Digital Operational Resilience:

The New Heart of Operational Risk

QA Financial (expleo) accourt PAYMENTS SPECIALISTS ReedSmith

Contents

Introduction

Digital Operational Resilience (DOR) describes an organisation's ability to avoid customer service interruptions, recover quickly from spontaneous server outages and fully appreciate potential vulnerabilities while adopting a proactive risk mitigation strategy.

As the wider regulatory environment continues to evolve at pace, adopting a strong compliance culture is no longer a 'nice to have' - it's a genuine prerequisite to business vitality and longevity. With the compliance era switching into next gear, remaining purely entrenched in the day-to-day operational challenges will leave enterprises at a marked disadvantage long-term. Fine-tuning DOR for sustained business gains means digitally rewiring business operations, such that operational change can be enacted swiftly when the regulatory guidelines inevitably shift.

Building a Culture of Compliance

Achieving and maintaining a robust bill of health on the DOR front will quickly become a key strategic objective for institutions operating within the confines of the forthcoming European Commission legislation, the Digital Operational Resilience Act (DORA), expected to come into force in 2024, and other similar international regulations, as well as future regulatory frameworks. Put simply, complacency around regulatory compliance will be the single biggest self-inflicted wound for enterprises moving forward, and they should be compelled to start routinely ruminating their DOR strategies.

This report - commissioned with QA Financial, and developed in conjunction with Reed Smith LLP, and Accourt Payment Specialists - offers high-level findings drawn from market analysis and personal interviews, further validating the concept of DOR as a fundamental business enabler. The report considers the current state, and understanding, of DOR and the future impact of DORA on the Banking, Financial Services and Insurance sector across the EU and UK markets.

Key findings:

20% of all financial firms interviewed recognise software quality as a risk area

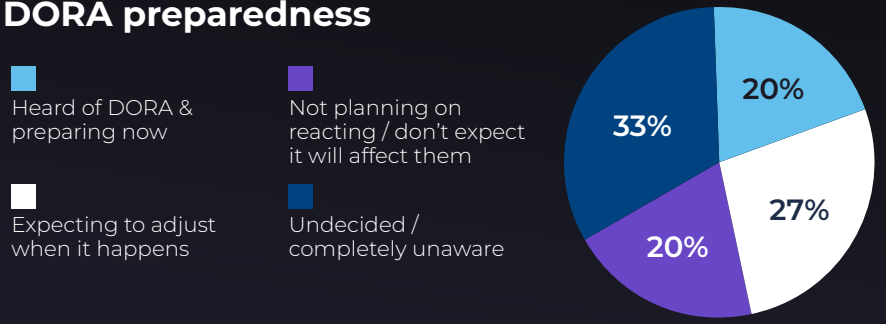
20% of firms recognised the DORA, while only one company is looking to take direct action as a result

25% of all firms interviewed explicitly recognised Digital Operational Resilience

1% The European Commission, which is drafting the DORA legislation, will impose steep penalties of up to 1% of average daily worldwide turnover from the preceding year in cases of non-compliance

Firms with increased focus explicitly due to regulation changes

DORA preparedness



50% of firms recognise an enhanced focus on Digital Resilience, driven by business demand for always-on access to systems and solutions and regulatory focus.

100% of firms with technologist board members have an enhanced focus on Digital Operational Resilience

Banks have the clearest routes of accountability

The shift in business-led needs to 24-hour accessibility for staff and clients is the primary concern around DOR for firms

Methodology

The term operational risk generally embraces a limited concept of digital operational risk. For regulators and businesses seeking greater resilience and improved risk management, the understanding is changing.

The objective of the research described in this paper sets to:

Evaluate the understanding of "digital risk" amongst senior leaders across financial services

Determine how regulatory drivers, including Financial Conduct Authority (FCA) rules taking effect in 2022 and DORA, are forcing firms to review their understanding of "digital risk", and their governance processes

Assess the business drivers that now require systems to be "always on" as customer and user expectations are shaped by the speed everyday technology in our hands is updated

Validate how "digital risk" needs to take more into consideration; particularly software quality, continuous testing, coding quality, and a revised approach to governance

For this analysis QA Financial Research analysed feedback from 39 traditional and challenger banks, asset managers, insurers, payment firms and other Fintechs in the UK and EU. The approach ranged from personal interviews with industry executives to deep dive analysis' of their annual reports and customer facing websites.

