ECIIA

THE DIGITAL OPERATIONAL RESILIENCE ACT AND ITS IMPACT ON INTERNAL AUDIT IN THE FINANCIAL SERVICES

TABLE OF CONTENTS

01. MANAGEMENT SUMMARY

The Digital Operational Resilience Act (DORA) is the European Union's (EU) strategic approach to managing systemic risk within the financial system*. DORA specifically addresses the digital operational resilience of Financial Institutions (FIs) and their supply chains by introducing dedicated operational resilience risk management requirements. These include technical measures, procedures, processes, and real-life testing to support FIs in detecting anomalies, containing cybersecurity incidents, and recovering from them. The new requirements are a regulatory response to increasing cybersecurity threats.

DORA provides the financial sector the opportunity to further improve and broaden operational resilience. Harmonizing IT cybersecurity requirements, coupled with a 'lex specialis' approach, aims to streamline and prevent the duplication of efforts. Furthermore, improving oversight and alignment of audits in this area can prevent multiple independent audits of the same critical ICT (Information and Communication Technologies) infrastructure provider by various FIs.

A critical attention point is the harmonization, or at least the mutual acceptance, of similar regulatory standards in other jurisdictions.

Implementing DORA may be challenging as several technical details and implementation standards (Regulatory Technical Standards, RTS) are still to be defined. ESAS currently consults on the first batch of DORA policy products. It is mainly the responsibility of the first and second line.

Internal audit functions will need to start early to assess and prepare changes to their audit programs and practices to meet DORA (*) requirements.

02. INTRODUCTION

Financial Institutions (FIs) efforts to digitally transform core products and processes have led to extensive use of Third-Party Providers (TPPs) for ICT-related services. These include among others cloud or transaction services and platforms. Managing the risks related to working with TPPs has always been crucial and today's volatile geopolitical and cybersecurity threat landscape only reinforces this. Even if the critical infrastructure of Western countries has not yet been significantly affected, state-backed and criminal attacks are expected to increase. Consequently, the necessity to address potential vulnerabilities and strengthen operational resilience against all types of ICT-related disruptions and threats will only become more important.

It is also important to mention that EBA updated the guidelines on outsourcing arrangements a few years ago.**

**These Guidelines provide a clear definition of outsourcing and specify the criteria to assess whether or not an outsourced activity, service, process, or function (or part of it) is critical or important.

KEY MESSAGES FOR INTERNAL AUDIT

DORA is designed to harmonize regulatory requirements, improve resilience against cybersecurity risks, and strengthen the management of concentration risks to critical Third-Party Providers(TTPs).

For Internal Audit (IA) functions, operational resilience assurance has already been incorporated into audit programs. Still, DORA and its associated international regulatory efforts do require targeted reviews and enhancements of audit plans and work programs

The need to adequately identify and manage concentration risks, especially those to critical TTPs, increases even further. Challenging and enhancing existing approaches and processes will be key

IA functions should align with the new critical TTP lead overseer on their scope and approach to identify potential overlaps or blind spots in their own audit plans and work programs.

With some technical specifications still in discussion and to be determined, FIs may have six months or less to implement all Regulatory Technical Standards (RTS). As a result, an early start by FIs to review and challenge the businesses' self-assessment activities is paramount to ensure that vulnerabilities are remediated timely.

03. DORA & THE SYSTEMIC OPERATIONAL RISKS

In 2017, the Cyber Expert Group (comprised of G7finance ministers and central bank governors) stated that "**there is an understanding that disruption will occur.**" (1)

This marks a fundamental mind-shift as the going position is that disruptions cannot be avoided and will occur at some point in time. The basic tenant of DORA therefore is to minimise the impact of disruptions to critical business operations, rather than only trying to prevent these from occurring. This change of approach also provides a broader range of mitigating measures. Maintaining control, even in the case of an incident, and the ability to recover timely are the major objectives of resilience instead of the unrealistic expectation to achieve a zero-failure environment.

The European Commission's (EC) concerns regarding European companies' growing dependencies on TTPs, often based outside of EU jurisdiction, resulted in the "European Digital Sovereignty" paper. While the paper recognizes the need to use state-of-the-art ICT services, European companies also need to comply with provisions to address the risk of dependencies on TTPs and external interference on these. A foundation for strengthening European digital sovereignty is to increase the resilience of EU companies and governments regarding cybersecurity threats. DORA is part of this overarching strategy and in particular addresses the operational resilience aspect.

