ARTICLE

Exploring the Digital Operational Resilience Act (DORA)

Five Key Questions Business Leaders Should Be Asking

1. What is DORA, and why should I pay attention?

The European Commission's (EC) most recent Digital Finance Package has been marketed as a means for Europe to become a global standard-setter in an increasingly digitalised financial sector. Whilst the package's retail payments strategy and legislative proposals around crypto-assets are important elements of the EC's new vision for a safer, more tightly-controlled and progressively democratised financial services field, DORA – the Digital Operational Resilience Act – has emerged as a standout talking point for the broad scope of the oversight measures it outlines.

Historically, the European Union has taken a high-level approach to regulating resilience in financial services, often allowing national governance bodies to exercise their own discretion in relation to directives that have been notably limited in application and scope. Thus, in addition to generating significant compliance costs for multi-national financial bodies, current processes around incident reporting and third-party supervision remain inconsistent across national lines. DORA's overall objective is to harmonise regulatory mandates whilst ensuring that financial services providers are primed to withstand cyberattacks. By its very nature, DORA is much more interventionist and prescriptive than previously issued guidelines.

COVID-19 has underscored the urgency of this legislation. Europe has seen a 72% increase in the use of finance-based applications[1] and a 38% rise in cyber-attacks on financial entities since the pandemic began,[2] whilst FTI's most recent Resilience Barometer found that 36% of EMEA-based financial organisations suffered data loss in the past 12 months. With dependencies on financial technologies stronger than ever, digital operational resilience has transcended its character as a compliance-based buzzword to become a critical facilitator of service delivery in increasingly threatened business environments. But what do corporates need to know about the implications of this new regulatory framework? And what are the questions they must consider to effectively innovate whilst meeting these new demands to regulate?

[1] The European Commission's Digital Finance Factsheet (2020)

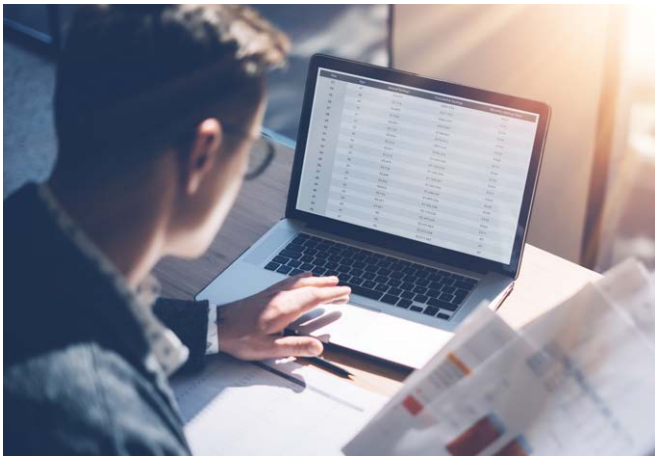
[2] The European Commission's Digital Finance Factsheet (2020)

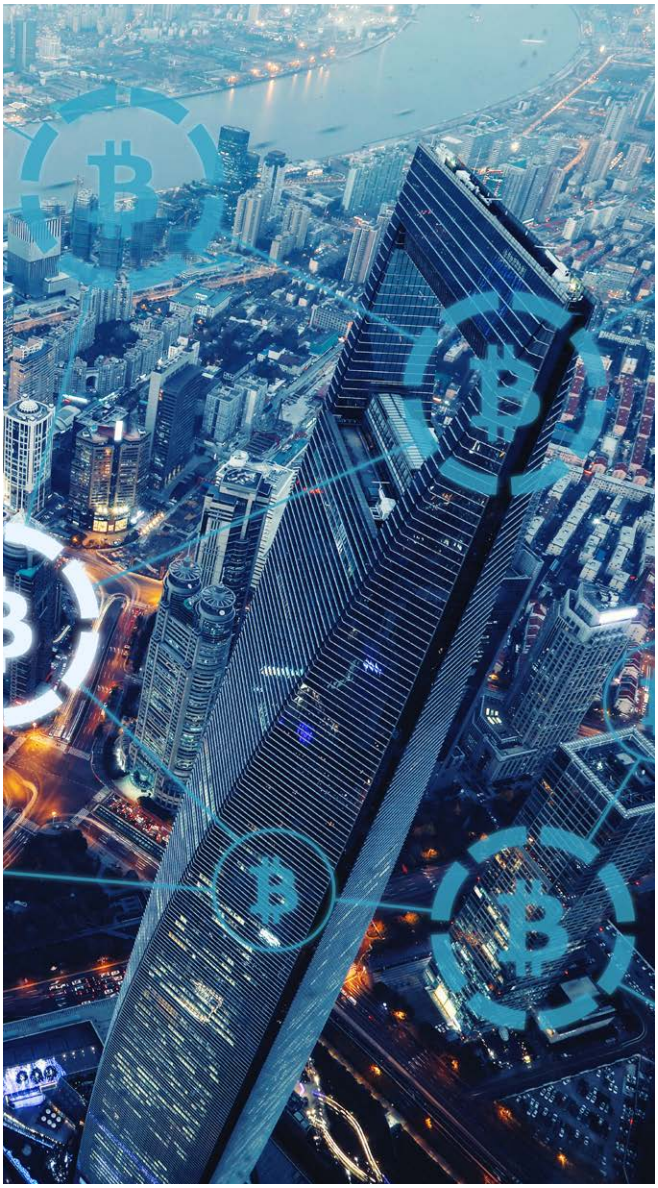
2. What is driving this change?

