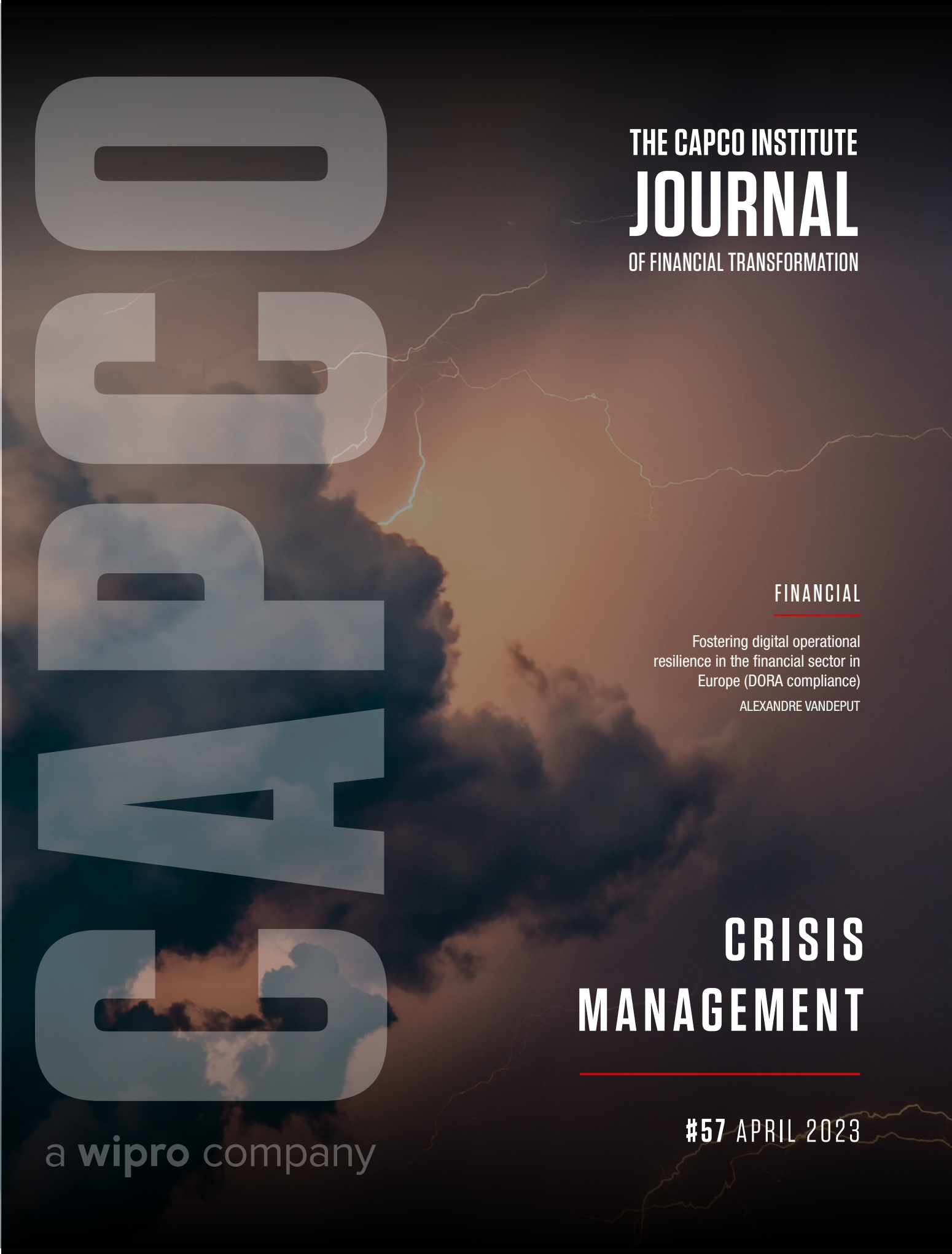


CAPCO

a wipro company

THE CAPCO INSTITUTE

JOURNAL

OF FINANCIAL TRANSFORMATION

FINANCIAL

Fostering digital operational resilience in the financial sector in Europe (DORA compliance)

ALEXANDRE VANDEPUT

CRISIS MANAGEMENT

#57 APRIL 2023

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

FINANCIAL

REGULATION

ESG

DEAR READER,

Recent events in the U.S. banking sector, and broader concerns around instability and contagion within the global financial services industry, have meant that crisis management is once more front of mind for many institutions.

