SOLUTION BRIEF

Everything you need to know about DORA

BITSIGHT®
The Standard in SECURITY RATINGS

The Digital Operational Resilience Act is being carried out by the European Union (EU) to harmonize information and communications technology (ICT) risk requirements across Europe. It specifically targets the banking and financial services industry, as well as critical ICT service providers. DORA aims to bring financial entities a harmonized and comprehensive framework for ICT risk management by potentially amending existing rules such as the Network and Information Security (NIS) Directive.

Companies around the world are transitioning their operations from physical to digital environments — with many forced to do so at an increased rate due to the widespread shift to remote work as a result of the COVID-19 pandemic. Organizations have become more dependent on ICT, and financial firms are no exception.

As a result, the world has seen an increase in the number and severity of cyber threats associated with ICT risks such as phishing, identity theft, and ransomware. The cases where organizations have dealt with new attacks targeting ubiquitous software and products — including SolarWinds Orion, Microsoft Exchange, and more recently the attack on Ireland's National Healthcare Service using Conti ransomware — further prove that cyber threats continue to evolve.

The financial resilience of organizations in the EU has been strengthened since 2008, following the European sovereign debt crisis that strongly affected some of the Eurozone countries and ultimately put the system's stability to test. However, ICT risks have not been addressed in the same incisive and coordinated manner. ICT risk has been addressed differently by the various financial supervisors of the EU member states — causing an individual, inconsistent approach that has resulted in the consequent proliferation of national, non-harmonized regulatory initiatives.

The harmonization effort sits on the global digital financial package adopted on September 24, 2020 by the European Commission, which includes a Digital Finance Strategy with legislative proposals on crypto-assets and digital resilience. This is where DORA fits in.

HARMONIZING EXISTING EU RULES: THIRD-PARTY MONITORING AND OVERSIGHT

With the Digital Operational Resilience Act, the EU aims to make sure financial organizations mitigate the risks arising from increasing reliance on ICT systems and third parties for critical operations. Organizations need to be able to "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 will promote 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.

UNDERSTANDING 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 can we help?	• BitSight helps organizations to comply with the governance principles around ICT risk. This includes identifying risk tolerance for ICT risk, based on the risk appetite of the organization and the impact tolerance of ICT disruptions.
BitSight features	• Security Rating to measure both first- and 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 can we 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 / services • Data breach reporting / 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 can we help?	• BitSight partners with security and risk leaders focused on managing cybersecurity performance to systematically lower breach risk across the full ecosystem. Our offer spans into 1st, 3rd, and 4th parties — and it further raises awareness on the importance of testing and measuring the effectiveness of the risk management framework.
BitSight features	• We detect 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 can we help?	• BitSight helps to promote sharing of information and intelligence on cyber threats between financial organizations — 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

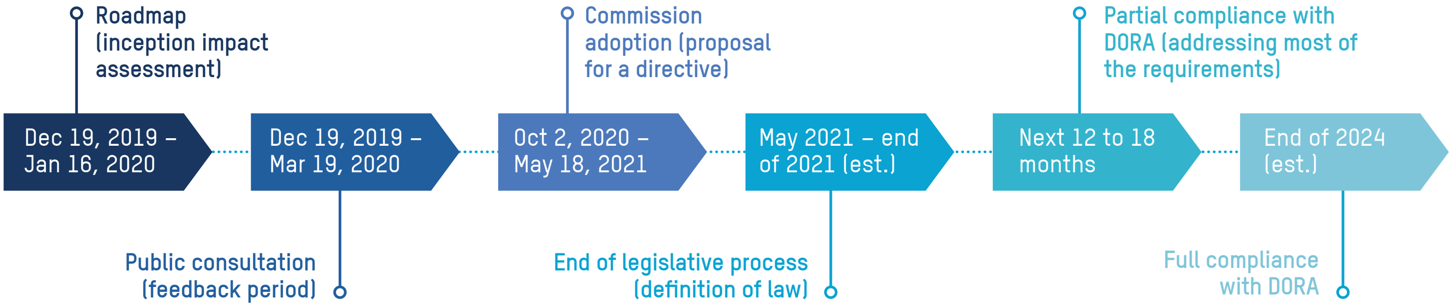
Scope of application	• Strategy, policy, and standardized register of information • Guidelines for pre-contract assessment, contract contents, termination, and stressed exit • Create oversight framework for critical providers across the EU with clear requirements and penalties
How can we help?	• BitSight 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 • Onboarding processes can be sped up and scaled by using the Security Rating and risk analysis • Improved collaboration through EVAs to create an onboarding baseline • Contracts can be drafted leveraging how the rating or event / risk level KPIs need to be managed (or additional measures allowed) • BitSight currently has ISO 27000 Based Alerts, and will map the Risk Vectors to new controls (final mappings may be more aligned when specific controls are published)