Within the organisations, those approached held a variety of positions, from quality engineering and risk managers to chiefs of technology and board members. This has allowed us to assess both variations across the sector as a whole and also how digital operational risk is seen and communicated between roles within the company. More specifically, we sought to take an early temperature on awareness of DORA and more generally regulatory focus on the area.

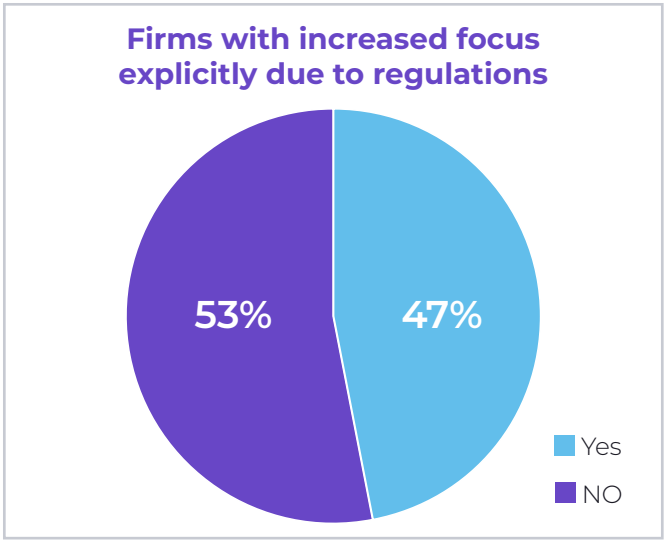
Understanding of Digital & Technology Risk

When asked about their understanding of digital and technology risk, Digital Operational Resilience (DOR) was recognised explicitly as a risk category in just over half of cases.

The majority of these were by banks, insurers and asset managers, with fintechs largely not focusing on this, and only one fintech considering DOR in this way. While fintechs largely recognise security and data management risks, there is no clear focus on DOR as a category - viewing digital change as a growth opportunity before a risk area.

Security is the dominant category recognised under digital risk, with almost all firms surveyed acknowledging it directly. This is largely the result of an appreciation for increased regulatory focus around security risk. Just over half of all firms acknowledged the issue of data management risk, with fintechs and asset managers giving it more regular attention than banks.

Additionally, software quality was generally not seen specifically as a risk category, with only **20% of all firms recognising this as an area of risk**, increasing to only **25% among those that explicitly recognised DOR**. Across the less senior survey participants interviewed, it was more common to find recognition of software quality as important, but this did not align with their CROs' objectives. It was primarily seen as a knock-on effect of data management, wherein poor software quality could open the company up to attack or leakage, rather than downtime or more general resilience.



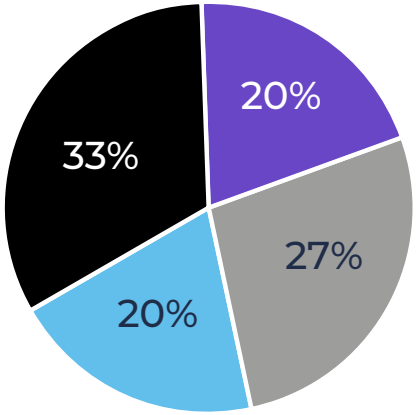
Recognition of DORA

DORA is hardly on the business agenda. Only 20% of firms recognised it, and only one company was looking to take direct action as a result of it. There was roughly equal acknowledgement of the act across each field, indicating that no single sector is particularly engaged.

