Deloitte.

Regulatory News Alert

Digital Operational Resilience Act (DORA): What are the strategic implications for the Financial Players Board?

21st December 2022

Digital Operational Resilience Act (DORA): What are the strategic implications for the Financial Players Board

In summary:

- The Digital Operational Resilience Act (DORA) has been approved by European legislators and will be enforced after 24 months from its enactment, scheduled for January 2023.
- Businesses in the financial sector will have to face a regulatory adaptation challenge which stems from the new normative requirements set by DORA. Moreover, they will have to be prepared to deal with the additional and broader strategic implications arising from the new regulatory standards.
- The new regulatory standards will call for a change in mindset, starting from the top management (Board e CxO), which will be required to increase the resilience level given the risks linked to digital evolution. Such change is necessary in order to promptly react to the evolution of threats and vulnerabilities coming from a new market context.
- The commitments – both immediate and continuous - set by DORA imply that Administration Boards and CxOs of the financial sector will be leading the process of change by defining the necessary response actions and investments aimed at increasing the level of resilience.

Audience: Administration Board members, CEO, CFO, CRO, COO, CISO, Compliance Officer.

Context

DORA, the most important EU initiative in the field of operational, digital, and cyber resilience for the financial sector, has been ratified by European legislators. The European regulation introduces a harmonized regulatory and supervisory framework by pushing businesses, operating in the financial sector, to make significant investments to strengthen their level of resilience to cyber and digital risks impacting on the business continuity of critical functions and services.

Deloitte.

The provisions of DORA must be implemented within 24 months from its entry into force, which will occur after the text is published in the Official Journal of the EU, scheduled for the end of 2022. Companies will then have to enable a compliance program to be completed by early 2025.

DORA: what strategic implications for businesses in the financial sector?

1. **The concept of "operational resilience" will result in a change of mindset for businesses**: DORA introduces for the first time the concept of operational resilience within the EU regulatory framework that governs financial services, moving beyond previous guidelines focused on cyber and IT risk with a new holistic approach, designed to strengthen resilience to digital disruptions. DORA represents more than just a change in terminology: operational resilience goes beyond the traditional risk management approaches used by the Cyber, IT risk and Business Continuity functions; it leads businesses to assume that serious disruptions are inevitable (regardless of how robust the business defenses are) and pushes them to build a higher level of resilience to such disruptions within the operating model of their most important functions and services. This assumption will involve an ongoing dialogue between businesses and authorities, the modalities of which have yet to be worked out by EU financial supervisors.

   The development of such an approach in the United Kingdom (which implemented its operational resilience framework in March 2022) has caused companies to set high future resilience standards that will require substantial investment to be achieved. The U.K. experience has also demonstrated the need for greater cross-sector collaboration on common risks and vulnerabilities that cannot be properly addressed at the level of a single operator but require a systemic response. In this regard, the industry will need to be proactive in developing models and methodologies to address concentration risks and testing practices related to third parties, and real-time sharing of threat intelligence information.

2. **Management's responsibility on operational resilience is strengthened**: DORA provides clear responsibilities on operational resilience for the Board and CxOs to take a leading role in the implementation of solutions to achieve the standards under the new regulatory framework. In practical terms, the Board and the top management will have to approve several key programs, such as the corporate digital operational resilience strategy, the ICT third-party management policy (TPPs) that will require targeted strengthening of safeguards against the status quo. In addition, the senior management will also be responsible for making operational model decisions in order to incorporate DORA requirements into day-to-day operations, such as defining risk tolerance levels and prioritizing remedial actions to respond to identified operational vulnerabilities.

   Although supervisory expectations of Boards will only fully emerge later, the components of DORA that require an active role in terms of direction, approval, and oversight will require additional skills and resources for most Boards. Implementation of the DORA standards will require Boards and CxOs to demonstrate to supervisors of corporate resilience to specific and broader sector-specific threats. They will also need to strengthen their understanding and level of awareness about the company's ability to cope with potential ICT disruptions while maintaining continuity of services. They will need to demonstrate to have made the right management decisions, to have reviewed and challenged resilience plans, and consequently to have strengthened their company's overall resilience. Management information on threats and vulnerabilities from the external environment will need to be considered dynamically within the overall operational resilience framework of the company.

3. **The continuous and required fulfillments will lead businesses' actions beyond the period of regulatory implementation:** The 24 months implementation period will challenge the majority of the businesses in the financial sector, even the biggest and most structured ones. Such challenge will take place in different areas, such as *operational resilience testing*, *incident reporting* and *business impact analysis*. DORA introduces a continuative approach in terms of resilience management for financial businesses. Such approach is based on a constant process of revision and evolution, and it will have long-term implications. To give an example, businesses will be required to perform resilience tests and assess both the risks and the suitability of their resilience plans. Moreover, businesses not only will have to continuously gather information on threats and incidents to comply to new incident reporting requirements but also, they will have to create their own risk scenarios. DORA requires businesses to identify their critical or important functions (CIFs) as a focal process in order to strengthen their resilience, particularly for what concerns the identification of threats and scenario testing.

