DORA's major step-up in EU cyber-security standards targets the finance industry but also its telecoms providers

July 2024

Annika Nitschke, Tarek Benamar

With supply-chain cyber-attacks on the rise worldwide, the European Union (EU) is working to manage risk across the region with new regulations, the most striking of which is the Digital Operational Resilience Act (DORA).

DORA is intended to help financial markets to control cyber-security risks, but also covers third-party service providers. That brings telecoms players squarely into focus, given their fundamental role in the industry's day-to-day operations and the broad target they represent for cyber attacks. To stay relevant to the EU's financial markets, third-party providers of information and communication technology (ICT) must become active partners in financial clients' efforts to comply with DORA.

Supply-chain cyber attacks are on the rise

The EU produces an annual report on the status of the cyber-security threat landscape, to identify the principal trends and threats, and to inform regulation. Its latest report shows marked growth in the number of supply-chain cyber attacks, rising from less than 1% of intrusions in 2020 to 17% in 2021.

The EU is adapting to this threat landscape with a co-ordinated cyber-security strategy and the implementation of new Regulations, including DORA.

DORA is intended to make the EU's cyber spaces more resilient against cyber attacks, to build capacity to respond to cyber-security incidents and to advance information-sharing among EU member states and global allies.

DORA requires third-party risk management

The finance sector is a major focus of cyber attacks, which target financial institutions themselves but also their third-party ICT providers. Financial entities accumulate highly sensitive data and typically have very advanced protection against cyber-security threats. Third-party ICT providers, such as telecoms operators, handle and process the same sensitive data but may offer an easier target due to the large potential 'attack surface'. This is because third-party ICT providers share contact points with multiple financial institutions, increasing the risk of spread and disruption in case of security incidents.

DORA stipulates the responsibility of financial institutions in managing third-party ICT risks: financial institutions will have to undertake pre-contractual due diligence, compliance auditing and continuous risk analysis of any ICT service provider. Moreover, they will have to maintain a register of their contracted ICT service providers, including information on the criticality of the services. This will require a complete third-party risk management strategy and, especially for critical services, an exit strategy to ensure that a change of service does not disrupt the availability of financial services.

Third-party businesses looking to maintain or expand their relationships with the financial sector must ensure they pass the mandatory pre-contractual assessments. That will require a close examination of their operations to ensure full and certifiable compliance with DORA's requirements, in addition to the ICT and cyber-security measures that many might already have in place. DORA requires the implementation of new incident reporting systems, business continuity plans and performance monitoring by the financial entity of contracted ICT third-party providers. These are significant additional obligations for ICT service providers that go beyond current information and cyber-security standards such as ISO27001.

Some telecoms operators may be classed as financial service providers

DORA's applicability to telecoms operators is principally a reflection of ICT's crucial role as the backbone of the financial sector. The wide variety of services offered by telecoms operators (such as data transfer services through public networks and data centres), using heterogenous and widely dispersed assets, creates a large cyber-attack surface. The stability and continuity of financial services are critically dependent on these services. Designation as critical infrastructure puts ICT service providers under the oversight of EU security authorities (ESA) (Articles 32–33), with additional obligations to manage the risks they pose to their financial customers. In addition, more innovative services (such as mobile payments and financial transaction services) blur the lines between fintech and telecoms: operators providing fintech services will be directly subject to DORA as financial service providers in their own right.

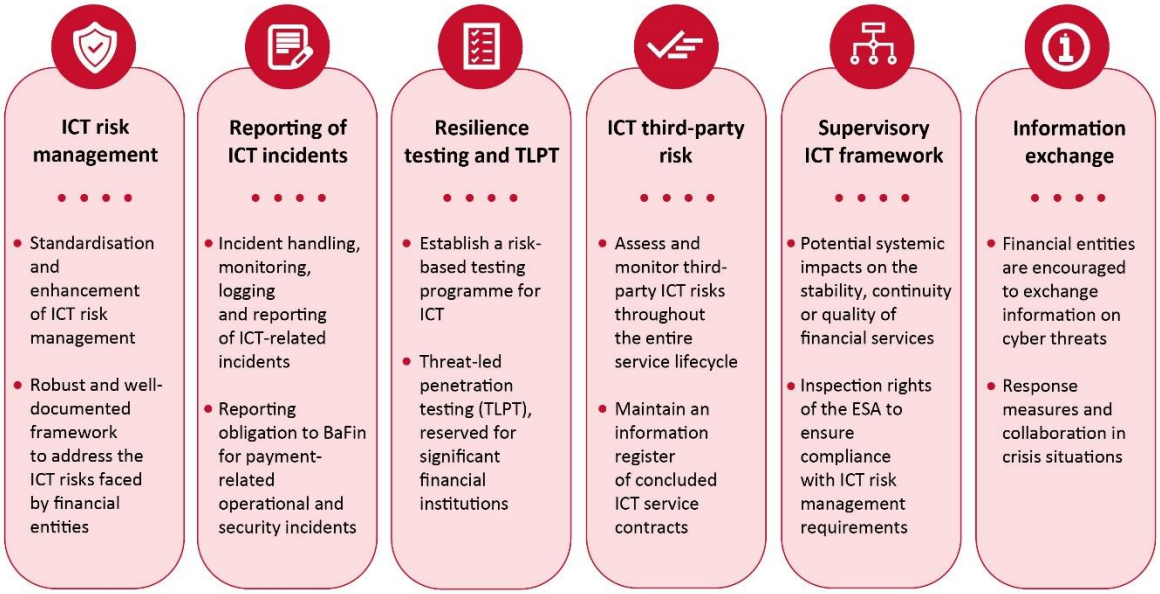
Immediate action will be invaluable

DORA was introduced in January 2023, and critical ICT service providers and financial institutions have to be compliant by January 2025.

Analysys Mason has put together a short list of specific activities that will be vital if critical telecoms operators are to achieve DORA compliance:

- **Contract management**: many existing ICT service contracts will have to be reviewed and new contracts will need thorough pre-contractual vetting.
- **ICT risk management system:** both financial institutions and critical third-party ICT providers will require an effective ICT risk management system (RMS) in place:
  - **risk register:** an important part of the ICT RMS is a risk register to track and identify risks
  - **data collection:** data is at the heart of any RMS, and efficient, scalable and sustainable data collection methods are important to ensure successful risk management.
- **Analysis and reporting:** continuous monitoring and incident reporting systems are key to DORA compliance.

Figure 1: Actions to be taken by critical telecoms operators and financial institutions to achieve DORA compliance



Source: Analysys Mason

About us

DORA is only one of a series of landmark regulatory instruments that telecoms operators will need to adhere to. For almost 40 years, Analysys Mason has been working with players across the TMT industry to adapt to technological and regulatory change. We have been instrumental in the development and implementation of the regulations that have shaped the European telecoms landscape, as well as helping operators to thrive in an evolving market. For further information on how Analysys Mason can help with contractual re-negotiation, the conception and implementation of RMS, or building tools for risk-related data analysis and management reporting, please contact Annika Nitschke (Expert Consultant) or Tarek Benamar (Consultant).