"I am not up to speed on that and I know about a lot of regulations"

- Insurer

Responses to DORA

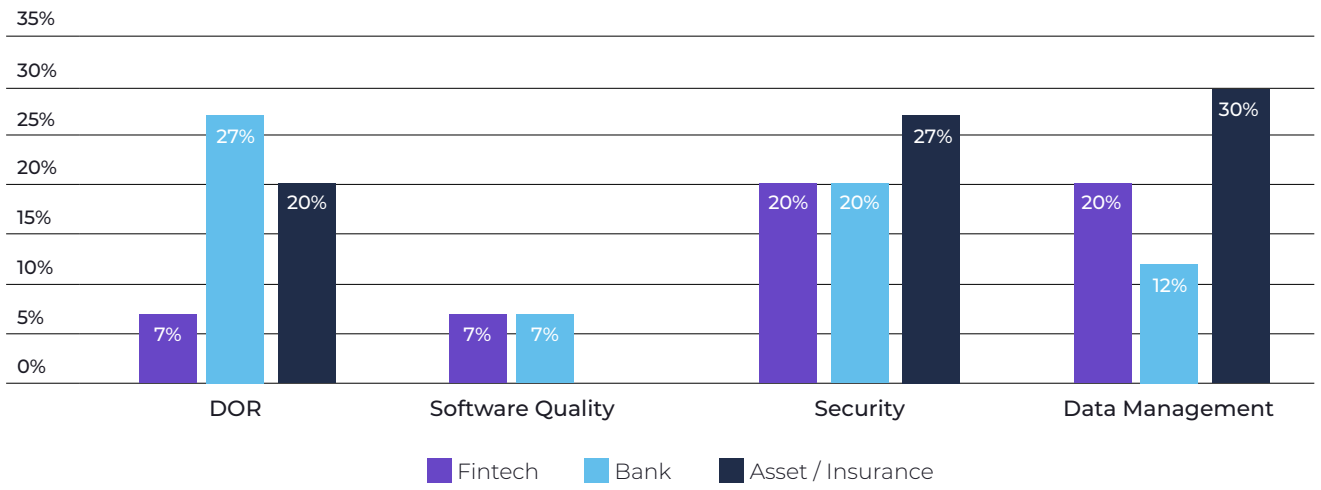


- Heard of DORA & preparing now
- Not planning on reacting / don't expect it will affect them
- Expecting to adjust when it happens
- Undecided / completely unaware

One challenger bank acknowledged a Basel Committee report on this, but not DORA, while some but not all banks report giving focus to the forthcoming Prudential Regulation Authority (PRA) changes of regulation.

While DORA itself was not recognised, the general increase in regulatory focus was noted by most banks and insurers. The FCA and PRA's focus on cybersecurity and operational resilience as a whole were noted several times by banks, referencing changes expected in 2022. Within firms themselves, half recognised an enhanced focus on operational resilience. This was driven equally by business demand for always-on access to systems and solutions and regulatory focus. One bank noted that the focus was largely on infrastructure around accessibility and responding to outages, with a **renewed interest due to COVID and the need for remote access.** To address this, it formed a continuity and security directorate.

Among asset managers and insurers, there was more of a split between those with increased focus and those without any at all. Those without any focus reported this to be a result of a more classical board structure that did not prioritise digital operational risk, focusing instead on business continuity and needs, such as actuarial risks. Those with increased focus spoke of monitoring current effectiveness, rather than driving to improve resilience directly.

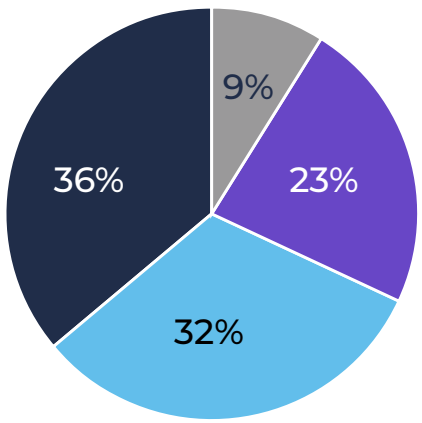


Chain of accountability

The chain of accountability varies across and within sectors. The greatest trend however, is that all firms that have technologist board members show their enhanced focus on digital operational resilience through improved systems and processes and a clear and direct path of accountability to the board. Equally, these firms often have multiple paths of accountability, normally in parallel to the CTO and CRO or risk committee.

