Rocket® software

Bringing Security and Resilience Into Alignment

Preparing for the Digital Operational Resilience Act

Contents

Introduction

Digital transformation projects are helping businesses achieve their goals and fuel innovation. Whether it's a push to tap into the growing wave of artificial intelligence or pressure to kickstart a cloud migration, modernization projects are redefining the way businesses operate. But the reality isn't quite so simple — as technology evolves, so do security risks and system vulnerabilities.

It's no secret just how much damage a cyber-attack or a data breach can cause, and government agencies across the globe are responding in kind with a variety of new regulations. As governments try to get a handle on IT security standards, the advent of major regulations, like the California Consumer Privacy Act (CCPA) or the General Data Protection Regulation (GDPR), has made it more important than ever for organizations to prioritize their security infrastructure.

Now, a new piece of legislation in the European Union (EU) — the Digital Operational Resilience Act (DORA) — is set to bring global-reaching consequences to the way businesses manage IT security, and requires companies to be compliant by January 2025. With less than a year until that deadline, operational resilience cannot be ignored. Failing to act and address the state of security infrastructure now will almost certainly generate disastrous ramifications.

Let's take a look at how this new batch of regulation impacts businesses around the world — and what IT needs to do now to improve their security posture and build resilience.

← Back to contents

What is DORA?

First introduced in 2020 and later enacted in 2022, the policies and guidelines within DORA aim to establish a consistent and common level of digital operational resilience across financial services firms in — or doing business with — the EU. Specifically, the stated goal of this policy is to develop a European approach that fosters a standardized structure of technological development while ensuring financial stability and consumer protection. DORA ultimately requires that EU financial entities begin to adopt comprehensive information and communications technology (ICT) risk management capabilities into their security processes. The regulation also creates a consistent set of requirements for the security of network and information systems used by those financial entities as well as critical ICT vendors. To achieve its outlined objectives, DORA lays out five specific focus areas for organizations to address concerning the security of network and information systems:

ICT risk management

Reporting of major ICT-related incidents

Digital operational resilience testing

Information and intelligence sharing

Management of third-party risk

What this means is that businesses need to act quickly to make sure they're ready to comply with DORA before it takes full effect starting in January 2025. Ultimately, the goal of DORA is to ensure that the EU financial organizations it affects will have policies in place for the testing of ICT system controls and processes and managing ICT third-party risk.

← Back to contents

Is My Organization Impacted?

Now for the question that's on every business leader's mind — does this impact my organization? In short, the answer is almost certainly. DORA places a heavy emphasis on financial organizations in the EU — ranging from banks to insurance companies — but those are not the only businesses that will be impacted. Any organization that does business with those EU-based banks, insurers, or financial organizations will also need to fall into compliance, even if they are not based in the EU.For example: this could mean that a major U.S. business that banks with an EU financial institution, or an organization with a subsidiary that operates in the EU, or a Hong Kong-based bank that has offices in the EU all need to adhere to the guidelines in DORA or face significant risks.

Considering how far-reaching DORA truly is, businesses will need to take immediate steps to start moving toward compliance — that includes modernizing mainframe systems and other critical IT infrastructure. The requirements outlined in DORA extend directly to any third-party provider of ICT services for financial services organizations, holding them to the same standards. So, whether it's a US-based cloud services provider or a software company with European clients, if they are working with financial firms in the EU compliance with DORA is required.

Failing to take steps toward compliance could not only preclude businesses from new opportunities in the EU, but could easily result in administrative sanctions issued by EU member states for breaches of the regulation. Compliance with DORA will require full adherence to all five of the focus areas outlined in the policy — ICT risk management, reporting major ICT incidents, digital operational resilience testing, information and intelligence sharing and third-party risk management — with an emphasis on the processes and systems needed to mitigate risk. All five of these pillars are critically important. As we dive into what this means for organizations and their customers and partners, we'll be drilling down into two of the most pressing of those groups: digital operational resilience testing and ICT risk management.

Digital Operational Resilience Testing

Unsurprisingly, one of the most important pillars outlined in DORA centers around digital operational resilience testing. As businesses prepare for that January 2025 deadline, testing will be a critical capability to build up as it sits at the core of DORA. As part of its guidance for businesses, DORA introduces a mandatory digital resilience testing program for financial entities as an integral part of the ICT risk management framework. But again, that expectation doesn't stop at the EU-based organization: testing capabilities will need to be in place for any business that finds itself involved in the EU in some way.

As far as the testing itself, businesses will need to conduct their testing through either internal or external independent parties. And, in turn, that means they will need to ensure their penetration testing and vulnerability scanning processes are up to the task of regular audits, as DORA lays out the need for testing on at least a yearly basis.