DORA should be considered as an opportunity for the financial sector

The first key objective of DORA is the harmonization of the regulatory requirements for IT security. To achieve this, existing national and European requirements such as the European Banking Supervision'sguidelines on IT security, the Threat Penetration Testing Framework (Tiber-EU), and the Directive on Network and Information Security (NIS 2) will be consolidated in a single, uniform, set of requirements. This will avoid the duplication of requirements and reduce bureaucracy for FIs to meet operational resilience requirements and security standards. **Secondly, DORA is designed to improve the resilience of FIs against risks resulting from cyber-attacks** which can scale up dramatically with a global reach.

The "Log4J" vulnerability in the widely used JAVA programme library, in December 2021, is an example of risk resulting from the ubiquitous use, and concentration, of software libraries and systems. As these types of incidents are often unavoidable, preventive measures alone are not sufficient and DORA requires effective measures to detect, manage, and recover from ICT incidents. DORA will help FIs to prepare for a robust incident response when dealing with cyber-attacks.

Managing risk due to the concentration of FIs supply chains (TTPs) is a third objective. The ubiquity of sourcing has dramatically changed the threat landscape of the financial sector as the risks posed by cyber-attacks to TTPs directly affect those FIs serviced by them. Furthermore, the concentration of IT sourcing among a few 'big tech' companies providing cloud services, mobile platforms, payment, and credit card processes further exacerbates this as a disruption to a TTP can impact several FIs at the same time. To address this, DORA will establish a direct oversight framework for all critical ICT TPPs, with designated European Supervisory Authorities (ESA) acting as the "lead overseer".

This direct oversight offers a great opportunity to make the oversight regime more effective and efficient for all by pooling and leveraging audit activities of FIs towards TPPs. Currently, the same standard services of ICT TPPs are audited by various internal and external auditors and their responsible NCAs (National Competent Authorities) separately.

DORA and the Three Lines Model

DORA (art 5) calls for financial entities to structure ICT risk management according to the Three Lines model or similar internal risk management and control models. Appropriate segregation of duties must be implemented:

1. ICT management, responsible for the implementation of the management system and business advisory
2. Control and oversight of ICT risks, responsible for governance model, management system, and compliance including reporting to the board
3. Internal audit in charge of assurance about ICT risk-related matters

The way forward: Regulatory Technical Standards (RTS) will shape the DORA implementation

With DORA, uniform requirements will apply throughout the EU. To achieve this, existing national regulations may need to be adapted to achieve alignment and avoid redundant or contradictory requirements. This may be challenging given the scope of DORA which aims to cover all aspects of IT security as well as the related areas of information and cyber security within the financial sector.

The responsible national financial authorities for banking supervision have the task of ensuring that requirements are aligned to deliver a single, uniform piece of legislation.

The above will need to be completed by January 2025. While the final DORA text (2) was published in the Official Journal of the EU on December 27, 2022, and became effective as of January 16, 2023, not all legal details have been settled yet. The ESAs (including ESMA, EBA, and EIOPA) are tasked to present the Regulatory Technical Standards (RTS) to the EC. Some of these RTS need to be drafted within 12 months, with the remainder to be delivered within 18 months. As a result, timelines to implement DORA fully by January 2025 may be challenging as FIs may have less than six months to implement those RTS which in parts still need to be defined. Starting early, monitoring progress, and ensuring resources for implementing DORA in time are critical.

Operational resilience as a global regulatory priority (3)

As there is a general understanding globally that disruptions will occur, strengthening operational resilience is not just a priority for the EU but rather a global priority for all regulators. Regulatory authorities in the U.S., U.K., Singapore, and China, among others, have recently enhanced or are in the process of enhancing their legislation. The following focus areas for regulatory attention are apparent: 1) End-to-end process view and value chain focus, 2) Identification of (critical) Third-Party Providers, 3) Immediate incident reporting and information sharing, and 4) Preparation for disruptions.