In addition, the world of business and finance is facing broader geopolitical and socioeconomic challenges, ranging from conflict, climate change, inflationary pressures, and precarious energy resources. Factor in heightened regulatory and competitive pressures, and it becomes clear that financial institutions must prioritize risk management, within their own organizations and with their counterparties.

The papers in this edition of the Journal address the theme of crisis management through various lenses, including regulatory compliance and traditional risk management, as well ESG, the low carbon economy, and sustainable finance. Our authors also explore topics such as the impact of social change on the world of finance, the rise of artificial intelligence and virtual reality technologies, and cybersecurity.

Contributions in this edition come from a range of world-class experts across industry and academia, and showcase some of the very best expertise, independent thinking, and strategic insights within the financial services sector.

As ever, I hope that you find the latest edition of the Capco Journal to be engaging and informative. Thank you to all our contributors, and thank you for reading.

Lance Levy, **Capco CEO**

FOSTERING DIGITAL OPERATIONAL RESILIENCE IN THE FINANCIAL SERVICES SECTOR IN EUROPE (DORA COMPLIANCE)

ALEXANDRE VANDEPUT | Principal Consultant, Capco

ABSTRACT

The European Union (E.U.) wants to position itself as a world leader in digital innovation in the financial services industry. Subsequent to the digitalization of the provision of financial services to European consumers and businesses, new kinds of digital risks have emerged. To reach that set objective, the E.U. must make sure those key risks are properly controlled. DORA, which stands for Digital Operational Resilience Act, is the answer from the E.U. to the increasing use of ICT systems and third parties for financial institutions' critical operations. This paper explores the key actions that financial institutions will have to undertake to comply with DORA guidelines. The emerging risks will require mitigations such as an appropriate ICT risk management framework, a robust incident management process including classification and reporting, a digital operational resilience testing program, as well as an end-to-end third-party management control framework.

1. THE E.U. DIGITAL FINANCE STRATEGY

The digital finance strategy sets out general guidelines on how Europe can support the digital transformation of finance in the coming years, while regulating its risks. The strategy sets out four main priorities: removing fragmentation in the "digital single market", adapting the E.U. regulatory framework to facilitate digital innovation, promoting data-driven finance, and addressing the challenges and risks associated with digital transformation, including the digital operational resilience enhancement of the financial system.

Embracing digital finance would unleash European innovation and create opportunities to develop better financial products for consumers, including for people currently unable to access financial services. Boosting digital finance would, therefore, support Europe's broader economic transformation.

As digital finance speeds up cross-border operations, it also has the potential to enhance financial market integration in the banking and the capital markets sectors, and thereby strengthening Europe's economic and monetary union.

A strong and vibrant European digital finance sector would strengthen Europe's ability to reinforce its open strategic autonomy in financial services and, by extension, its capacity to regulate and supervise the financial system to protect Europe's financial stability and values.

The fourth priority of the "digital finance strategy" for the E.U. is to address new challenges and risks associated with the digital transformation.

Europe and its financial services sector must embrace all the opportunities offered by the digital revolution. Europe must drive digital finance with strong European market players in the lead. The aim is to make the benefits of digital finance available to European consumers and businesses. And finally, Europe should promote digital finance based on European values and a sound regulation of risks.

At the same time, innovation is changing market structures. Europe is home to many successful fintech startups. Incumbent firms are fundamentally overhauling their business models, often in cooperation with those fintech companies. Technology companies both large (bigtech) and small are increasingly active in financial services. These developments are not only changing the nature of risks to consumers, users, and financial stability, but may also have a significant impact on competition in financial services.