As financial services providers know, consumers' traditional transactional behaviours are changing - and so are their expectations in relation to the security of, and their ease of access to, the services they employ. Whilst corporate strategies have long focused on attracting consumers to their various tech-based offerings, business leaders must now internalise a core understanding that cyber professionals have long advocated: that cybersecurity and cyber resilience must become mainstream and considered integral elements of business operations.

Given the centrality of information and communication technologies (ICT) to business delivery in the financial services sector, flaws and vulnerabilities in digital infrastructures are not IT problems but firm-wide issues; securing these systems must therefore be incorporated as a critical element of business delivery strategies. When DORA comes into effect, it will force financial services providers to move beyond cyber compliance to cyber assurance. This will involve a shift in perception and action that not only has the potential to catalyse significant hardening of critical service delivery functions, but ultimately translate into business advantage. Individual consumers and larger client entities will choose to do business with providers who demonstrate their commitment to the confidentiality, integrity and availability of their systems.

As financial services providers consider the implications of the rising popularity of cryptocurrency and ever-evolving methods of payment and money movement, definitive leadership in this area will demand business executives who recognise the fundamental importance of cybersecurity to the services they provide – business leaders with the vision to acknowledge and integrate cyber resilience into the corporate digital strategies of the future.





3. Does tighter regulation of critical third-party providers risk heightening barriers of entry?

Despite intending to nudge what is currently a rather patchy and limited set of legislation around digital finance into a robust and effective set of cross-border mandates, one of DORA's most controversial elements – and the one which will play a defining role in generating forthcoming digital operational strategy – is the proposal's discussion around the oversight of corporate entities' critical third-party providers (CTPPs). Responding to long-standing concerns around tech provider concentration risks in a closely connected business sector, DORA asks businesses to define who their CTPPs are and demands clear contractual outlining of roles, responsibilities, liabilities and monitoring rights.

DORA's suggestion of a mandatory multi-provider approach, however, is a contentious one. Whilst limiting a single vendor's exposure to any one financial entity might well reduce reliance risk, boards will have to consider several key questions. Historically, for example, security providers have not been thought of as critical to service delivery in comparison with host providers. However, as the successful targeting of dozens of U.S. federal agencies and major corporations at the hands of a recent SolarWinds software compromise has demonstrated, perceptions of criticality must themselves shift to effectively mitigate the real risks that exist within supply chains.

Several other questions arise here: what are the implications of spreading risk in a multi-cloud environment? What challenges would a rotating provider system generate for data portability; and would there be an increased risk of data leakage in a structure such as this one? When it comes to DORA's discussion around CTTPs, questions far outnumber the answers. It is in the asking of these very questions, though, that business leaders will be able to evaluate the critical needs and resilience capabilities of their enterprises on the micro and macro levels the current threat landscape demands.