Banks often had the clearest routes of accountability, having already made changes in recent years, for example setting up new directives or disconnecting positions like Strategic Information Security Officer (SISO) from the technology department. Only one fintech and a single asset firm still had accountability limited to the local or department level. This is likely to change for the asset manager as they noted testing teams have already grown dramatically in the last 5 years and the transformation is now growing upwards in the company.

The proportion of firms whos path of accountability reaches the board or CRO



Impact on recruitment

Almost all other firms in every field took accountability to either a C-suite officer or the board, if not briefing the CEO directly. One insurer already has a third party that oversees vendor accountability. Another buys in expert advice at a senior level to monitor and challenge the CRO and COO on accountability. There seems to be little focus on site reliability engineering as an end in itself. While automation and CI/CD are noted by firms moving towards DevOps, scalability of systems was not called out as a focus. Roles are being affected by the additional focus being granted to digital operational resilience. CSOs, CISOs and security architects take the primary role in dictating changes to requirements, following the dominant focus on security risk and regulation.

> **Testing teams have generally increased, sometimes by as much as threefold within the last five years.**

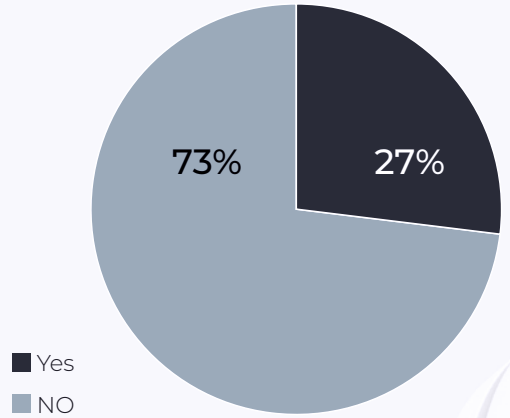
A European bank that is currently formulating its next four-year plan is set to make direct reference to DOR and quality, after having previously focused on measurable up-time and availability due to client needs. Changes here are set to affect test data and release management. Five firms reported an impact on board-level hiring practices, and these were primarily in the banking sector and among those firms that best recognised the different categories of digital operational resilience.

One bank noted a change in its hiring on the operational resilience team that is based in France to account for changing needs post-brexit. Similarly, an asset manager noted the increased focus on regulations as the UK diverges from the EU. One bank spoke of the introduction of a COO that had overhauled test data, functions and strategies to allow for greater transparency and more detailed statistics for root cause analysis. Another hired a new technology proficient director in support of the CSO's work around development changes and tool upgrades. This bank had seen an impact on all sections of the testing and development system, including around security in CI/CD.

An impact on CI/CD and security integration was not generally seen by other firms. This is perhaps due to their varied positions along the path to technical transformation. CI/CD is not a priority for firms that have only recently begun to transform. It can be said that generally the most impacted regions are test data management and increased defensive testing. An insurer made direct reference to this being the result of meeting measures required by the strategic information security officer. However, among Fintechs, there has been little effect on release management or test data management, while security is increasing the need for defensive programming.

Asset managers and insurers noted the same focus on defensive programming while also highlighting better care for test data, having transitioned from anonymised data to purely synthetic test data.

% of firms reference direct impact on hiring practices at board level



Best practices

There are two primary drivers for change around operational resilience. One being the evolution in the regulatory environment.

> **Some experts project that DORA will seek to impose fines of 1% of average daily revenue as a result of vendor software problems.**

Even for UK firms, DORA is a factor - an executive at a UK supervisor pointed out the UK commitment to ensure UK regulations and standards are sufficiently aligned to allow businesses to operate across the EU borders. Within the UK and elsewhere, digital factors and processes form a growing part of the regulatory framework.