Financial services migrate to digital environments with fragmented ecosystems, comprising interconnected digital service providers falling partially outside financial regulation and supervision. Digital finance may, therefore, make it more challenging for the existing regulatory and supervisory frameworks to safeguard financial stability, consumer protection, market integrity, fair competition, and security. These risks must be addressed to ensure that digital finance enables better financial products for consumers and businesses. The E.U. will, therefore, pay particular attention to the principle of "same activity, same risk, same rules", not least to safeguard the level playing field between existing financial institutions and new market participants. This principle will also apply to another key category of controlled entities, the "critical third-party providers" (CTPPs), which will be controlled as any other financial institution.

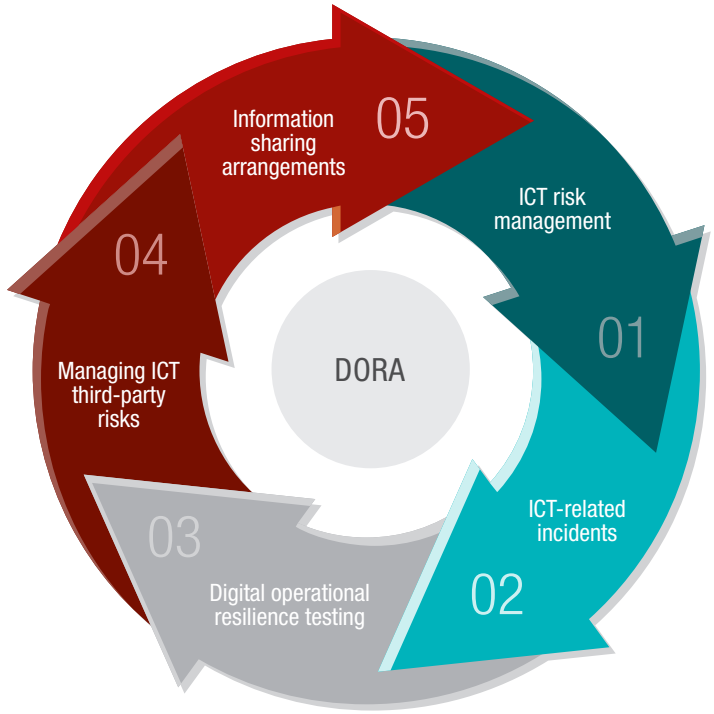
By setting up the Digital Operational Resilience Act (DORA) initiative, the E.U. wants to remediate the current situation:

- the heterogeneity and disparity of ICT (information and communication technologies) security rules out of operational resilience requirements across the E.U. financial services legislation
- the absence of requirements or a multiplication of obligations on the reporting of the same ICT incident to different authorities
- a diversity of digital operational resilience testing frameworks
- a lack of coherent oversight over the activities of third-party providers to financial sector entities.

In response, the E.U. has defined the following five pillars of DORA:

1. ICT risk management
2. ICT incident reporting
3. Digital operational resilience testing
4. ICT third-party risk management
5. Information and intelligence sharing.

Figure 1: DORA five key pillars



2. MAIN PRACTICAL REQUIREMENTS OF DORA

Digital operational resilience is the ability to build, ensure, and test the technological operational integrity of an organization. It ensures that an organization can continue to guarantee the continuity and quality of its services in the face of ICT operational disruptions.

The regulation delivered by the E.U. focuses on harmonizing national rules around operational resilience and cybersecurity. DORA establishes uniform requirements for the security of network and information systems of companies active in the financial services industry as well as critical third parties that provide services related to ICT, such as cloud platforms and data analytics services. DORA creates a regulatory framework in digital operational resilience whereby all in-scope companies will have to make sure they can withstand, respond, and recover from all types of ICT-related disruptions and threats.