THE ROAD TO DORA

The legislative track that will drive the implementation of the DORA regulation should be relatively long, depending on how quickly potential third-party risk management issues are addressed and agreed on by the EU regulatory body. It's also important to note that there's a similar process underway for the UK in the face of Brexit, which may add time to the overall process.

DORA should gain most of its form by the end of this year, giving firms 12 months (or possibly 18 months) to comply with most of the requirements. It is also expected that the following subset of legislation will give firms another 1.5 years to get into compliance. The whole process should be running at full steam by the end of 2024.

While these deadlines may seem reasonable, it's important to note that this is a pressing subject. The new DORA framework will very likely introduce some degree of complexity, and there will also be penalties for failing to comply with the directives, which may be applied both financially and criminally. DORA should therefore be addressed with all due urgency.



Roadmap (inception impact assessment)

Dec 19, 2019 – Jan 16, 2020

Public consultation (feedback period)

Dec 19, 2019 – Mar 19, 2020

Commission adoption (proposal for a directive)

Oct 2, 2020 – May 18, 2021

End of legislative process (definition of law)

May 2021 – end of 2021 (est.)

Partial compliance with DORA (addressing most of the requirements)

Next 12 to 18 months

Full compliance with DORA

End of 2024 (est.)

SOLUTION BRIEF

Everything you need to know about DORA

ABOUT BITSIGHT

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Fifty percent of the world's cybersecurity premiums are underwritten by BitSight customers, and 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks.

For more information, please visit www.BitSight.com, read our blog or follow @BitSight on Twitter.

WHY BITSIGHT?

- BitSight helps firms to systematically lower cyber risk by supporting cybersecurity governance, management, and assurance. BitSight helps firms to continuously measure the effectiveness of controls recommended by best practice frameworks including ISO27000 and NIST Cyber Security Framework.

- BitSight is the only Security Rating Service provider with a third-party validated correlation to breach. Read our corporate overview to learn why BitSight is the leader in the security ratings market and how BitSight transforms how companies manage risk. And dive into our Methodology & Governance Process to see how we incorporate only the most critical, high-quality Risk Vectors into the Security Rating.

- BitSight has a solid track record on mapping our Risk Vectors and data to standard frameworks in order to help firms comply with the various existing regulations. Our Risk Vectors provide evidence for compliance with regulations and standards, such as ISO, NIST, and more specifically GDPR in the case of the Eurozone. DORA has not evolved yet to include a controls framework. However, BitSight will provide a mapping to our Risk Vectors as soon as the proposal is approved and clarified.

- BitSight understands how increasingly challenging managing third-party risk has become. Based on history in an industry we created in 2011, we give firms the confidence to make faster, more strategic cyber risk management decisions. BitSight for Third-Party Risk Management allows organizations to quickly launch, grow, or optimize vendor risk assessment validation, continuous monitoring, and assurance with the resources they have today.

- BitSight empowers organizations to establish a universal understanding of cyber risk. We hold 32 patents and have rated over 40 million companies. And with the help of our vast BitSight community we contribute to making sure organizations collectively reduce cyber risk and foster digital operational resilience. BitSight provides extensive visibility into key areas of cyber risk that are correlated to breach, including compromised systems, open ports, mobile and desktop software, and file sharing.

- BitSight is leading the cybersecurity ratings industry with the most customers, robust quality data sources, and third-party validated correlation to breach. We are dedicated to helping customers identify, quantify, and mitigate security risks.