While there seems to be a common understanding of how to achieve operational resilience, international efforts still show differences in levels of maturity as well as design and implementation across the regional jurisdictions. Given that most European FIs are either directly or indirectly connected to jurisdictions outside the EU, it is important to align technical standards globally.

04. STRATEGIC IMPACT ON INTERNAL AUDIT

Providing assurance on operational resilience is not new and is part of most standard audit programs. Having an end-to-end overview of business processes, including the involvement of(critical) TPPs, is a foundation of risk-oriented audit programs and audit cycles. Aspects such as Business Continuity Management, Incident Management, TPP Risk Management, and Cyber Resilience Testing are regularly covered by audit and the focus on continuous improvement regards methodology and techniques reflects the growing importance of these. For Third Party Risk Management, the right to access and audit are included in standard legal frameworks and pooled audit approaches have been established. The Collaborative CloudAudit Group is an example of a pooled audit approach towards 'big tech' cloud providers. In addition, Cyber Resilience Testing audit functions are ideally integrated into industry-wide testing activities like TIBER.

DORA and its associated international regulatory efforts will require Internal Audit (IA) functions to review and possibly enhance their audit plans and work programs. Most importantly, the need to adequately identify concentration risks to ICT service providers will increase even further as it will ultimately determine the exposure of an FI to the respective critical ICT TPPs. Accordingly, IA functions should challenge established concentration risk processes, particularly on the approach and data used to identify potential critical TPP exposures through 4th party providers. Moreover, it will be important to see whether, and to what extent, IA functions may rely on the work of the newly established lead overseer for each individual critical TPP and evaluate potential overlaps or blind spots in the audit approaches and plans. It will be interesting to see, what the final definition of critical TPPs will be as it will affect the number and ultimately degree of exposure of FIs to critical TPPs. Another important question is whether, and to what extent, pooled audit approaches may be applied to other critical TPPs than those providing cloud services, leveraging the experience gained with the cloud services industry. With increased attention to sourcing constructions (TTP or 4th party), a thorough analysis of existing audit and follow-up approaches is required whether these are still suitable moving forward.

Possible internal audit assurance strategies

In addition to the strategic view, IA functions should also act as a change facilitator by designing and implementing an assurance approach whilst maintaining independence. In particular, the extensive knowledge of existing end-to-end business processes and understanding of the complex international regulatory environment may add direct value to FIs' respective implementation projects.

Accordingly, IA functions should review the approach taken to identify and prioritize Important Business Services (IBS) and whether the most critical resources, technologies, and third parties involved are adequately mapped. Based on that, it will be important to assess how potential vulnerabilities are identified as well as to challenge the criteria and data used to define impact tolerances for each IBS. Given DORA's emphasis on preparing for incidents, IA functions should pay extra attention to evaluate the designs of the different types of scenario testing, and whether their results are translated into lessons learned and remediation plans. It will be key to closely monitor the timely remediation of these vulnerabilities and update respective incident and crisis management processes.

"Resilience is a matter of capabilities, not plans" (4)

The implementation of DORA and its associated international efforts is not a paper exercise. Preparing for critical cyber incidents requires training and exercises (drills) with participation from senior management security operation teams and business functions.

Most importantly, DORA requires well-designed standards (RTS) to achieve technical implementation and continued, active political support across the EU and member states. Engagement and cooperation between the National Competent Authorities and FIs is essential to achieve this.

05. APPENDIX

(*) DORA in a nutshell

1. What is the aim?
DORA creates a regulatory framework on digital operational resilience whereby all firms need to make sure they can withstand, respond to, and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states.

2. Who is impacted?
More than 22,000 financial institutions and ICT service providers based in the EU will be subject to DORA. In short, all financial market participants - including banks, investment companies, insurance companies and intermediaries, data reporting providers, and cloud service providers - will be subject to the regulatory framework introduced by DORA.