DORA will apply to financial entities including credit, payment, and e-money institutions, investment firms, crypto asset service providers and issuers of asset-referenced tokens, central securities depositories, central counterparties, trading venues, trade repositories, managers of alternative investment funds and management companies, data reporting service providers, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries, institutions for occupational retirements pensions, credit rating agencies that administrate critical benchmarks, crowdfunding service providers, and securitization repositories. DORA will also apply to ICT third-party service providers designated as "critical" ICT services providers to financial entities (called "critical ICT third-party providers", or CTTPs) through a newly created established oversight framework. The criticality of those third parties will be a function of different parameters: their systemic impact on the stability, continuity, and quality of financial services in the event of a failure, the systemic character of financial institutions relying on them, the degree of reliance of those financial institutions in relation to "critical or important functions" (CIFs) of those institutions, and finally, the degree of substitutability of the ICT third-party provider.

The regulation imposes new requirements divided into five domains or pillars. Some of the requirements imposed by DORA, such as for ICT risk management, are already reflected to a certain extent in existing E.U. guidance; for example, the EBA Guidelines on ICT and security risk management.

It is well understood that the principle of proportionality fully applies to DORA requirements. The degree of applicability of those requirements to the financial institutions will be a function of risks and needs applicable to their specific characteristics in terms of their size and business profiles. The proportionality principle is embedded in the rules of each DORA pillar.

In addition, there are many reasons why the E.U. has opted for a regulation instead of a directive, including the fact that the use of a regulation reduces the regulatory complexity by fostering supervisory convergence – it increases legal certainty while limiting compliance costs. This reduces competitive distortions overall. Consequently, a regulation appears to be the ideal compromise to guarantee a homogeneous and coherent application of all components of the ICT risk management guidelines applied to the E.U. financial sector.

DORA is Lex Specialis with regards to another interrelated Directive focusing on cybersecurity, NIS2.[1] Both entered into force at the end of December 2022, but NIS2 will be applicable three months before DORA. NIS2 is a horizontal legislation, focusing on critical sectors like transport, water distribution, telecom, and healthcare, as well as banking, while DORA is a vertical legislation focusing on financial services only. There are some overlaps between the two legislations, but DORA being Lex Specialis will get priority over NIS2 in cases where both set of rules would regulate the same topic.

As already mentioned, DORA regulation is divided into five pillars, which are described in more detail below.

2.1 Pillar I – ICT risk management

All in all, the key focus of the first pillar is to identify the crown jewels, or critical assets of a financial services firm, and putting in place the necessary ICT risk controls framework to make sure they are properly, and always, protected against all kinds of digital risks.

[1] Network and Information Security Directive (NIS2) is the second set of measures for a high common level of cybersecurity across the Union.

Consequently, firms must identify their "critical or important functions" (CIFs) and map their assets and dependencies, as well as the data that flow through those assets. Firms will need to conduct "business impact analyses" (BIAs) to identify their exposure to severe business disruptions. As a prerequisite, firms will need to set risk tolerances for ICT disruptions supported by key performance indicators and risk metrics.

Alongside this framework, entities will have to use and maintain ICT systems that meet requirements so as to promptly detect anomalous activities, identify all sources of ICT risks on a continuous basis, design and implement security and threat-prevention measures, and promptly activate response and recovery measures. On top of that, there will be a need to identify useful data, through incident reporting, post incidents reviews, and active monitoring, to understand the evolution of cyber risks and support management to shape digital resilience strategies.

Financial institutions are required to create and maintain a sound, comprehensive, and well-documented ICT risk management framework. This must include a dedicated and comprehensive business continuity policy, disaster recovery plan, and communication policy. Institutions shall implement an "information security management system" (ISMS) based on recognized international standards.

At the communication level, it will be required to establish a communication strategy and related planning to actively inform European supervisory authorities[2] (ESAs), clients, and counterparties, as well as the public, on matters related to their cyber threats and incidents.

