SAI360

EBOOK

EU's Digital Operational Resilience Act: Your guide to ICT risk management

"DIGITALIZATION AND OPERATIONAL RESILIENCE IN THE FINANCIAL SECTOR ARE TWO SIDES OF THE SAME COIN."[1]

The European Commission (EC) has expressed its desire to ensure Europe is “fit for the digital age” by granting consumers access to innovative products while ensuring consumer protection and financial stability. Ultimately, the EC wants to not only embrace the digital revolution but drive it with innovative European firms at the forefront, making the benefits of digital finance available to all consumers and businesses.

The EC does, however, acknowledge the importance of balancing digitalization with risk mitigation measures, and its broad Digital Finance Package[2] includes a range of supporting proposals on crypto-assets and digital resilience. European financial services, like many other industries, are growing increasingly reliant on digital technologies, and while these solutions facilitate a more accessible, inclusive and efficient financial system, the resulting opportunities enjoyed by firms create a myriad of opportunities for bad actors probing for vulnerabilities. If found, these can be especially impactful given the highly sensitive nature of personal financial data and the general importance of financial services in our daily lives.

Research from IRONSCALES[3] shows an 81% increase in email phishing attacks since March 2020 with a lack of awareness of, and preparedness for, cyber threats existing as primary contributors. Such threat statistics should resonate with firms and highlight the need for operational resilience to be a business-led and business-owned initiative. The consequences of missing the mark on operational resilience can make or break a business, causing tremendous financial losses, reputational damage and regulatory fines. However, institutions have generally been slow to address IT-related business continuity.

1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

2 https://finance.ec.europa.eu/publications/digital-finance-package_en

3 https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/

EU DORA

The Digital Operational Resilience Act (DORA), approved in 2022 for enforcement in 2023/24, introduces EU-wide laws to ensure the operational resilience of the financial services industry. The proposal builds on existing Information and Communications Technology (ICT) risk management requirements established by various EU institutions and combines recent EU initiatives into a single regulation.

While changes to EU financial services legislation implemented in response to the 2008 financial crisis introduced a single rulebook governing large parts of the financial risks associated with financial services, they failed to fully address digital operational resilience. For example, they were often devised as minimum harmonization directives or principles-based regulation such as 'Shaping Europe's digital future' and 'A European strategy for data', as well as the EC's 2020 report on Digital Finance. Broader directives and strategies include the Directive on Security of Networks and Information Systems (NIS) Directive, European Critical Infrastructure (ECI) Directive and Security Union Strategy.

The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies).

The globalized nature of financial services and their subsequent cross-border ICT risks means that state level regulation can have only a limited impact. Hence, there has, until now, been limited or incomplete focus on ICT risk in the context of operational resilience – DORA stands to fill that gap.

4 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, Shaping Europe's Digital Future, COM(2020) 67 final.

5 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Region, A European strategy for data, COM(2020) 66 final.

6 'Report with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets (2020/2034(INL))

WHAT'S INCLUDED?

DORA serves to deepen the digital risk management dimension of the EU's Single Rulebook and forms part of the European Commission's Digital Finance Package. DORA, specifically, was designed to consolidate and upgrade ICT risk requirements throughout the financial sector to ensure that *all* participants of financial systems are subject to a common set of standards to mitigate ICT risks from their operations. DORA includes a broad range of obligations contained within five overarching pillars; ICT Risk Management, Incident Reporting, Digital Operational Resilience Testing, Information and Intelligence Sharing and ICT Third-Party Risk Management (Figure 1).