4. How do I balance competitive advantage against the needs of the industry?

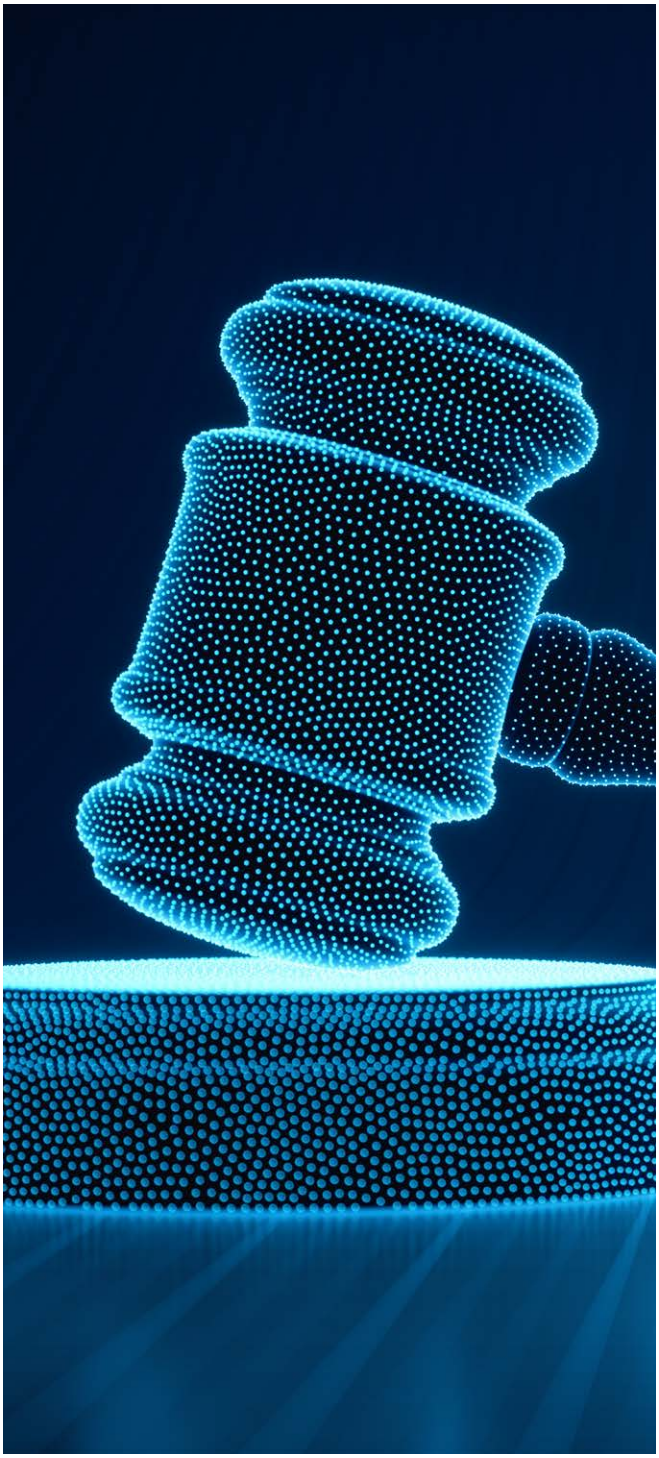
An opportunity for regulation to meet innovation also arises in DORA's discussion around cyber threat intelligence sharing: talks that can be conducted in a format decided by financial entities themselves. There are, of course, inherent challenges here. In addition to the cyber threat landscape's characteristic rapid evolution and consequent unpredictability, the lack of any defined mandate around threat-sharing forums may well see this provision fall by the wayside. However, it presents a significant opportunity for bold financial institutions to position themselves as leaders in the field of cyber resilience by directing discussions of this kind; discussions that will not only demonstrate an enterprise's cyber assurance, but ensure that businesses participating in these talks – in partnership with expert cybersecurity practitioners – have access to cutting-edge conversations around how and where they are most vulnerable, and how they can best build resilience to continue delivering business services in the event of an incident.

5. DORA: A mandate to regulate or opportunity to innovate?

Any legislation as broad as DORA in scope and application will face dissenting voices and challenges around practical implementation. Homogenising legal requirements around multi-national entities already subject to jurisdiction-specific cyber regulation is no small undertaking, and many will focus on the compliance burden DORA will impose on firms.

However, the principle underpinning DORA – that standardisation will drive cyber robustness in the financial services sector – is a powerful and logical one. Just as DORA recognises that digitalisation and operational resilience are two sides of the same coin, we recognise that regulation and innovation are two parts of the same journey towards secure digital futures.

Cyber professionals understand that building cyber resilience is an inherently creative and strategic process. It involves consideration of issues such as alternative methods of service delivery and planning how to communicate in moments of crisis. Business leaders who wish to retain their competitive advantage in an increasingly evolving threat landscape know that today, cyber disruption is not a possibility but a probability – a realisation that makes engagement with DORA and the questions it generates imperative components of any winning corporate strategy.



ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 207 632 5147
david.dunn@fticonsulting.com