systems, at the event level. • Continuous monitoring of internet-facing resources based on potential breach and risk-based analysis. • Security ratings correlated to the likelihood of a data breach, providing risk quantification at scale. Fourth-party data to identify risk concentration (for example, which cloud providers are more prevalent.) • Intelligence at scale around the ICT vendor ecosystem with automated technology, including alerts and risk tiering. • Alerts related to specific control changes, allowing for management by exception • Data on historical trends up to 12 months, allowing for a better understanding of risk evolution.

4. Information and Intelligence Sharing

Scope of Application	How Bitsight Helps	Enabling Capabilities
• Guidelines on information sharing arrangements for cyber threats and vulnerabilities	**Facilitating cyber threat information and intelligence sharing** between financial firms—enabling them to be better prepared to address digital vulnerabilities.	• Inviting participants into the Bitsight product to share findings and foster data-driven, evidence-based conversations that make vendor risk management a more collaborative process. • Simplified vendor risk assessments and overall engagements, as well as evidence collection and additional risk classification and monitoring. It also reduces the repetitive work for vendors to address multiple security review requests from their customers, allowing them to share previous assessments and artifacts.

5. ICT Third-Party Risk Management

Scope of Application	How Bitsight Helps	Enabling Capabilities
• Strategy, policy, and standardised register of information • Guidelines for pre-contract assessment, contract contents, termination, and stressed exit • Create oversight framework for critical providers across the EU with clear requirements and penalties	**Ensuring the appropriate, effective security controls** and monitoring of ICT third parties are in place—specifically targeting those that can be deemed critical to the supply chain.	• Continuous monitoring that provides immediate warnings of changes in vendors' security status, including cloud security risk, in addition to annual assessments of vendor risk. • Tiering and segmenting vendors by business criticality aligned with third-party inventory. • Scalable vendor risk assessments, onboarding, and overall vendor management, complementing security artifacts with objective and dynamic security ratings. • Improved collaboration with vendors to foster collaborative remediation efforts. • Contracts can be drafted leveraging how the rating or event / risk level KPIs need to be managed, and also making sure collaboration is enforceable. • NIST-based alerts.

Why Bitsight?

Maket-Leading Cyber Risk Data
Get a complete picture of potential risk and vulnerabilities with the most extensive cyber risk data in the market

Objective Universal Standard
Measures and communicate cyber risk with the world's most widely trusted and adopted universal standard.

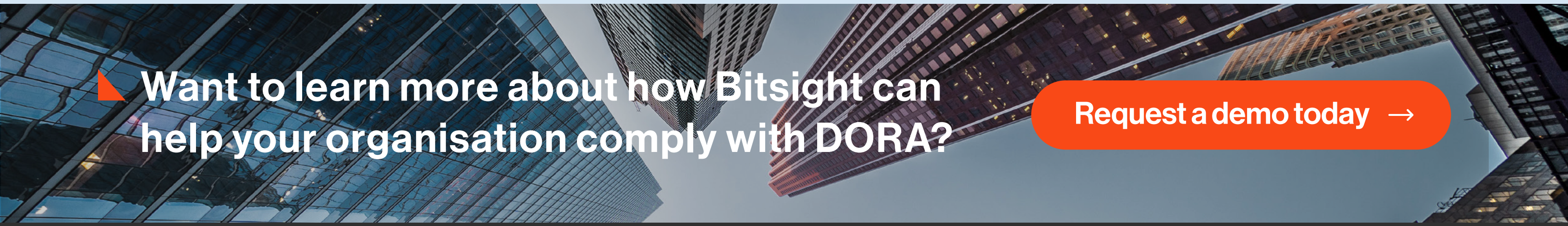
Actionable Risk Insights
Confidently build your cyber risk program with our unique and actionable insights powered by extensive data and metrics.

40M+
actively monitored organizations worldwide

400B
security events processed daily

49
granted patents

1M+
entities mapped



Want to learn more about how Bitsight can help your organisation comply with DORA?

Request a demo today →

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE