BITSIGHT

SOLUTION BRIEF

Enabling DORA Compliance with Bitsight

The Digital Operational Resilience Act (DORA) is a regulation that proposes a comprehensive information and communication technology (ICT) risk management framework for the financial sector across the European Union (EU). DORA encompasses a set of technical standards that financial entities and their critical third-party service providers are required to adopt in their ICT systems by January 17, 2025. Here's what you need to know to meet the deadline.

After years of inconsistent, individual regulations pushed by EU member states, DORA is harmonizing efforts to establish a universal framework for managing and mitigating ICT risk in the financial sector. With a shared set of rules across the EU, DORA creates a comprehensive approach to ensuring organisations can withstand, respond, and recover from the impacts of ICT incidents, thereby continuing to deliver critical and important functions and minimizing disruption for customers and the financial system.

DORA promotes the need to establish robust measures and controls on systems, tools, and third parties—as well as the need to have the right continuity plans in place and test their effectiveness.

The five pillars of DORA

01 ICT Risk Management

02 ICT Incident reporting

03 Digital operational resilience testing

04 Information and intelligence sharing

05 ICT Third-Party Risk Management

The five pillars of DORA

1. ICT Risk Management

Scope of application	• Governance (accountable management body) • Risk management framework and associated activities (identification, protection and prevention, detection, response and recovery, learning and evolving, crisis communication)
How we can help	Bitsight helps organisations to comply with the governance principles around ICT risk. This includes identifying risk tolerance for ICT risk, based on the risk appetite of the organisation and the impact tolerance of ICT disruptions.
Bitsight features	• Security Rating measures the organisation and its third-party risk for financial service providers and their ICT vendor ecosystem • Mapping Risk Vectors to frameworks

2. ICT Incident reporting

Scope of application	• Standardized incident classification • Compulsory and standardized reporting of major incidents • Anonymized EU-wide reports
How we can help	Bitsight helps to assess 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, and criticality of services affected and economic impact.
Bitsight features	• Risk Vector Alerts based on business context and/or services • Data breach reporting and classification • Risk hunting through filters

3. Digital operational resilience testing

Scope of application	• Comprehensive testing program, with a focus on technical testing • Large-scale, threat-led live tests performed by independent testers every three years
How we can help	Bitsight partners with security and risk leaders focused on managing cybersecurity performance to systematically lower breach risk across the full ecosystem. Our cyber risk management capabilities span across organisations, its third- and fourth-parties —and empower teams to test and measure the effectiveness of the risk management framework.
Bitsight features	• Bitsight detects malware, botnets, and compromised systems data (at the event level) from the outside • Continuous monitoring of internet-facing resources based on potential breach risk drivers and risk-based analysis • Rating correlates to the likelihood of a data breach, providing risk quantification at scale • Fourth-party data allows for identification of risk concentration (such as which cloud providers are more prevalent) • Intel at scale for ICT/vendor ecosystem in an automated way (including alerts and risk tiering)

4. Information and intelligence sharing

Scope of application	• Guidelines on information sharing arrangements for cyber threats and vulnerabilities
How we can help	Bitsight facilitates sharing of information and intelligence on cyber threats between financial organisations —enabling them to be better prepared to address digital vulnerabilities.
Bitsight features	• EVAs allow for information sharing between stakeholders

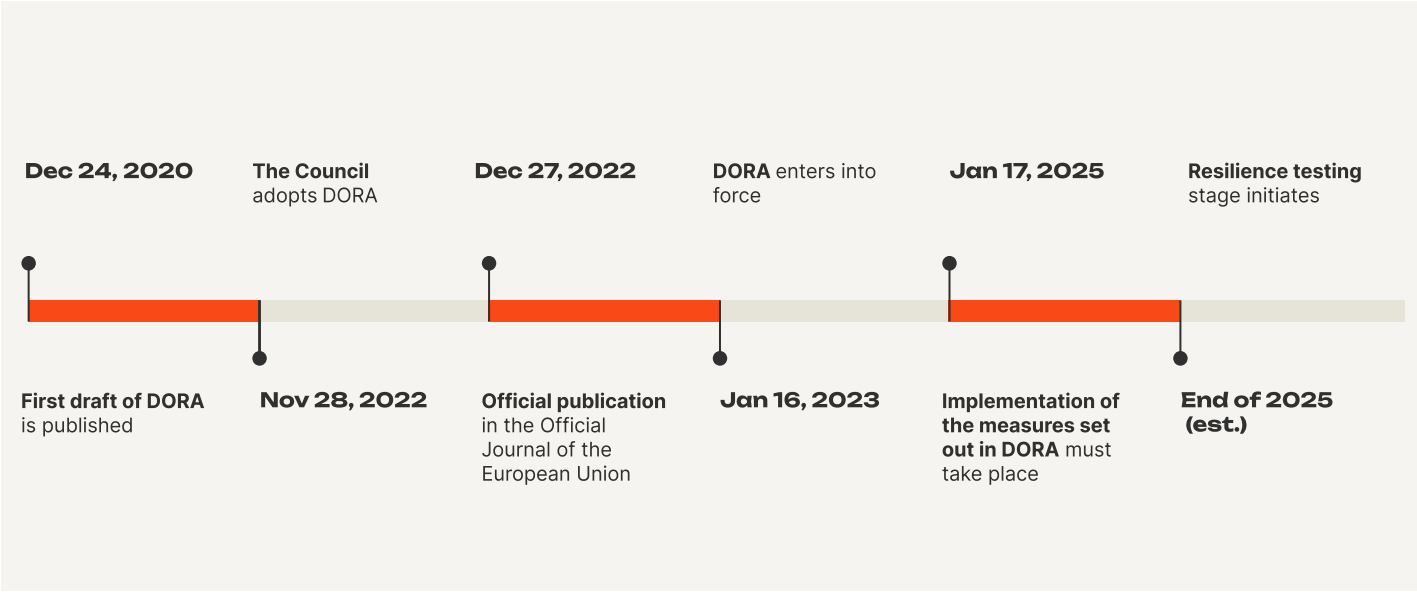
5. ICT Third-Party Risk Management

Scope of application	• Strategy, policy, and standardized 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
How we can help	Bitsight helps firms ensure they have an appropriate level of effective security controls and monitoring of their ICT third parties in place —specifically targeting those that can be deemed critical to their supply chain, as well as setting up oversight on specific providers that can be considered critical to the global market.
Bitsight features	• Continuous Monitoring provides immediate warnings of changes in vendors' security status, rather than point-in-time annual assessments of vendor risk • Tiering and segmenting vendors by business context aligned with third-party inventory • Bitsight VRM automates and scales vendor onboarding and risk assessments with custom requirements • Improved collaboration through EVAs to create an onboarding baseline • Customers can dictate to vendors how the rating or event / risk level KPIs need to be managed (or additional measures allowed) • Third-party vulnerability detection and response shows vendor exposure to known vulnerabilities and enables collaborative, evidence-based remediation • Bitsight currently has NIST based alerts, and is able to map risk vectors to specific frameworks such as ISO 27001 or common vendor questionnaires

The road to DORA

The European Commission proposed DORA in September 2020 as part of a larger package that also includes a Digital Finance Strategy with legislative proposals on crypto-assets and digital resilience. The Council of the European Union and the European Parliament formally adopted DORA in November 2022, and the European Supervisory Authorities (ESAs) are drafting the regulatory technical standards (RTS) and implementing technical standards (ITS) that will pave the way for compliance. These standards, as well as an oversight framework for critical ICT providers, are anticipated to reach their definitive form in 2024.

With the clock ticking, financial entities and third-party ICT service providers are working towards the imminent deadline of January 17, 2025.



DORA 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 controls 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 minimize 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 →