Capgemini

ARE YOU READY FOR DORA COMPLIANCE?

ENSURING STABILITY FOR AN EVER-CHANGING DIGITAL BUSINESS ENVIRONMENT

Content

Introduction

Ever since the financial crisis of 2008, the European Commission (EU) has been working to strengthen the financial resilience of the EU financial services sector, adopting measures aimed at increasing capital resources and liquidity, as well as reducing market and credit risks. Indeed, the European regulatory context becomes more complex every year, requiring transformation projects and remediation initiatives by players all across the financial services industry. And while other aspects of business resiliency have received some attention, too – information technology, infrastructure, and more – efforts here have often been in a more piecemeal and sometimes even divergent fashion across individual country jurisdictions.

A recent regulatory initiative of the European Union works to broaden the resiliency lens across the financial services industry. While financial and capital-management resiliency remain paramount, the Digital Operational Resilience Act, or DORA, ensures that infrastructure and software resilience are also a part of the requirements of operational risk management for financial institutions, as well as for critical information and communication technology (ICT) providers, operating within the EU. The regulation aims to protect, promote, and strengthen the technology development of business, while also protecting consumers' finances.

This paper focuses on implications and needed action for financial services institutions as the deadline for DORA compliance approaches – January 17, 2025. By introducing a consistent supervisory approach across the industry, DORA ensures convergence of security and resilience practices across firms operating in the EU.

Understand DORA and implications for your organization

So what exactly is DORA? The Digital Operational Resilience Act is a new law from the European Parliament implemented in December 2022. It requires companies to do a detailed risk assessment and figure out what could go wrong with their digital systems; in addition, businesses must report any problems that do happen so that they can be tracked, controlled, and stopped from happening again. DORA imposes new responsibilities on EU financial institutions in a variety of areas, and the regulation also introduces a new framework for direct EU financial regulator supervision of critical ICT service providers. It will be vital to accelerating digital innovation in the European financial services sector and will go into full effect on January 17, 2025: impacted organizations in the EU and their critical ICT providers must be ready to comply with DORA by this date.

DORA AND FINANCIAL SERVICES ENTERPRISES	DORA AND ICT PROVIDERS
Banks, auditors, and audit firms	Information and communication technology vendors
Brokers, credit rating agencies	Digital and data services providers
Payments institutions	Cloud computing services providers
Credit institutions	Software providers
Investment firms	Data analytics services providers
Crowdfunding services	Data centers and hosting providers
Trading venues and repositories	
Insurance and reinsurance firms	
Crypto-asset providers	

In sum, DORA aims to consistently target cyber and digital risk for all financial entities. It is intended to address the growing risk of illegal activity and consequent disruption of digital services in institutions where such disruptions can have a direct negative impact on society and the economy.

DORA introduces new challenges for financial services organizations

While many aspects of the new regulation are not entirely new, rather building on risk management and other initiatives already in place or in various stages of development, industry players will be required to meet new challenges across multiple technology and digital dimensions because of DORA:

- **Formal approach to resiliency**: DORA introduces a standardized set of requirements across the financial services sector. DORA sets high resilience expectations, with entities expected to be able to quickly restore services after a cyber incident. This requires advanced disaster recovery and business continuity measures. Financial institutions must create and regularly update an ICT risk management framework containing information on strategies, procedures, and tools. An ICT third-party risk strategy has to be a key component of the overall framework.
- **Cyber risk management**: Cyber risks must be actively managed: processes are to include risk classification, monitoring, documentation, and reporting. Response and recovery, as well as business continuity management, strategies must be implemented.
- **Testing and reporting**: IT systems must be tested regularly, and the testing strategy reviewed and updated continuously to ensure compliance. Tests will include vulnerability scans, network assessments, and penetration assessments.
- **Incident reporting and collaboration**: DORA requires entities to report promptly significant cyber incidents to competent authorities. Although not mandatory, financial institutions are also encouraged to set up collaborative alliances within the industry; procedures and rules should be defined and enacted, all with the goal of sharing cyber-threat intelligence and information between entities.
- **Third-party risk**: Third-party ICT providers will be subject to contractual changes and their ICT resilience strictly assessed. DORA emphasizes the need for entities to manage and monitor these external risks. Contracts must be reviewed and potential rewritten to meet DORA rules, and collaboration with non-compliant providers stopped.

Non-compliance penalties are under development

Monetary penalties for financial entities have not yet been set; member states will lay down frameworks in due course, and DORA also leaves the door open for potential criminal liability for non-compliance. Monetary penalties for critical ICT third-party service providers will be up to 1% of their average daily worldwide turnover in the preceding business year, applied on a daily basis until compliance is achieved, for a maximum of six months.

A quick word about related developments in the UK and the US

While a European regulation, DORA may apply and have implications for foreign-domiciled enterprises with operations in the EU, including those from the US and the UK.