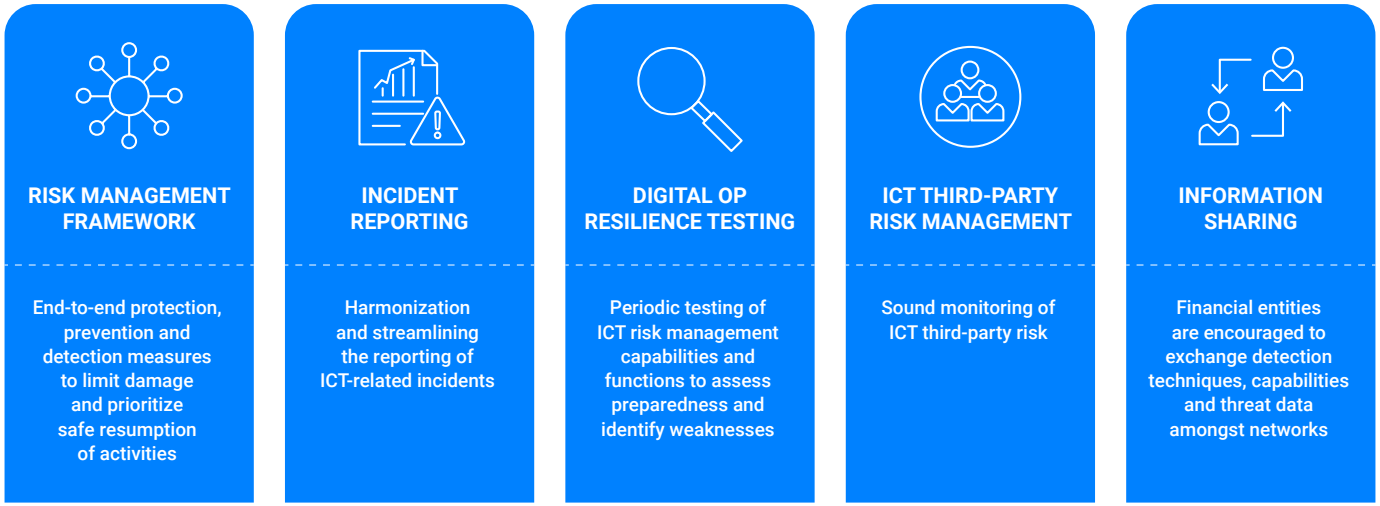


Figure 1: Five pillars of DORA obligations

DORA's scope is sufficiently wide to capture all financial entities – from electronic money institutions to securitization repositories – but it will also apply to third-party IT service providers. In the following section we explore the obligations in more depth and provide examples of where firms can utilize emerging technology to future-proof their digital dependencies.

ICT RISK MANAGEMENT – "BUILD, ENSURE AND REVIEW OPERATIONAL INTEGRITY"

DORA requires institutions to implement internal governance and control frameworks to ensure the effective management of all ICT risks. Practically speaking, the management body needs to define, approve, oversee and be accountable for *all* arrangements related to the organization's ICT risk management framework.

The risk management framework itself must include strategies, policies, procedures, ICT protocols and tools necessary to duly and effectively protect all relevant infrastructure, ensuring that systems are adequately protected from risks including damage and unauthorized access or usage.

BUILD OPERATIONAL INTEGRITY

Modern institutions represent sprawling networks of complex technology infrastructure. So a successful risk management framework hinges on effective and accurate system mapping. Firms must identify, classify and document all ICT-related business functions, the information assets supporting these functions and the ICT system configurations and interconnections with internal and external ICT systems.

In its proposal, the EC encourages the procurement and implementation of "appropriate ICT security tools" to enable institutions to prioritize data driven risk mapping. Technology can offer a range of capabilities here by automating the mapping of ICT risk requirements and streamlining subsequent risk assessments by visualizing the relationships between assets and business processes. Risk assessments can be further enhanced through the integration of threat, vulnerability and incident data allowing managers to intelligently prioritize mitigation measures based on business impact.

ENSURE OPERATIONAL INTEGRITY

Once risk mapping is complete, organizations must implement mechanisms to detect, protect and respond to breaches and outages. Such workflows must be captured within a dedicated and comprehensive ICT Business Continuity Policy, forming an integral part of the ICT risk management framework, prescribing how the firm is to act to ensure the continuity of critical functions.

Technology can support here, too, comprehensive and tech-enabled risk mapping means assets affected by a crisis event instantly activate corresponding crisis and recovery plans. Teams are instantly alerted to outages via a mass notification system and management can track progress and resources in real-time, enabling them to manage all activities needed to respond in a crisis situation.