2.2 Pillar II – ICT-related incidents

DORA will harmonize and streamline the reporting of ICT-related incidents. This obligation is split in three main requirements. The first is to make sure that financial institutions establish and implement a management process to monitor and log ICT-related incidents, as well as implementing early warning indicators. Secondly, financial institutions will have to classify ICT-related incidents and report "significant" ICT-related incidents to a central E.U. hub. Only ICT-related incidents that are deemed major must be reported to the competent authorities. Finally, financial institutions should submit initial, intermediate, and final reports to the competent authorities, and must inform their users and clients where the incident has, or may have an impact on their financial interests. Cyber threats will be reported on a voluntary basis only. There will be a need to assess the effectiveness of the post-incident review and thematic analysis capabilities to learn from disruptions and to anticipate and avoid future incidents.

2.3 Pillar III – Digital operational resilience testing

Two types of testing will have to be implemented. The first will apply to all financial institutions and will cover a full range of tests, including vulnerability assessments and scans, open-source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews, scenario-based tests, compatibility testings, performance testings, and end-to-end testings or penetration testings.

The second type will apply to financial entities identified as "significant" or "systemic" by the competent authorities. Those tests will be based on the "threat-led penetration testing" (TLPT) model, will have to happen every three years, will need to be delivered by an external entity, and their results will be formalized in an attestation.

Financial institutions will be required to conduct regular digital operational resilience testings by independent internal or external parties. This comprehensive digital operational resilience testing program will be done in consideration of the proportionality principle. Hence, no internal tester will be allowed for systemic institutions, the threat intelligence will always be delivered by an external party. This program should include a range of assessments, tests, methodologies, practices and tools, procedures, and policies to prioritize, classify, and remedy defects and ensure all are fully addressed. Threat-led penetration testing should be developed in line with the ECB's existing TIBER-E.U. framework.[3]

TIBER-E.U. framework is the current framework that delivers a controlled, bespoke, intelligence-led red team test of entities' critical live production systems. Intelligence-led red team tests mimic the "tactics, techniques, and procedures" (TTPs) of real-life threat actors who, on the basis of threat intelligence, are perceived as posing a genuine threat to these entities. An intelligence-led red team test involves the use of a variety of

[2] European Banking Authority (EBA), European Insurance and Occupational Pensions Authority (EIPOA), and European Securities and Markets Authority (ESMA)
[3] European framework for threat intelligence-based ethical red-teaming.

techniques to simulate an attack on an entity's critical and important functions and underlying systems, meaning its people, processes, and technologies. It helps an entity assess its protection, detection, and response capabilities.

A test completion attestation will be issued, together with a summary of the relevant findings and remediation plans. There is a possibility for pooled TLPT for ICT critical TPP (CTPPs) providing the same service is provided to several financial institutions.

2.4 Pillar IV – Managing third-party risks

DORA will prescribe strict content requirements for contracts between financial entities and ICT third-party service providers.

These elements cover minimum aspects deemed crucial to enable complete monitoring by the financial institution of ICT third-party risk throughout the conclusion, performance, termination, and post-contractual stages of their relationship.

Here, key building blocks of third-party or supply chain management framework are described.

There is a need to develop a structured third-party engagements register. Financial institutions can start by leveraging their actual outsourcing register, as this was already needed to comply with the EBA Guidelines on Outsourcing, which came into force in September 2019, while making sure that the relevant fields are added in order to reflect DORA compliance scope. Indeed, the scope now includes not only intra- and extra-group outsourcing engagements but also all third parties, which is a much broader scope.

The focus of DORA is not outsourcing versus non-outsourcing but on the level of materiality, or criticality of the supplier, instead. This exercise is done through the lens of the service receiver, and the register needs to be considered from a legal entity standpoint. Furthermore, financial institutions will need to make sure that all critical sub-contractors are properly identified. More specifically, entities are to engage in an in-depth analysis of sub-contracting arrangements, especially when concluded with ICT third-party providers established in a third country.