- **For certain, DORA will apply to certain UK financial services firms if they operate in the EU: UK entities will need to determine if they fall in scope of DORA, based on the broad range of types of financial markets activities included and whether those take place within EU jurisdictions. In addition, there are also plans to expand the operational resilience regime in the United Kingdom: in July 2022, the UK Parliament proposed amendments to various laws that would permit direct regulation by UK financial authorities of critical third-party service providers in the UK financial sector, similar to DORA. A discussion paper delineating implementation options for their proposed new powers has been released and the consultation process concluded in December 2022, but the timetable for any broader implementation remains uncertain.**

- **In the US, the New York Department of Financial Services is presently revising its 2017 Cybersecurity Regulation to, among other things, impose stricter business continuity and data retention requirements on large entities. While DORA imposes broader obligations on financial institutions, New York's updated cyber rules may be more stringent in certain respects.**

Focus is needed across all five of DORA's pillars

The DORA regulation is based on five pillars of resilience, which are described below.

1. ICT risk management

ICT risk management significantly reduces the likelihood of unanticipated cyberattacks by conducting effective and exhaustive risk assessments that seek to prevent and detect cyber threats prior to their gaining a foothold. This pillar assigns ultimate responsibility for implementing the appropriate measures and controls, ensuring operational and security risk management, and a robust, well-documented ICT risk management framework, to each firm's management body. In order to comply, businesses must identify their impact tolerance, risk associations, and critical functions.

Action steps:

- Develop a comprehensive risk identification, classification, and management framework
- Define risk prevention, response, and recovery plans
- Plan for training of management and staff

2. ICT incident reporting

This pillar requires companies to submit a report regarding any ICT related incidents or threats that have occurred. Reports must include details around the number of users affected, the amount of data lost, the severity of the impact on ICT systems, the geographical spread, the criticality of the services affected, and the economic impact. By submitting a detailed report, incidents can be appropriately monitored and managed, and organizations and regulators can gain knowledge to continuously enhance recovery.

Action steps:

- Update incident classification methodologies
- Set up both internal and external notification channels

3. Digital operational resilience testing

Financial institutions must conduct proportional, threat-based penetration testing every three years. Companies should not conduct these evaluations themselves: rather, independent testers should be scheduled in advance with DORA regulator sanction to ensure accurate test results. The prescribed planning time for this procedure is approximately two years. This is perhaps the most challenging of the pillars: companies are urged to begin preparations as soon as feasible to meet the end of 2024 deadline for regulator authorization.

Action steps:

- Develop threat led penetration testing
- Seek approvals and certification on testing scenarios and processes
- Include all third-party systems in resilience testing

4. ICT third-party risk

This pillar asserts that organizations must implement third-party risk management as a fundamental element of their ICT risk management framework. This includes a multi-vendor ICT third-party risk policy strategy, and an information register comprising details on all ICT providers, the services they provide, and the functions they support, as well as an annual report on changes to the information register. In addition, DORA enforces annual regulatory assessments for essential providers to ensure organizations' compliance with the law; any standard checks that reveal noncompliance will result in legal and monetary sanctions.

Action steps:

- Create a well-defined strategy and policy
- Develop a third-party register
- Perform third-party audits and assessments

5. Information and intelligence sharing

In order to create a more robust and resilient environment for financial services organizations across Europe, sharing intelligence and information serves to protect and support other financial services against operational threats. DORA has introduced guidelines for sharing arrangements between companies, creating stable communities that transfer intelligence and information in accordance with regulations, requirements for confidentiality, data protection, and trade secrets.

Action steps:

- Participate in groups and consortiums
- Develop automation solution for information and intelligence sharing
- Determine an internal communications mechanism for digesting and saving shared knowledge

Meeting financial services enterprise resiliency challenges will bring industry benefits

Managing internal and third-party risk has become increasingly challenging in today's world, and financial services enterprises are under pressure to account for how they and their third-party providers use and protect their data. With the adoption of DORA, significant benefits from entities having a harmonized and comprehensive framework for ICT risk management may accrue. And in addition to bringing synergies at the EU level, DORA may also have enough impact to help push for a digital single market adoption across financial services more globally.

In conclusion: accelerate DORA compliance

January 2025 will be upon us all in a flash and DORA compliance has to be achieved: make sure leadership across your organization comprehends fully what true operational resilience – the continuation of all business operations in the face of unforeseen disruptions and obstacles – requires. While the specific DORA pillars and considerations for compliance within each have already been discussed, as your program moves forward, remember to focus on the following to strengthen implementation and evaluation efforts:

- Ensure business continuity planning is robust and include strategies for the resumption of normal operations quickly and efficiently; data center migrations, data recovery planning, backup systems, and stakeholder communications plans are all necessary components.
- Create detailed and specific mapping of internal and external dependencies and interconnections required to execute crucial operations; documentation needs to include all pertinent contacts and elements, including individuals, facilities, technologies, and processes.
- Perform periodic self-assessments to capture consistent and up-to-date information on any vulnerabilities or threat opportunities, and then work to mitigate these potential risks and maintain the highest resilience levels.

