SecurityScorecard

Your DORA To-Do List:
How to prepare for the Digital Operational Resilience Act (DORA)

REGULATION (EU) 2022/2554

Overview

The Digital Operational Resilience Act (DORA) is a pivotal piece of legislation aimed at strengthening the digital resilience of regulated financial entities in the European Union, including: credit institutions, investment firms, insurers, and more. Included in DORA are five key pillars that will shape how these organizations manage Information and Communication technology (ICT) and cyber risks. **They are:**

- ICT risk management
- Incident reporting
- Digital operational resilience testing
- ICT third-party risk management
- Sharing of information and intelligence

Below are five steps you can take now to prepare your organization for DORA:

1 KNOW YOUR THIRD-PARTY RISKS

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.

Our 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.

2 HAVE THE TOOLS READY FOR 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.

SecurityScorecard's **reporting platform** can help you efficiently detect, analyze, and report incidents, offering a streamlined solution for organizations seeking to maintain DORA compliance. Get direct access to elite **incident response** experts, ready to support with triaging, recovering from, and responding to cyber incidents.

3 ENABLE CONTINUOUS MONITORING

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 ESTABLISH A RISK MANAGEMENT FRAMEWORK

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.

5 CONDUCT REGULAR RESILIENCE TESTING

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.

SecurityScorecard's **threat intelligence capabilities** can proactively identify and mitigate potential risks, supporting DORA's emphasis on resilience testing and incident reporting.

Additional DORA tips:

- **Get your board on board.** DORA places responsibility for cybersecurity on the shoulders of the board. A company's board must ensure that these protocols, policies, and tools are enforced. Failure to do so could result in fines or reputational damage. So make sure management is on the same page, and understands the importance of DORA.
- **Bring in multiple teams.** Cybersecurity is no longer just an ICT issue, which means that compliance with DORA shouldn't be the sole responsibility of the CISO. Involving legal, compliance, risk management, and other relevant teams from the start will ensure your company can meet the DORA requirements faster and more efficiently.
- **Get ready now.** Firms should start planning now for how to align with the new regulations. Most firms that fall under DORA's scope no doubt have some of these policies and protocols in place, but this is an opportunity to streamline cybersecurity and become more cyber resilient.

How SecurityScorecard can help

SecurityScorecard is the trusted, must-have standard for measuring cybersecurity, with over 12 million companies continuously rated. Our platform offers a comprehensive solution covering all major aspects of DORA, including ICT risk management, resilience testing, incident reporting, and third-party risk management. Organizations are empowered to identify and mitigate risks before they become incidents, and with continuous monitoring and vendor risk management, businesses can stay informed about potential threats and vulnerabilities.