REVIEW OPERATIONAL INTEGRITY

The final component of the ICT risk management framework requires firms to introduce “post ICT-related incident reviews” following any significant disruption. Such reviews should include root-cause analysis to identify required improvements to operations and these must then be incorporated within the associated ICT Continuity Policy. Importantly, any policy changes must be communicated to competent authorities.

A fully integrated risk management system allows managers to easily assess what happened during a breach or outage, and more importantly, why it happened. Stakeholders can leverage full workflow capabilities to document employee actions, follow up on issues and track remediation plans to evaluate how components may be improved. Once identified, users can instantly transpose changes into corresponding policy documents and distribute to necessary stakeholders, all within a unified cloud platform.

ICT INCIDENT REPORTING

EU DORA seeks to provide a consistent and uniform reporting mechanism to reduce the administrative burden for financial entities while strengthening supervisory effectiveness. Only ICT-related incidents deemed to be "major"[7] are expected to be reported via the common template to competent authorities. Additionally, institutions must submit initial, intermediate and final reports and ensure users and clients are informed when an incident may impact their financial interest.

Novel software solutions offer built-in reports which leverage centralized risk and incident data allowing stakeholders to instantly generate reports on ICT incidents with meaningful and coherent data insights from the single system record.

Key Considerations

- Is reporting integrated into the broader workflow or a reactive/emergency process?
- Is incident / risk data easy to find, access and interpret?

DIGITAL OPERATIONAL RESILIENCE TESTING

Firms' ICT risk management frameworks must be periodically tested to identify any deficiencies or gaps. Testing must incorporate regulatory-driven and critically assessed exercises, including the use of TIBER red team tests[8] that replicate the actions of real-world threat actors to evaluate cyber defenses in real-time. If deficiencies are flagged, institutions must promptly implement and document corrective measures.

Manual penetration testing, while accurate and reliable, is an extremely resource-intensive endeavor that requires meticulous planning and preparation. Although there may be scenarios in which manual testing is appropriate, it is advantageous to supplement this with automated alternatives where possible to facilitate the execution of a full spectrum of appropriate testing such as vulnerability assessments and scans, open source analyses and network security assessments. Solutions such as SAI360's Operational Risk module facilitate top-down and bottom-up assessments with consolidation techniques to summarize the risk profile of a business unit or the organization. DORA also encourages collaboration to ensure that institutions are able to stay abreast of the rapidly evolving cyber threat landscape.

To raise awareness of ICT risk, minimize its spread and support defensive capabilities, DORA encourages institutions to formalize information-sharing arrangements to exchange testing data and cyber threat intelligence. Firms may wish to share information regarding indicators of compromise, tactics, techniques, and procedures, cyber security alerts and configuration tools. It's important then, that firms operational risk data is easy to find, access and interpret so it can be shared across peers and contribute to broader financial market stability.

7 'major ICT-related incident' means an ICT-related incident with a potentially high adverse impact on the network and information systems that support critical functions of the financial entity

8 https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf

ICT THIRD PARTY RISK MANAGEMENT

DORA is comprehensive in its approach to mitigating firms' internal ICT risk, but this rigor also extends to third-party ICT providers. The EC plans to introduce powers for supervisors to oversee risks stemming from dependencies on third-party service providers. The proposal includes a range of principles-based rules applying to financial institutions monitoring of third-party ICT risk.

Regulators across the globe are paying more attention to firms' networks of suppliers. Increasing interconnectedness across all markets, not just financial services, means it is no longer sufficient to solely monitor internal operational dependencies. Institutions must perform similar mapping across all third-party dependencies and document continuity workflows in associated policy documents. Importantly though, DORA will require firms to include information pertaining to these dependencies within their contracts with ICT third-parties:

- A complete description of services
- An indication of locations where data is to be processed
- Full service level descriptions accompanied by quantitative and qualitative performance targets

The Coronavirus pandemic has only accelerated digitization across the financial sector, and with institutions' networks of third-party ICT service providers expanding quicker than ever, it's nigh-on impossible to monitor such relationships and their associated risks without technological support. Modern software enables firms to leverage configurable profiling portals to on-board and prioritize vendors based on associated risk profiles. This allows all vendor records to be centralized alongside other risk data to provide a 360-degree view of internal and external ICT risk across all locations, assets and 3rd and 4th parties.

