WEBINAR REPORT

Mastering DORA:

A Strategic Guide to Operational Resilience for the Financial Services Industry

Sumant Kumar
CTO, Banking and Financial Services, NTT DATA

Kaspar Loog
Director of Product Management, LHV Bank

Andreas Papaetis
Senior Policy Expert, Digital Finance Unit, European Banking Authority

Ramon Villarreal
Payments Sector Global Lead, Red Hat

Finextra® | NTT DATA

Contents

00 | Market Context

The Digital Operational Resilience Act (DORA) is a regulatory framework introduced by the European Union to strengthen operational resilience in the financial services industry. This is particularly important given the increasing digital transformation and associated risks in the industry. DORA provides a set of rules for managing Information and Communication Technology (ICT) risks, including those associated with third-party providers. It also mandates regular testing of ICT systems and harmonises rules on incident reporting. Despite some debate over its necessity, DORA is seen as a crucial step in bolstering operational resilience, particularly in the face of rising cyber threats and the growing reliance on digital and third-party services.

This report summarises the discussion had during a Finextra webinar, hosted in association with NTT DATA, by a panel of industry experts, including:

Sumant Kumar
CTO, Banking and Financial Services, NTT DATA

Kaspar Loog
Director of Product Management, LHV Bank

Andreas Papaetis
Senior Policy Expert, Digital Finance Unit, European Banking Authority

Ramon Villarreal
Payments Sector Global Lead, Red Hat

01 | Introduction

In the dynamic world of financial services, operational resilience has risen to critical importance. The Digital Operational Resilience Act (DORA) has emerged as an essential regulatory framework designed to bolster operational resilience within the industry. This is particularly pertinent given the escalating digital transformation in financial services and the accompanying risks inherent in digital supply chains. The geopolitical landscape and rising cyber threats further highlight the necessity for robust operational resilience.

DORA, introduced by the European Union, provides a dedicated framework for the EU financial sector, aimed at protecting digital operational resilience—a vital aspect of contemporary business operations. The European Banking Authority (EBA) serves a pivotal role in this initiative, developing supplementary legislation to reinforce the core DORA text. A significant innovation under DORA is the direct oversight framework for critical ICT third-party providers, indicating the shift from analogue to digital, where instantaneous and increasingly connected operations are the norm.

In the constantly evolving landscape of Information and Communication Technology (ICT), businesses face a plethora of challenges and risks. A major concern is the growing reliance on third-party providers, which can introduce vulnerabilities and potential risks. Existing legislations often provide inconsistent and fragmented guidelines for managing these ICT risks. This highlights the need for a harmonised, comprehensive set of rules that cuts across different sectors, including insurance companies and banks.

The significance of operational resilience in today's business landscape cannot be overstated. As businesses become increasingly reliant on third-party entities, the necessity for robust control mechanisms and risk management frameworks is paramount. This dependency poses significant implications on both the individual business entity and the macro level. Managing these dependencies and mitigating associated risks is a formidable challenge, further complicated by contractual inflexibility with providers that can lead to operational inefficiencies and potential vulnerabilities.

In the rapidly evolving fintech world, robust, reliable, and resilient systems are more crucial than ever. The industry must grapple with the challenges of instant payments, uptime, and external cyber threats. The advent of new players, running on varied infrastructures and offering unprecedented uptime levels, compels established institutions to rethink their strategies. The key to navigating this new landscape lies in data-driven decision-making, practical testing, and a commitment to continuous improvement.

02 | **DORA Regulation:** Strengthening Operational Resilience

DORA is primarily aimed at introducing operational resilience within the digital supply chains in financial services. A significant focus of the regulation is on cyber threats, which are emerging and evolving constantly. The regulation is designed to address these threats and mitigate the risks associated with them. The regulation is also aimed at managing the risks associated with the growing digital ecosystem within the financial services industry.

The regulation can be broken down into five key pillars. These pillars provide a comprehensive framework for operational resilience within the financial services industry. They address various aspects of operational resilience, including cyber threats, supply chain risks, and the need for robust risk management practices. The regulation also emphasises the need for financial institutions to be proactive in managing these risks and enhancing their operational resilience.

However, it's important to note that while DORA provides a regulatory framework for operational resilience, it does not replace the need for financial institutions to take proactive measures to manage their risks. In fact, many of the practices outlined in DORA are things that financial institutions should already be doing. The regulation simply provides a more rigid and bureaucratic structure for these practices.

Loog's initial view about DORA was that the regulation would help banks "tame cloud providers." However, he soon realised that "there's nothing new there, nothing from a practical perspective that a financial institution shouldn't be already doing in my opinion."