Gaining full DORA readiness is no small lift for any enterprise, and it may even require some rebuilding of technology architecture for some players in addition to all other workstreams. Make sure the right in-house resources are fully engaged and focused, and that needed collaborations with third-party providers, ICTs and others, are firing on all cylinders. While there are certainly challenges to be overcome, DORA will bring significant benefits to your organization and across the financial services industry.

Ask the experts

Ramandeep Singh
Financial Services Cloud Engineering Leader
ramandeep.singh@capgemini.com

Endnotes

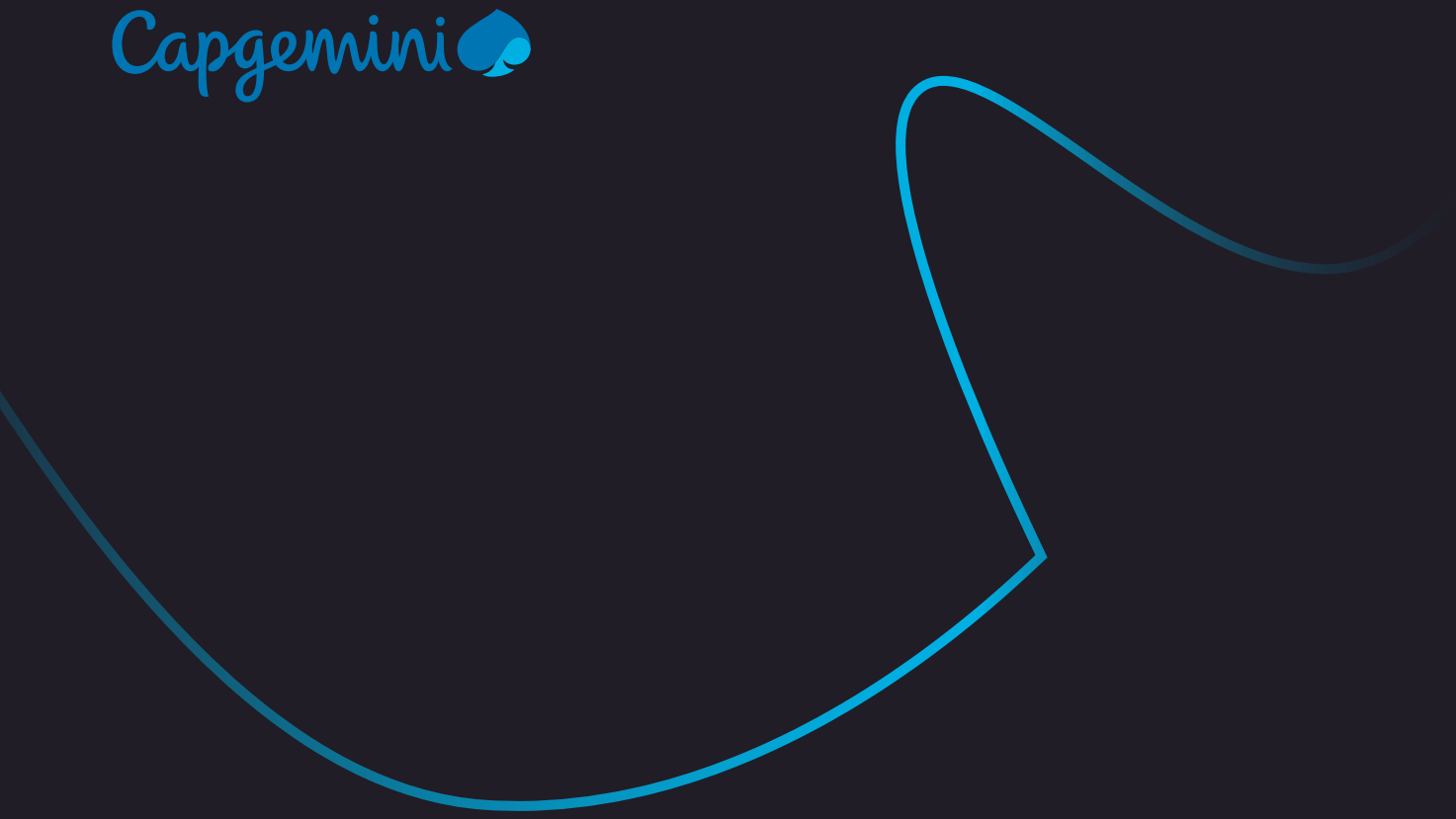
[1] EUR-Lex, Final Regulation Text.

[2] EBA, Draft Regulatory Technical Standards – Risk Management.

[3] EBA, Draft Regulatory Technical Standards – Incident Classification.

[4] EBA, Draft Regulatory Technical Standards – Register of Service.

[5] EBA, Draft Regulatory Technical Standards – Third Party Contracts.



About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com

Disclaimer