RISKS OF NON-COMPLIANCE

POWERS OF THE LEAD OVERSEER

DORA grants competent authorities the power to adopt "any type of measure, including of a pecuniary nature, to ensure that financial entities continue to comply with legal requirements." For the purpose of carrying out investigative duties, regulators may wish to perform the following:

- Request all relevant information and documentation
- Conduct general investigations and inspections
- Request reports after the completion of oversight activities, specifying remediation actions that have been implemented by critical ICT third-party providers

The "Lead Overseer", as it is referred to within DORA, may impose periodic penalties on ICT third parties that fail to meet the required standards. These penalties shall be imposed on a daily basis until compliance is achieved and for no more than a period of six months following the notification to the critical ICT third-party service provider. The value of the penalty may be up to 1% of the average daily worldwide turnover of the critical service provider in the preceding business year.

With that said, the EC encourages national regulators to consider proportionality in their issuance of punishments and asks member states to consider a range of factors in the decision-making process such as the gravity and duration of breaches, the degree of responsibility of the legal person and losses incurred by third parties.

BROADER IMPLICATIONS OF ICT FAILURES

The broader implications of system outages pose far greater risks to firms, customers and financial markets than regulatory fines alone. From the perspective of the customer, the impacts of ICT incidents can range from a mere inconvenience through to customer harm as they risk losing access to vital services, or worse, having their personal information exposed in data leaks or breaches. For institutions, system outages can halt critical operations and incur devastating impacts to revenue and productivity. It is estimated that IT downtime can cost firms anywhere from $5,000 to $10,000 per minute,[9] with 15% of outages costing more than $1 million.[10]

ICT failures of any kind are likely to shatter an institutions' reputation. Customers have come to expect round-the-clock access to financial services through the rise of mobile banking and equivalent platform services. System outages cause many to switch providers without hesitation, and with the barriers to changing providers lower than ever, these risks are only growing. Trustee Savings Bank (TSB) felt the full bore of these risks in 2018 when a failed IT migration project left almost two million customers locked out of their accounts, some for weeks at a time. The events are thought to have cost TSB circa £330 million and 80,000 customers.[11]

9 https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

10 https://trilio.io/resources/cost-of-downtime/#:~:text=The%20average%20cost%20of%20downtime,per%20hour%20to%20over%20%24500%2C000.

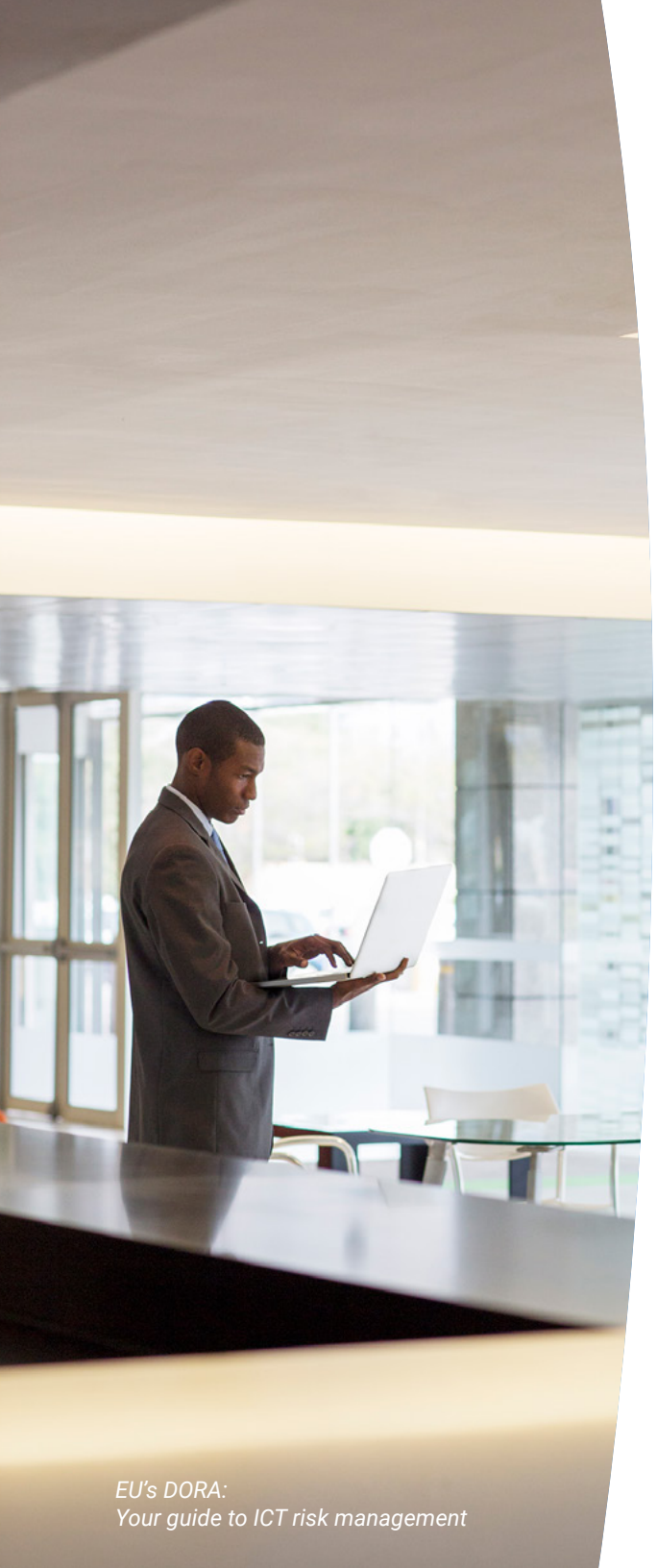
11 https://www.tsb.co.uk/news-releases/slaughter-and-may/