For critical or important functions, financial institutions must assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions, and the competent authority's ability to effectively supervise the institution. The only contractual requirements relating to subcontracting set out in DORA are for the contract to specify whether subcontracting is allowed, the conditions thereof, and the locations of subcontracting functions, services, and data processing activities.

On the contractual side, DORA sets out several requirements for contracts between financial institutions and ICT third-party suppliers. These will impact existing and new contracts. There will be more extensive requirements applying to those contracts that support critical or important functions. Again, the contractual requirements are closely aligned to the EBA Guidelines on outsourcing arrangements. Financial institutions will have to ensure that those contractual agreements include the locations where data is processed, as well as the service level descriptions accompanied by qualitative and quantitative performance targets, the reporting obligations, the rights of audit and access, and the circumstances in which such contracts must be terminated.

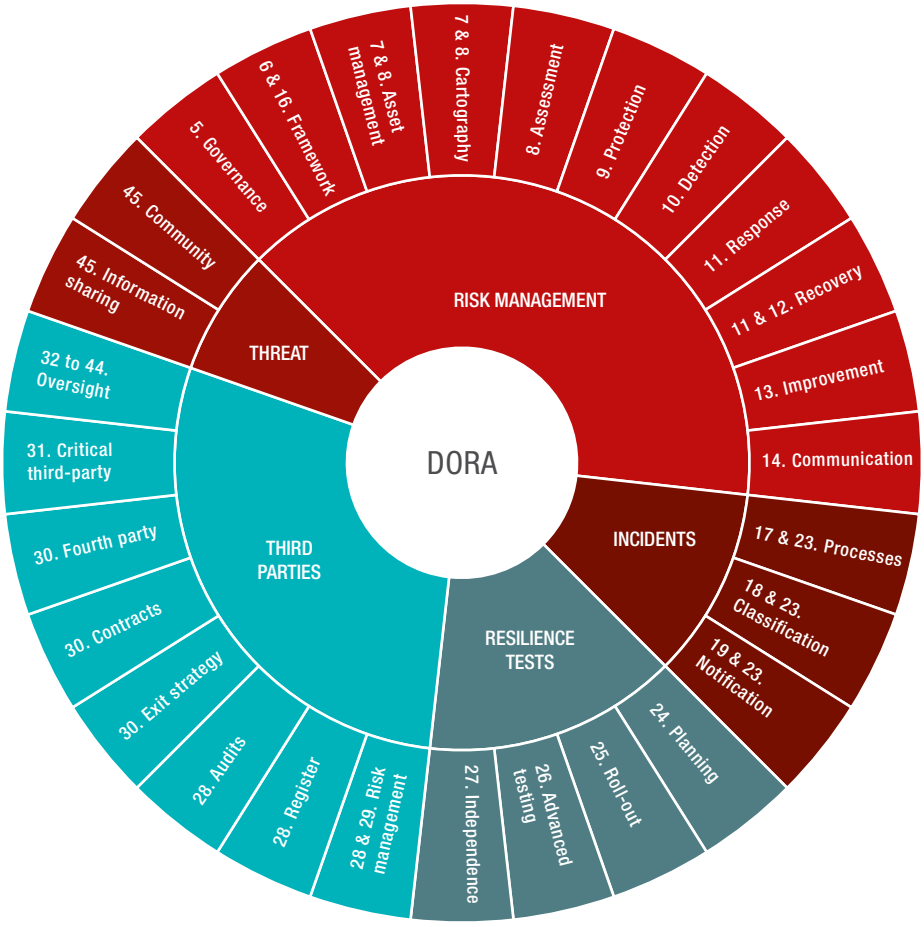
Contracts with third parties will need to include personal data-related provisions on accessibility, availability, integrity, security, and protection of personal data, and guarantees for access, recover, and return in the case of failures of the ICT third-party service provider, as well as clear termination rights and dedicated exit strategies.