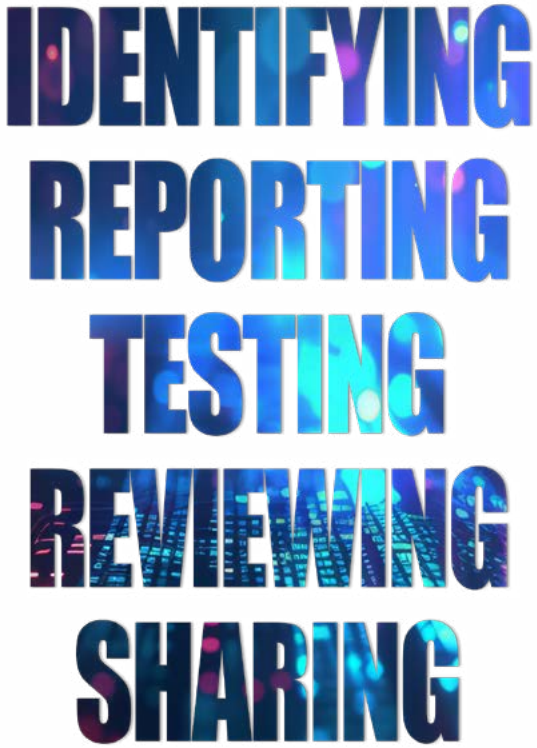
The financial sector, particularly the payments market, has had to consider operational resilience, business continuity, and cyber threats for a long time. However, the advent of DORA and similar regulations in other regions like the UK and the US signifies a global shift towards prioritising these aspects. The EU's swift action in releasing DORA and its focus on regulating interactions with infrastructure providers, business continuity factors, and concentration risk is commendable. These areas are of high priority for every organisation operating in the financial sector.

> **This is a new digital world that we are living in and that is changing the way that we apply concepts. I think it's great that we have regulations like DORA or others that are incoming.**
>
> Andreas Papaetis, senior policy expert, digital finance unit, European Banking Authority

As Papaetis explained: “We are more or less one year before DORA enters into application. The main aim of DORA is to provide a dedicated framework for the EU financial sector to safeguard operational resilience. So, the performance of the system and protection against attacks are all areas that are a big priority and we’ve been working with [banks] since the beginning. This is a new digital world that we are living in and that is changing the way that we apply concepts. I think it’s great that we have regulations like DORA or others that are incoming.”

DORA is structured around five main pillars addressing different areas of risk reduction and strengthening the IT infrastructure.

1. The first pillar is ICT risk management, which involves identifying critical services and setting up impact tolerances
2. The second pillar focuses on incident management, classification, and reporting.
3. The third pillar emphasises digital operational testing to provide assurance on various risk elements.
4. The fourth pillar is about third-party risk management, which involves assessing third-party risk, monitoring these risks, and conducting periodic reviews.
5. The fifth and final pillar is about establishing information sharing agreements, particularly for sharing threat intelligence in the financial services sector.



03 | **Understanding DORA:** Operational Resilience in the Financial Sector

The implementation of DORA signifies a significant international effort in the area of operational resilience. The attention from international competitive authorities and other regulators on the EU's approach to operational resilience is noteworthy. As we move into an increasingly digital and connected world, regulations like DORA are crucial to ensure the operational resilience of the financial sector.

DORA is a response to this need. It provides a common set of rules on ICT risk management and resilience across the entire EU financial sector. DORA applies to a broad range of financial entities, from banks and payment institutions to insurance companies and investment firms. It mandates yearly testing of ICT systems for all financial entities, with significant entities required to perform thorough penetration testing every three years. DORA also aims to harmonise the rules on incident reporting, creating a single reporting regime for the financial sector.

However, the introduction of DORA has sparked a debate on whether it is necessary and beneficial. Some argue that the regulation is needed to create a level playing field in the single market of Europe, where previously each country could set their own requirements for resilience. Others question whether there is a real problem with resilience in the banking sector that needs to be addressed. They argue that the move to cloud and third-party services has actually increased resilience, and question the need for regulation in the first place.

Kumar mentioned that "it's very early stages in terms of what needs to be done." He continued to say that "the bigger banks, rather than the smaller financial services firms, are at the early stages, because UK regulators have done a systemic review of operational resilience, have found that it is systemically important and can have a massive impact on the local financial market. However, more smaller institutions are starting to look into third party risk alignment."

Break the problem down into smaller, more manageable chunks, rather than attempting to tackle an entire portfolio of services at once.

04 | **Operational Resilience:** A Key to Business Continuity in Banking

The criticality of payments infrastructure is another area of concern. Banks are at the core of a country's business continuity, and their operations are closely tied to the operation of the country's critical infrastructure. The question arises as to how to regulate and control the dependencies of these operations, especially when they are outsourced to external organisations like cloud providers. There have been instances where major cloud providers have experienced downtime, raising concerns about the resilience of the services they provide.

The key to addressing these challenges lies in the adoption of a comprehensive strategy for operational resilience. This strategy should encompass all aspects of the business, from cybersecurity risk management to third-party risk alignment. It is crucial to identify and assess the critical services within the organisation and prioritise them accordingly. This approach allows businesses to break down the problem into smaller, more manageable chunks, rather than attempting to tackle the entire portfolio of services at once.

