DORA

A Journey to Cyber Resilience

SecurityScorecard

INTRODUCTION

In January 2023, a pivotal regulation took center stage for the European Union (EU) financial services sector. The Digital Operational Resilience Act (DORA) emerged as a requirement, ushering in a new era of cybersecurity.

This regulation mandates banks, financial entities, and select ICT third-party providers within the EU to adopt robust cybersecurity measures. The goal? Safeguarding consumers and reinforcing the EU's financial system against the intricate risks posed by informationand communication technologies (ICT).

DORA builds on over a decade of global and EU efforts to address systemic risks to financial stability in the aftermath of the 2008 global financial crisis. This new legislation aims to counter the speed and scale of adversarial cyber threats that result from complex interdependencies across the EU's financial services sector.

At its heart, DORA is designed to ensure cyber resilience. It mandates financial organizations establish networks of trust among themselves and with their ICT vendors. And financial entities subject to DORA must take steps now to manage third-party risk more effectively.

DORA's pillars of transformation

Included in DORA are five key pillars that will shape how financial services organizations manage Information and Communication technology (ICT) and cyber risks.

1. ICT risk management
2. Incident reporting
3. Digital operational resilience testing
4. Third-party risk management
5. Sharing of information and intelligence

1 ICT RISK MANAGEMENT

Organizations must develop and implement a comprehensive ICT risk management framework as part of their overall risk management system. Having a platform in place that can help develop, implement, and monitor this framework will address regulatory requirements, while cybersecurity ratings will provide a quantitative, data-driven assessment of your organization's cybersecurity posture.

Our comprehensive Enterprise Cyber Risk Management solution can help you stop cyberattacks before they happen. And our security ratings provide a data-driven assessment of an organization's cyber health so you can manage cyber risk and comply with DORA's ICT risk management requirements.

SecurityScorecard's reporting platform can help you efficiently detect, analyze, and report incidents, offering a streamlined solution for organizations seeking to maintain DORA compliance. SecurityScorecard also offers direct access to highly-skilled and elite incident response experts who are standing by and ready to support your organization with triaging, recovering from, and responding to cyber incidents.

2 INCIDENT REPORTING

Under DORA, financial institutions are required to report ICT-related incidents to regulators in a timely manner. The following details should be reported: the number of users affected; the amount of data lost; the geographical spread; the economic impact; and more. This plan should also include a detailed description of how employees will respond in the event of a cyberattack, and how operations will be restored if such a breach occurs.

3 DIGITAL OPERATIONAL RESILIENCE TESTING

Continuous monitoring of your cybersecurity posture will keep your organization informed of potential risks so that it can quickly address any issues that arise. This includes regularly monitoring and evaluating the security posture of your third-party vendors to identify any changes or vulnerabilities that may impact your organization's overall risk profile.

SecurityScorecard's platform enables continuous monitoring of your cybersecurity posture by employing automated threat detection. This aligns with DORA's requirements for ongoing risk management and incident reporting.

4 THIRD-PARTY RISK MANAGEMENT

DORA will mandate that third-party risk be managed as an integral component of overall ICT risk, to ensure that providers will support your firm in the event of a cybersecurity incident and adhere to tighter security standards. As a result, organizations should regularly assess and monitor these relationships in order to gain instant visibility and keep an eye on red flags and the providers who are critical to the supply chain.

SecurityScorecard's flexible third-party risk management solution enables quick and accurate control of risk across your entire digital ecosystem. This 360-degree view into the cyber posture of third-party vendors, directly supports DORA's focus on third-party risk management.

5 SHARING OF INFORMATION AND INTELLIGENCE

DORA requires relevant entities to regularly test their cyber resilience, which can include conducting vulnerability assessments, penetration tests, red teaming, tabletop exercises, and more. Staying proactive will help to identify and mitigate potential risks while ensuring business continuity in the event of a cyber incident.

Make your organization cyber resilient with a range of services that battle-test your security controls, identify gaps in your attack surface, and enhance your ability to defend against cyberattacks. SecurityScorecard's threat intelligence capabilities can proactively identify and mitigate potential risks, supporting DORA's emphasis on resilience testing and incident reporting.

UNITING FOR CYBERSECURITY: A COLLECTIVE CALL TO ACTION

DORA signifies a cross-functional strategy. Legal, compliance, risk management, and other teams must unite alongside the CISO. This collaboration ensures swift and efficient DORA compliance. As 2024 approaches, organizations must prepare for the DORA journey. Policies and protocols already in place need refinement. The path is clear: streamline cybersecurity and amplify cyber resilience.

Unleashing the power of SecurityScorecard

SecurityScorecard stands as the beacon for cybersecurity measurement, rating over 12 million entities continuously. Our platform encompasses DORA's core facets: ICT risk management, resilience testing, incident reporting, and third-party risk management. It empowers organizations to identify and neutralize risks proactively, delivering continuous monitoring and vendor risk management to stay vigilant against potential threats.

For Further Guidance: To delve into DORA's nuances and chart your path to readiness, visit:

securityscorecard.com/dora-compliance GET STARTED

SecurityScorecard