3. What are the obligations?
DORA consists of 5 pillars that layout requirements and expectations for different aspects of operational resilience

ICT Risk Management Framework and Governance

Set up a comprehensive ICT Risk management Framework, based on key performance indicators and risk metrics. The Framework must be continuously monitored and include:
-Set up and maintain resilient ICT systems and tools that minimize the impact of ICT Risks.
-Map ICT assets and dependencies; identify critical or important functions
-test regularly BCM, DR activities

ICT Incident Management and Reporting

Classify and report on ICT-related incidents based on novel classification and reporting framework:
-Implement an ICT-related incident management process
-Assess the quantitative impact of ICT incidents and analyse root causes
-Submit a report to the competent national authority (based on RTS)

Digital operational resilience testing

Implement a proportional and risk-based digital operational resilience testing programme:

-Conduct annually advanced security and resilience tests on critical ICT systems and applications

-Eliminate any vulnerability, or deficiency through the implementation of mitigation measures

-Conduct periodically advanced Threat-Led Penetration Testing for critical or important functions

ICT Third-party risk management

Implement Third Party Risk Management Requirements including:

-Conduct concentration risk assessments of all outsourcing contracts that support the delivery of critical and important functions

-Ensure that the contracts with the ICT third-party providers contain all the necessary monitoring and accessibility details and binding contractual terms

-Critical ICT third-party service providers will be subject to a Union Oversight Framework

Information Sharing

Share with each other cyber threat information and intelligence, in line with the existing TIBER-EU Framework

-The Supervisory authority will provide relevant anonymized information and intelligence

4. What is the implementation timeline?

The act was published on 27 December 2022 and came into force on 16 January 2023. There is an implementation period of 24 months à The applicability starts on 17 January 2025.

The DORA package delegates significant decision-making authority to the ESAs and the RTS will be crucial to understand the full spectrum of requirements from DORA.
The first consultation on RTS has been launched in July 2023.

To operationalize the application, DORA mandates the European Supervisory Authorities (ESAs) to prepare jointly, through the Joint Committee (JC), a set of policy products with two main submission deadlines: 17 January 2024 (first batch) and 17 June 2024 (second batch). More information here.

06. ABOUT

Thank you

This paper was prepared by the Commerzbank team, in collaboration with the ECIIA Banking Committee. We would like to thank the authors, Verena Bitter, Stefan Stein& Dr. Boris Hemkemeier for their expertise. We also thank Keith Raper from ING, for his review.

About ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin. The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence. The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight.

About ECIIA Banking Committee

ECIIA set up a Banking Committee1 in 2013 with Chief Audit Executives of the largest European Banks, supervised by the ECB. The mission of the ECIIA Banking Committee is: "To be the consolidated voice for the profession of Internal Audit in the Banking sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at the European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Banking Sector in Europe ». ECIIA represents around 55.000 internal auditors and around 15.000 are active in the banking sector.

References

((1)G7 Fundamental Elements for Effective Assessment of Cybersecurity in the financial sector | Deutsche Bundesbank[SS1]
(2)EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu) [SS2]
(3) U.S.: Interagency Guidance on Third-Party Relationships: Risk Management (Federal Register :: Interagency Guidance on Third-Party Relationships: Risk Management); FED, FDIC & OCC interagency paper "Sound Practices to Strengthen Operational Resilience" (The Fed - SR 20-24: Interagency Paper on Sound Practices to Strengthen Operational Resilience (federalreserve.gov)) U.K.: BoE, PRA & FCA interagency policy and supervisory statement "Operational resilience: Impact tolerances for important businessservices" (SS1/21 'Operational resilience: Impact tolerances for important business services' (bankofengland.co.uk))
Singapore: RevisedMAS guidelines on Technology Risk Management (Guidelines on Risk Management Practices – Technology Risk (mas.gov.sg)) and Business Continuity Management (Guidelines on Business Continuity Management (mas.gov.sg)); "Information Paper on Operational Risk Management –Management of Third Party Arrangements (Operational Risk Management - Management of Third Party Arrangements (mas.gov.sg))"
China: CBIRCRules on InformationTechnology Outsourcing Risks of Bankingand Insurance Institutions (国家金融监督管理总局 (cbirc.gov.cn)) and CAC Cybersecurity Review Measures (网络安全审查办法-中共中央网络安全和信息化委员会办公室 (cac.gov.cn))[SS3]
(4)Phil Venables"Risk and Cybersecurity" 2020 (Resilience is about Capabilities not Plans (philvenables.com))

Avenue des Arts 41
1040, Brussels—Belgium
TR: 849170014736652