Secondly, the need for 24-hour accessibility for staff and clients pushes a business-led need for high availability and greater resilience. Several firms stated this was their primary drive behind concerns around DOR.

Should you prepare?

While only 20% of firms had heard of DORA and plan to act, just under half of all firms expect to have to adjust to it, on discussion of DORA. Fintechs were the most unaware, generally expecting to just respond to requirements as they are enacted, but this response was mimicked even by some banks and insurers. This strategy leaves businesses open to a higher shock and diversion of resources as they struggle to meet the requirements in the closing months, instead of moving to respond now.

Some firms are already preparing for changes in FCA guidelines for managing and reporting on operational resilience in March 2022, with one bank already embedding operational risk controls into their first line of defense.

How to align with DORA now?

While the legislation has not fully crystalised, some facets can be addressed. As noted in the following case study 2, a key point to align on now is ensuring vendors strictly meet software quality standards, rather than self certify.

Best practices for risk reporting

It is clear from interviews that those firms with technology inclined board hiring practices have improved systems of reporting and accountability. There is regularly a clear route to the board, or even multiple routes of communication here.

It has been noted through these interviews that some quality heads are not currently aware of regulatory needs and are simply responding to piecemeal requirements passed down to them. By cementing routes of communication and accountability, these members will be better educated and therefore derive greater importance from their requirements. It may be necessary to allocate additional time or expenditure to vendors to ensure they certify and provide improved testing and valuable metrics.

By improving report metrics, monitoring becomes easier, allowing firms to perform root cause analysis. A well-prepared insurer requires vendors to log their liabilities within 10 days. Several banks reported that improved testing strategies allowed for greater transparency and accountability across the company.

> **A fintech reported the introduction of a new full-time team under the CRO focused on operational resilience.**

Two firms looked to bring in a separate consultant to evaluate risk, reporting directly to the CRO or the board.

Concluding observations

Most firms are on the back foot for responding to forthcoming regulatory requirements, including DORA. In fact, just over half recognise the importance of a broadened and deepened approach to digital operational risk directly. Security and data management in particular are seen as important risk categories within the industry.

The most powerful and immediate drivers of change in this area are business requirements to move to an always-on stance. As DORA and similar FCA/PRA regulations come into effect, a greater emphasis will need to be put on software quality, with related revisions to risk governance, a factor only acknowledged by 20% of firms.

Current chains of accountability do not uniformly reach the board, though just over half of firms do have a path here. This seems best improved by strengthening the board with more technologically savvy directors, a feature less present in more established banks, asset managers and most insurers.

Case Studies

Case study 1

A bank that was just starting its digital transformation, the priority is on securing front-end access for its brokers and clients. DOR is of course a part of this process, but only to the limit of securing these services. Strong focus on stability around these, mostly for remote working, business continuity and the continuous client access. Software code matters here, but only in basic measures of uptime and limiting vulnerability. This is not seen as a risk by the CRO as improvements largely pushed at local level, rather than dictated by CISO or otherwise.

The bank was not aware of DORA specifically, but expects that as the standards become clearer, the CISO will direct teams to meet the regulations. Path of accountability is from each tech to the QE, onto the CTO and to group COO. Separate reporting to CISO, now external to the tech group due to the increased importance of this position. There has been a clear impact on defensive programming and release management, as a security architecture team dictates new requirements. A new group head of data governance has been appointed to oversee a framework for test data provisioning and ownership. Specifically appointed a new director with a technology background who aligns with and supports the CISO here.

Case study 2

This bank has heard of DORA, and is beginning to align with its needs. They now assert defect liability on their vendors and require vendors to certify their software resilience through a third party. The increase in focus is largely driven by upcoming changes to FCA and PRA regulations, with direct reference to Bank of England joint papers and PRA questionnaires. More guidance around best practices is still wanted though. There is a clear path of accountability up the company. Teams report to a newly hired COO at board level and separately consult the CRO. Expert advice is also brought in to challenge current accountability on the board.