   The reasoning behind the new regulatory framework is that the achievement of a "good" operational resilience level will constitute a regulatory obligation which will evolve along with the evolution of threats and vulnerabilities stemming from the reference context. Investing on strategic capabilities, such as threat intelligence and resilience testing, Boards and CxOs will have additional instruments to understand not only how risk scenarios can influence their critical and or important functions but also, what necessary investments need to be made in order to reach a sufficient level of preparation. Furthermore, strategic capabilities of this kind will be fundamental, even to guarantee more efficient response capabilities to unexpected interruptions.

4. **Businesses outsourcing strategies will be challenged:** Addressing third-party vulnerabilities is one of the key challenges on the path to strengthen operational resilience. DORA introduces at world level the first framework for supervision of critical third-party service providers (CTPs) by assigning to the European Supervisory Authorities (ESAs) new powers to supervise third-party providers and to manage the risks these operators might pose to the financial services industry. In this regard, EU regulators also reiterated that the new supervisory regime does not imply a review of the individual responsibilities of financial sector businesses for outsourcing. In fact, DORA imposes several new third-party risk management requirements on financial sector companies, the level of severity of which increases in cases where third-party providers play a role in supporting the businesses' critical or important functions (CIFs). This can become particularly impactful for FinTech and digital-native companies, whose dependence on certain digital platforms could potentially make them more exposed to ICT risk and require increased supervisory oversight of that risk.

   Businesses will also need to pay special attention to assessing the risk of third-party concentration. Potential vulnerabilities – such as over-reliance on a single vendor or the criticality of the functions served- may expose financial operators to increased supervisory scrutiny. This could also put pressure on Boards to review their sourcing strategies (aiming, for example, to a multi-vendor strategy), their risk appetite for entering into third-party relationships, and the role of risk management and procurement functions.

5. **The path to strengthening operational resilience will require investment decisions by the Top Management:** In order to build operational resilience into a company, it is required that the company itself becomes a key factor in business decisions and in the design of operating models (*resilience by design*).

Deloitte.

More specifically, companies in the financial sector will have the task of identifying the expected level of resilience as part of the digital operational resilience strategy that DORA requires them to define, essentially binding top management to take a proactive decision-making role in ICT risk management and resilience. This implies that Boards and CxOs will need to assess the overall business case for investing in strengthening resilience capabilities, and also be able to demonstrate how the upfront costs are offset by a more resilient and sustainable operational model in relation to ongoing regulatory evolution and intensified supervisory action. At a practical level, highest level priority should be given to those areas that could potentially be central to supervisors' agendas as they implement DORA, such as requirements that demand for recurring outputs that can challenges by supervisors (for example, identification of CIFs, business impact analyses, operational resilience testing, incident reporting processes).

In making key decisions, management will also need to take into account how supervisors will effectively apply DORA's principle in practice. Operators of larger size and operational complexity are likely to have more advanced capabilities in certain areas (e.g., resilience testing), but they will also be subject to a stronger scrutiny, given the potential systemic importance of their key services. Smaller operators, on the other hand, will benefit from less stringent requirements (e.g., they are not required to conduct advanced TLPT testing and are subject to DORA's simplified ICT risk management framework), but they will still face large investments to equip themselves with the necessary capabilities to align with the requirements of the regulation that apply on a general level, such as the ICT incident reporting requirement and third-party risk management provisions.

Final considerations

DORA will not be a "*one-off*" compliance exercise. In fact, it will push businesses to maintain an adequate resilience level in a context where threats are in constant evolution and technology is increasingly complex.

For the next 24 months, European supervisory authorities will focus on declining the secondary normative part of DORA and on assessing their expectations in terms of operational resilience. Despite this, it is already clear that Boards and CxOs will be called to action to make decisions on the matter of operational resilience throughout the DORA implementation period. For this reason, it will be paramount to establish a strong "*tone from the top*" regarding the commitment that businesses will put into the creation of their operational resilience – such element will be increasingly taken into account by regulatory and supervisory authorities, investors and stakeholders, given the rising numbers of operational threats in the financial sector.

Deloitte.

Contacts

Andrea Rigoni
EU Digital Policy Center Director – Deloitte Risk Advisory
Tel: + 39 3355772342
arigoni@deloitte.it

Gianfranco Tessitore
Partner | Regulatory Strategy & Controls Transformation Leader – Deloitte Risk Advisory
Tel: + 39 3488862150
gtessitore@deloitte.it

Deloitte Risk Advisory S.r.l. S.B.
Via Tortona 25, Milano, 20144, Italia