EU 2022/2554: Digital Operational Resilience Act

Regulation Overview and ICT Risk Management Framework

Rule Overview

The Digital Operational Resilience Act (DORA) covers EU No 2022/2554 and amended regulations EC No 1060/2009, EU No 648/2012, EU No 909/2014, EU No 600/2014, and EU No 2016/1011. The rule aims to make the financial sector more resilient to information and communication technology (ICT) breaches and incidents with requirements on ICT risk-management capabilities, incident reporting, operational resilience testing, and ICT third-party risk monitoring. Financial entities will need to be compliant with the rule from January 17, 2025.

ICT Risk Management Framework Requirements

The regulation includes several requirements to financial entities regarding the security of the network and information systems supporting their business process. In order to achieve a high level of digital operational resilience, financial entities would need to meet the following requirements:

	Requirements
ICT Risk management	- Have in place an internal governance and control framework covering the management of ICT risk. The management body of the financial entity shall approve, oversee and is ultimately responsible for its implementation; - The ICT risk management framework shall include strategies, policies and procedures , ICT protocols, and tools to protect information systems from potential incidents and cyber threats. Such policies and procedures include ICT business continuity policy, ICT-related incident response procedures, and backup procedures. - Maintain an inventory of all ICT supported business functions, and ICT assets supporting those functions; - Yearly reporting to the board of directors of the digital operational resilience testing outcome with recommendations
ICT-related incident management process	- Develop ICT-related incident management processes to (i) continuously monitor and promptly detect threats, and (ii) track, log, and classify all incidents according to their priority and criticality of services impacted; - ICT-related incidents and cyber threats shall be classified based on the number and/or relevance of those affected, duration of incident, geographical spread, data losses, criticality of services affected, and economic impact; - Ensure that major ICT-related incidents are reported to senior management; - Assign roles and responsibilities that need to be activated for each type of ICT-related incident type and establish ICT-related incident response procedures to mitigate impacts and ensure services become operational in a timely manner; - Set out plans to communicate ICT-related incidents to staff, external stakeholders including clients, and media.
Reporting of incidents and cyber threats to authorities and clients	- Report major ICT-related incidents to the local authority, including all information relevant to its significance and impacts. Also, significant cyber threats shall be reported on a voluntary basis to the local authority. Reporting shall include (i) an initial notification, (ii) intermediate report if the status of the original incident has changed significantly, and (iii) a final report when the root cause analysis has been completed and actual impact figures are available. - Inform clients when a major ICT-related incident occurs that impacts them.
Reporting of major operational or security payment related incidents	Report operational or security payment-related incidents where they concern credit institutions, payment institutions, account information service providers, and electronic money institutions.

EU 2022/2554: Digital Operational Resilience Act

ICT Risk Management Framework and Oversight Framework

ICT Risk Management Framework Requirements (Continued)

	Requirements
Digital Operational Resilience Testing	Maintain a sound and comprehensive digital operational resilience testing program, including: - Yearly tests by independent parties on all ICT systems and applications supporting critical or important functions, such as scenario-based tests, compatibility testing, performance testing, end-to-end testing and penetration testing; - At lest every 3 years advanced testing by means of Threat Lead Penetration Testing (TLPT) covering several or all critical or important functions and be performed on live production systems. The financial entity shall ensure the participation of ICT third-party service providers in the TLPT, where applicable. A report of the findings, remediation plans, and documentation demonstrating that TLPT was conducted is to be provided to the local authority.
Information sharing arrangements	- Financial entities may exchange among themselves cyber threat information and intelligence, so long as (i) it aims to enhance the digital operational resilience of the financial entities, (ii) takes place within trusted communities, and (iii) is implemented through information-sharing arrangements to protect the sensitive nature of the information shared. - Financial entities shall notify the local authority of their participation in the information-sharing arrangements.
Sound management of ICT Third-Party Risk	- Manage ICT third-party risk taking into account a multi-vendor strategy, where applicable; - Maintain and update at the entity level, a register of all ICT services provided by ICT third-party service providers; - Report yearly to the local authority details of new ICT third-party service provider arrangements; - Only enter into contractual arrangements with the ICT third-party service providers that comply with appropriate information security standards; - Ensure that they are able to exit contractual arrangements without disruption to their business activities, and maintaining compliance with regulatory requirements. Contingency measures shall be in place such as identifying alternative solutions and creating transition plans in the event of significant breach or evidenced weakness. - The contractual arrangements with the ICT third-party service providers shall include specific elements; - Establish a role (or designate a member of senior management) to monitor the arrangements with ICT third-party service providers on the use of ICT services and its related risk exposure;

Oversight Framework of Critical ICT Third-Party Service Providers

The ESAs shall designate the ICT third-party service providers that are critical for financial entities and appoint a Lead Overseer for each critical ICT third-party service provider. The Lead Overseer is to provide an oversight function to assess whether the ICT third-party service provider has in place comprehensive, sound and effective risk management processes to manage the ICT risk it may pose to financial entities. To carry out their duties, the Lead Overseer shall have the power to (i) request all relevant information and documentation required by these rules, (ii) conduct investigations and inspections, (iii) issue recommendations to improve the risk management processes, and (iv) request reports specifying the actions or remedies implemented after recommendations are issued.

Digital Operational Resilience Act

Botsford Team Contacts

For additional information about this Regulatory brief or Botsford Associates Financial Services Regulatory Practice, and how we can help you, please contact:

Jon Block
Managing Partner
Financial Services
NYC: 917.647.3434 / TOR: 416.915.0438
jblock@botsford.com

Andrew Moreira
Managing Director - Consulting
Financial Services
NYC: 917.722.0939 / TOR: 647.361.4404
amoreira@botsford.com

Gordon Wong
Managing Director - Advisory
Financial Services
NYC: 917.722.1200 ext 319 / TOR: 437.253.4933
gwong@botsford.com