As a preliminary assessment, firms will have to conduct concentration risk assessments of all contracts with ICT third parties that support the delivery of critical or important functions (CIFs). This will be based on a substitutability assessment, as well as taking into account multiple contractual agreements in relation to the provision of services with the same ICT third-party provider or with closely connected ones. On that note, the adoption of a multi-vendor approach is considered as recommended, but optional, in order to demonstrate a credible resilience framework.

The regulation seeks convergence on supervisory approach regarding ICT third-party risk in the financial services sector by subjecting critical ICT third-party service providers (CTTPs) to an E.U. oversight framework. To that end, the E.U. has developed a new harmonized legislative framework that will grant new and substantial supervisory powers to newly designated ESA as "lead overseer" in order to adequately monitor critical third parties at a pan-European scale.

CTTPs that do not as yet have a subsidiary in the E.U. will have 12 months to do so in one of the member states.

Figure 2: Main DORA topics and articles applying to financial institutions



2.5 Pillar IV – Information sharing agreement

DORA will allow financial institutions to exchange cyber-threat information and intelligence among themselves and with the ESAs. The key focus here will be to raise awareness about ICT risk in the financial services sector and to minimize the impact of ongoing and upcoming threats. The principle will be a voluntary exchange amongst financial institutions of cyber-threat information and intelligence in trusted communities. Elements that could be reported are indicators of compromise, tactics and techniques, and cybersecurity alerts.

3. ENFORCEMENT

The proposal has passed through the E.U.'s ordinary legislative procedure. The draft law adopted by the European Commission on September 24th, 2020, was submitted to the European Parliament for review and approval on November 10th, 2022. The final version of the text was finally approved by the Council on December 14th, 2022. The text was then published in the Official Journal of the European Union on December 27th, 2022. Finally, after 20 calendar days, DORA entered into force on January 16th, 2023. DORA will, therefore, apply as of January 17th, 2025, after the transitional period of 24 months. Regulatory Technical Standards (RTSs) and Implementation Technical Standards (ITSs) guidelines will be issued subsequently.

4. NEXT STEPS

Financial institutions that currently fall within the scope of the European Commission should assess the gaps between their operating models and the expanded regulations and should then start to plan accordingly to adapt to the upcoming changes.

To be prepared, we recommend that organizations take the following steps:

1. **Act now to improve your operational resilience awareness:** involve general staff and senior management. This is not a tick-box exercise, as it needs to focus on the full scope of DORA and encompassing its organizational, technology, and processes impacts.

2. **Follow-up on level 2 texts that will define RTSs and ITSs:** those elements will be delivered jointly by all involved ESAs[4] in a time period spanning 12 to 24 months after the effect date of DORA. Of course, one should not wait for the full disclosure to take place, as there are still a lot of requirements that are clearly defined. Additionally, financial institutions will have some kind of flexibility to leverage existing capabilities. For instance, financial institutions can start leveraging the ongoing work on consolidated and sub-consolidated registers of information for all ICT third-party providers, as well as material subcontractors, as it is currently imposed by the EBA guidelines on outsourcing. Another example is the process of ICT incident management that can be fully harmonized with already existing processes dedicated to PSD2 or GDPR incident reporting.

3. **Perform a maturity assessment against DORA requirements:** with associated gap analysis and mitigation plans related to policies, procedures, processes, and capabilities to reach compliance. Gap analysis needs be done for the five pillars of DORA. First and foremost, at the ICT risk management level, where the overall existing governance, the organization, and the ICT risk control framework will be mapped against the obligations as set forth in DORA. Then, there is a need to have a thorough look at the detection, management, and classification of ICT-related incidents and potential cyber threats, as institutions will have the possibility to report them on a voluntary basis. On that level, the need is to assess the impact and root causes of those incidents, as well as defining the communication plan. The resilience testing program will be analyzed, where a risk-based approach will be adopted, taking into account the proportionality principle and adequate consideration of evolving ICT risk landscape, the criticality of assets, and services provided. Firms will define the range of assessments, test scenarios, methodologies, practices, tools, and external parties needed to support digital operational resilience testing programs. At the level of third-party management, there is a need to have a close look at the strategy and policies to put in place, the assessment practices, the exit strategies and plans, as well as the contractual terms. And finally, when working on the information and intelligence sharing model to put in place, the confidentiality and data protection aspects will be key.

