Deloitte.

DORA, a regulatory revolution on digital risk management for the entire financial sector

The first challenge companies need to win with the new Digital Operational Resielience Act is a shift in mindset from all levels, starting from top management.

Andrea Rigoni, Gianfranco Tessitore

9th November 2022

On November 10th, the European Parliament will vote on DORA - Digital Operational Resilience Act -, the new European regulation that will trigger a momentous change in the financial sector. The new regulation has a very broad scope and will impact not only banks, but also insurance sector and financial market operators, regardless of their size. This is already a very important first change, because the same rules will be imposed to everyone. It will also include IT service providers and next generation operators such as fintech, including Crypto Assets managers or financial services providers in Crowdfunding. DORA will ask top management from all these operators to guarantee their ability to define strategies and models capable of minimizing impacts from events deriving from the digital domain that could impact the confidentiality, availability or integrity of the most critical services and functions.

DORA will impose a mindset shift in the approach to digital and related risks, influencing the business model: top management of all the operators involved will be asked to not only worry about financial sustainability, but also "resilience," or the ability to continue to operate even in the event of accidents or threats caused by digital sphere. These requirements will come into force within 24 months from the publication of DORA: operators will have until December 2024 to prepare to meet the new requirements, taking into account the second level regulation (RTS - Regulatory Technical Standards) which must be submitted within 12 months, leaving little time for financial operators to adapt to the new requirements.

DORA is the first intervention of this kind that will enforce requirements and a supervisory system for Digital and ICT third parties. In fact, financial sector operators will have to consider in their plans all the risks deriving from the adoption of specific digital and ICT services. With DORA, the granted authorities will launch a direct supervisory system on these operators, who will have to respond not only to the new and more stringent requirements, but also prepare themselves for additional pressures from the authorities, opening new regulatory and control scenarios in the digital sector.

DORA reaffirms the approach of the European regulators to use Information Sharing: sharing of information and data to face new generation of cybersecurity threats. The financial ecosystem to be protected is not only strongly interconnected, favoring the propagation of incidents from one operator to another, but is also characterized by

common infrastructures and technologies, as well as threats that often target the entire sector, regardless of the individual financial operator. A holistic approach is essential to be able to anticipate the continuous changes both in threat scenarios and in digital services, imposing a change of pace in risk management, which with DORA becomes "dynamic and pervasive."

The practice of "stress tests" is also introduced, already used in other contexts with a high level of complexity. It is an approach that is added to the compliance practices, which are enriched with this additional tool: the financial operator will be periodically tested against threat scenarios that will be defined based on the most recent and probable threats. These are typical techniques of intrusion and attack to verify the effectiveness of the defense strategies implemented by the financial operator. On this front, the regulation will accelerate the development of new technological solutions based on AI to carry out invasive tests without harming real systems, such as simulators of attack and defense systems and so-called "Digital Twin," or digital copies of the operator's systems.

It is therefore a regulation that will require a change of approach at all levels, starting with top management. The first challenge to overcome is cultural change, bridging risk culture and adequate leadership. This will lead to a future of increased and effective digital and security talent representative in Board of Directors and in business creating a transversal expertise able to connect the various company areas. Furthermore, for smaller operators, it will be necessary to evaluate different sourcing models to have these skills available through specialized services without losing control and responsibility over the most strategic choices.

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