OPERATIONAL RESILIENCE – A HIDDEN OPPORTUNITY?

While the regulatory, monetary and reputational risks of IT outages are evident, the extent of the associated damages are entirely dependent on how quickly you can recover. DORA encourages robust, uniform and comprehensive ICT risk mitigation measures across the EU, and the new legislation will significantly improve the operational resilience of market participants. Firms mustn't be afraid to innovate and automate, instead it is critical to adopt a technology strategy that is resilient to risk, in which technologies are:

- Well understood across the business
- Chosen and integrated from a holistic perspective
- Flexible and adaptable to changing and challenging external circumstances
- Harmonized with third parties

As well as being less likely to lead to regulatory breaches and penalties, such a technology strategy is also likely to result in a more efficient user experience and technical performance and is better set up for the long-term (as opposed to being reactive and constantly changing). As such, technology is not only a means for improving operational resilience, but also a strategic route to competitive advantage.



OPERATIONAL RISK SOFTWARE – FUTURE PROOF YOUR DIGITAL INFRASTRUCTURE

Operational risk software, such as that offered by SAI360, exists as the foundation upon which surrounding business continuity processes can be built. By leveraging emerging technologies, stakeholders are able to ingest and analyze data across the entire organization to create a 360-degree view of risk that is dynamic, comprehensive and accurate. It's no longer sufficient for firms to rely on reactive decision making in our increasingly digital economy, instead, managers must proactively manage and mitigate ICT related risks with a data-led approach. Of course, even with the best planning in the world there will still be breaches and outages, but through the use of operational risk software, firms can reduce the severity and duration of such downtime, limiting the associated economic, operational and reputational risks in the process.

SEE WHAT SAI360 HAS TO OFFER

SAI360 are GRC experts and a leading cloud-based solution provider for EU DORA and more. Our modular approach allows you to take advantage of configurable solutions and quickly shape them to help you thrive in the evolving Governance, Risk and Compliance landscape. To learn more about the SAI360 platform and how we can advance your GRC goals, **contact us** online to set up a call with one of our representatives.

SAI360

About SAI360

SAI360 is the leading ESG cloud provider connecting GRC, EHS, Sustainability and Learning. Our SAI360 platform streamlines workflow and drives outcomes through flexible, scalable, and configurable modules. Our integrated approach sets us apart, helping organizations thrive, create trust, understand their impact, and achieve resilience for over 25 years. SAI360 is headquartered in Chicago, with operations and customers across the globe. Discover more at **sai360.com**.

107700 0123