ICT Risk Management

Next, let's dive into the ICT risk management element of DORA. Being compliant with the policy will require significant investment in setting up an internal governance and control framework. Beyond the set of strategies, protocols, and procedures that make up that framework, complying with the ICT Risk Management component of DORA also requires that companies deploy systems to detect anomalous activities and potential material single points of failure. From there, compliance will also require considerable focus on vulnerability management. From a mainframe perspective, firms will need to ensure their systems are ready and modernized with the right mitigation solutions and processes. The way vendors process and report security vulnerabilities will undergo significant changes as DORA brings increased scrutiny and a renewed focus on vulnerability mitigation.

← Back to contents

How Can You Start Preparing for DORA Today?

The arrival of DORA will have implications for businesses far beyond the EU and far beyond the financial services vertical. As businesses look at their IT systems and security capabilities, the need for significant digital transformation is clear.

As IT leaders begin navigating the complexities of this regulation, organizations need to prioritize several key areas for optimal risk management:

01

Define clear roles and responsibilities

DORA outlines that management bodies will be expected to maintain an active role in adapting their ICT risk management framework and overall operational resilience strategy. Board members and executive leaders are responsible for defining, approving and overseeing the implementation of all arrangements related to the ICT risk management framework, including setting clear expectations and roles. Among others, these overarching responsibilities include putting policies in place that will ensure the highest standards of availability, authenticity, integrity, and confidentiality, of data as well as setting clear roles and responsibilities for all ICT-related functions. They will also need to establish appropriate governance arrangements to ensure timely communication, cooperation, and coordination across all of those functions and roles.

02

Implement a periodic review of the ICT Business Continuity Policy and ICT Disaster Recovery Policy

Implementing a regular review cadence for ICT business continuity and disaster recovery policies is crucial for effective risk management oversight. According to DORA, “financial entities shall regularly review their ICT Business Continuity Policy and ICT Disaster Recovery Plan taking into account the results of tests carried out in accordance with recommendations stemming from audit checks or supervisory reviews.” With regulatory technical standards outlining the need for organizations to design their IT infrastructure and business continuity measures to achieve less than 2 hours of downtime, moving to this model is a critical way to meet this challenge. Implementing these changes will help ensure they get the right people, processes, and technology in place for compliance, stay ahead of current threats, and achieve business continuity amidst the ever-changing threat and regulatory landscape.

← Back to contents

03

Allocate and consistently review budget related to fulfilling digital operational resilience needs

Preparing for a new set of regulations requires the right resources to be effective. As an example, DORA requires a crisis management function that implements clear procedures to manage internal and external crisis communications in accordance with Article 13. As organizations look to implement new digital operational resilience capabilities, they need to prioritize allocating enough budget to fully address risks and implement new technologies and processes. But since security risks and new vulnerabilities are always evolving, as are regulations, there should also be a periodic review of budgeting to ensure security concerns are adequately addressed at any given time.

04

Implement ICT security tools and processes

Any DORA-focused preparations need to take tools and processes into account. Organizations need to consider legacy systems like the mainframe as well as vulnerabilities that might be leaving the business exposed to excessive risk. Particularly as systems evolve, implementing the right security tools is critical to identifying and managing mainframe vulnerabilities. Precise vulnerability management tools, penetration testing, and compliance assessments are a few of the critical technologies and processes a business should consider for optimal risk management oversight.

Rocket Software brings a unique set of solutions that are ready to help modernize and secure critical IT infrastructure, regardless of whether it's legacy systems, hybrid cloud, or cloud-based, to help keep up with evolving demands. We will partner with you on mainframe security when it comes to vulnerability management, penetration testing, and compliance assessments, as well as securing your open-source languages and tools, managing and recovering your data, and automating the health of your DevOps ecosystem.

Keeping Pace with Evolving Regulatory Demands

New regulations like DORA can be difficult to understand and keep up with, especially when managing regulatory compliance across a handful of regions and governments. When it comes to remaining compliant, mainframe modernization will only become more important. Equipping IT teams with the right tools and solutions to meet the most stringent security requirements will help build critical resiliency for the long run. process and report security vulnerabilities will undergo significant changes as DORA brings increased scrutiny and a renewed focus on vulnerability mitigation.

About Rocket Software

Rocket Software partners with the largest Fortune 1000 organizations to solve their most complex IT challenges across Applications, Data and Infrastructure. Rocket Software brings customers from where they are in their modernization journey to where they want to be by architecting innovative solutions that deliver next-generation experiences. Over 10 million global IT and business professionals trust Rocket Software to deliver solutions that improve responsiveness to change and optimize workloads. Rocket Software enables organizations to modernize in place with a hybrid cloud strategy to protect investment, decrease risk and reduce time to value. Rocket Software is a privately held U.S. corporation headquartered in the Boston area with centers of excellence strategically located throughout North America, Europe, Asia and Australia. Rocket Software is a portfolio company of Bain Capital Private Equity. Follow Rocket Software on LinkedIn and X.

Learn more about what DORA means for the mainframe and talk to an expert about how Rocket Software can help.

Visit RocketSoftware.com ›

Talk to an expert

Rocket software

MAR-9436_Whitepaper_DORA_V1