However, the implementation of such a strategy is not without its challenges. The level of preparedness varies greatly among businesses, with larger, more established entities typically being better equipped to manage operational resilience. Smaller businesses, on the other hand, often struggle with understanding and implementing the necessary measures. This disparity can lead to a significant gap in operational resilience across different sectors and industries.

Despite these challenges, the implementation of a robust operational resilience strategy can yield significant benefits. Beyond mere compliance with regulations, it can serve as a platform for innovation and business development. By leveraging the capabilities generated through operational resilience, businesses can enhance their service offerings and provide added value to their customers. This shift in perspective, from viewing operational resilience as a regulatory requirement to seeing it as a business enabler, can significantly accelerate its adoption.

> **It is now necessary to "accelerate the utilisation of the applicability of DORA – looking into innovation, the long term benefits, what we can bring to the customer, and the potential security benefits."**
>
> Ramon Villarreal, payments sector global lead, Red Hat

Villarreal said that "there is big potential in terms of innovation. I think that is the shift that is necessary to accelerate the utilisation of the applicability of DORA – looking into innovation, the long term benefits, what we can bring to the customer, and the potential security benefits.

The concept of uptime, or the amount of time a system is operational and available, is a crucial metric in this new landscape. In the world of instant payments, any downtime can have significant consequences. It's clear that there is a correlation between the age of a bank and its likelihood of experiencing downtime, often due to system upgrades or legacy systems. This highlights the need for financial institutions to invest in modern, reliable systems that can handle the demands of real-time payments.

However, it's not enough to simply invest in new systems. Financial institutions must also be proactive in monitoring and improving their uptime. This requires a commitment to data collection and analysis, allowing institutions to identify and address any potential issues before they become major problems. By being data-driven, institutions can make informed decisions that enhance their resilience and ensure they are providing the best possible service to their customers.

In addition to uptime, financial institutions must also consider the threat of external cyber-attacks. The rise of new players in the financial technology space has brought with it an increase in potential threats. To combat this, institutions must be proactive in their approach to cybersecurity. This includes regular testing and practical trials to identify and address any potential vulnerabilities. By taking a proactive approach, institutions can ensure they are prepared for any potential threats and can respond quickly and effectively if an attack does occur.

"There's nothing new there, nothing from a practical perspective that a financial institution shouldn't be already doing in my opinion."

Kaspar Loog, director of product management, LHV Bank

05 | Conclusion

In closing, DORA marks a crucial advancement in fortifying operational resilience within the financial services industry. It introduces a thorough framework for managing digital supply chain and cybersecurity risks. However, it is important to understand that DORA is a supplement, not a substitute, for proactive risk management practices within financial institutions.

The EU's approach to operational resilience, as demonstrated through DORA, serves as a blueprint for other regions, setting the stage for a more secure financial sector. The evolution and increased interconnection of the financial industry underscore the growing importance of such regulations.

While there is ongoing debate about the necessity and effectiveness of regulations like DORA, the increasing reliance on digitalisation and third-party services makes a harmonised approach to ICT risk management imperative.

In our modern, interconnected world, operational resilience becomes a crucial business strategy. Despite its challenges, the benefits of risk mitigation, business continuity, and innovation potential make the ambitious journey worthwhile.

As the financial technology landscape undergoes rapid changes, institutions must adapt to survive. This adaptation requires a commitment to data-driven decision making, practical testing, and continuous improvement. By focusing on uptime and cybersecurity, institutions can bolster their resilience and prepare for future challenges. Therefore, the road to resilience, albeit challenging, is a journey that all financial institutions can and should embark on.

About

Finextra Research

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology news and information source. It offers more than 130,000 fintech news, features and TV content items to some 800,000 monthly visitors to www.finextra.com.

Finextra covers all aspects of financial technology innovation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide. Finextra's unique member community consists of over 40,000 fintech professionals and 200,000 social followers working inside banks and financial institutions, specialist fintechs, consulting organisations and technology providers.

The Finextra community actively participates in contributing opinions, ideas and comments on the evolution of fintech.

For more information visit **www.finextra.com** and become a member, follow **@finextra** or email us via **contact@finextra.com**.

About NTT DATA UK

NTT DATA – part of the NTT Group – is a trusted global innovator of IT and business services, headquartered in Tokyo.

We help clients transform through consulting, industry solutions, IT modernisation and managed services. NTT DATA enables clients to move confidently into the digital future. We are committed to our clients' long-term success and combine global reach with local expertise to operate in over 50 countries.

Visit us at **uk.nttdata.com**

For more information

Finextra Research
77 Shaftesbury Avenue
London
W1D 5DU
United Kingdom

Telephone: **+44 (0)20 3100 3670**

Email: **contact@finextra.com**

Follow: **@finextra**

Web: **www.finextra.com**

Finextra® | NTT DATA