4. **Make provisions for budgetary planning:** in accordance with the proportionality of the estimated efforts needed to apply the required changes. As those budgetary cycles are quite often long, it is important to start aligning early with the required stakeholders able to define the best delivery approach. At that stage, alignment will be needed with the IT and transformation teams on a transversal and end-to-end perspective. However, before doing this, we recommend working on a clear and robust DORA compliance implementation roadmap. This exercise should include a project plan and the necessary capacity planning.

5. **Adopt one standard to assess your controls maturity:** if we take a step back, one should consider the full scope of compliance that any financial institution is currently facing. We previously mentioned NIS2, which has also come into force.[5] From an information security risk framework, entities are often applying different standards according to their risk appetite, risk perimeter, and risk culture. Our approach is to encapsulate all controls into the prominent ISO 27000 set of standards. We noticed that financial institutions are facing multiple regulatory obligations: they need to comply with different standards (PCI-DSS[6] for payments-related activities, for example) and they are facing a number of binding guidelines, such as EBA's on outsourcing and on ICT and security risk. We advise firms to consider all those and formalize the right level of control into the ISO 27002 controls set. Any remaining requirements need to be taken care of separately. For example, the digital operational resilience testing requirements cannot fit into this framework. Consequently, they need to be considered independently.

[4] European Supervisory Authorities, composed of the EBA, the ESMA, and the EIOPA.
[5] NIS2 will be transposed into national laws in October 2024
[6] Payment Card Industry – Data Security Standard

6. **Ensure your current controls are properly implemented:** based on our observations, lots of key ICT-related controls can still be further improved and integrated into the overall ICT risk management framework of financial institutions. For example, building and maintaining core IT competences could be necessary, also at the board level. The management of ICT risks may still be underestimated and poorly applied, like on roles and responsibilities or in terms of risk treatment and monitoring levels. The classification of IT assets, including related data, and configuration management is too often neglected. There is often no clear alignment with IT security best practices, like on monitoring and detection capabilities, prevention of data loss, system hardening, end-of-life systems management, privileged access management, segregation of duties, or exit plans. Furthermore, we see too many end-user computing applications that require close attention and can generate data leakage issues. There is quite often inadequate experience with IT continuity and security testing, which requires a complete and end-to-end view on prior identification of impacted systems chains.

5. CONCLUSION

The E.U., with its "digital finance package", wants to foster competition and innovation in the financial services sector, by giving consumers access to innovative financial products while ensuring consumer protection and financial stability. One of the main priorities of the digital finance strategy is enhancement of the digital operational resilience of the financial system. DORA was designed to mitigate risks arising out of the ever-increasing dependency of the financial services sector on software and digital processes. In this paper, we extensively explained what the key focus areas of this regulation are, by describing the key actions that banks and other financial institutions need to implement from an ICT risk management framework, incident and testing management, as well as how they will manage third parties in the future. Just as importantly, how they will share information among themselves to make the E.U. a more secure place, where competition and innovation can grow in a controlled and positive environment, for all.

ABOUT CAPCO

Capco, a Wipro company, is a global technology and management consultancy focused in the financial services industry. Capco operates at the intersection of business and technology by combining innovative thinking with unrivalled industry knowledge to fast-track digital initiatives for banking and payments, capital markets, wealth and asset management, insurance, and the energy sector. Capco's cutting-edge ingenuity is brought to life through its award-winning Be Yourself At Work culture and diverse talent.

To learn more, visit www.capco.com or follow us on Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Dubai
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
a wipro company