Site reliability engineering and outages are a clear priority for this bank. Additionally, recruitment at a team and board level is affected. Teams addressing operational resilience have grown 3-4 fold while the new COO has driven forward risk-awareness dramatically, increasing accountability across the firm. Since the COO joined, there is a drive for transparency in testing and reporting, with detailed test strategies and statistics, allowing the root cause to be passed to the board, driving capability.

Financial Firms Analysed

Our research encompassed analysis of annual reports, websites and some 20 personal conversations with executives. Firms covered were those below. Nothing in this report should be understood to imply an endorsement by any of these firms of any of the comments or observations in this report.

- Admiral Group
- Adyen
- Aegon
- Allianz
- Arbuthnot Latham
- Atom Bank
- Axa
- Bank of England
- Barclays
- BNP Paribas
- Close Brothers
- Curve
- De Silva
- Deutsche Bank
- Hiscox
- HSBC
- ISP
- Klarna
- Legal & General
- Lloyds
- London Stock Exchange
- M&G
- Metrobank
- Miller Insurance
- Monese
- Monzo
- Nationwide
- NORDEA
- Osper
- Planet Payments
- Quilter
- RBS
- Revolut
- Schroders
- Skrill
- Standard Chartered
- Starling Bank
- Stripe
- Transferwise

Industry Dissect with Reed Smith LLP

Reed Smith LLP is a leading global law firm that acts for 48 out of the 50 global banks, supporting their DOR legal and compliance strategies, offering best-in-class advisory.

Howard Womersley Smith
Partner, Reed Smith LLP

Q1 From your previous experience with Standard Chartered bank - what insights can you share about implementing regulatory-induced change from inside a bank?

The most incisive viewpoint I can share from my experience working in the bank, is that all projects - particularly those that are induced by regulation - involve a significant amount of cross-department collaboration and interaction. When all of these departments come together, they will establish an end-to-end process from feasibility, due diligence, all the way to implementation into the business. One of the components in between that process is the legal and compliance perspective, which comes within my remit. Understanding the impact of the regulation from an internal, customer and a third party supplier perspective is essential to achieving regulatory compliance. This often involves changing how a regulated firm conducts its daily business and how staff members behave within it. It may also require the contractual relationships that a regulated firm has with its customers or suppliers to be uplifted, as well as the business relationships themselves with those third parties.

It may of course be a combination of all of those and more as sometimes the messaging of a certain regulated business may also have to be adjusted. In terms of a real life example, we've seen how regulation has required key information to be given to consumers when issuing a loan.

Q2 How can financial institutions ensure their ability to sustain service delivery consistently in the face of external threats?

That is the killer question. In the context of the relatively new subject matter of Operational Resilience - which encapsulates how an organisation can maintain business continuity when impacted by an operational event or shock - operational shocks can destabilize the operation of a business. Being operationally resilient, so to speak - by virtue of implementing certain preparations to respond to these shocks, and to reduce their effect should ensure that the business continues, can ensure you remain largely unaffected however. Those preparations are key to sustaining service delivery from external threats that turn into operational shocks. The key to a robust preparation strategy is appreciating the perspective of the customer.

In an Operational Resilience context, an important question regulated firms need to ask themselves is: how could an external threat affect my customers or clients? If we are looking at prevalent external threats, the challenges that the UK financial regulators have referenced are typically around cyber attacks and therefore cyber risk. Cyber attacks target technology systems and the data hosted within them. Technology is something that all regulated firms rely on and banks, in particular, are highly reliant on in order to deliver its services to consumers, through online banking, ATMs, or back office processing. Once customer data generated by the banks using that technology is stored in a cloud environment, the risk of external threats becomes omnipresent.

Operational Resilience rules are challenging regulated firms to come up with a way to maintain business as usual (BAU) even when their technology and/or operations have been attacked or otherwise disrupted. This can only be achieved through careful determination of what is considered to be your important business services; a mapping of the systems and processes used to support them (which will invariably include third party or outsourced service providers); and how much tolerance they have to disruption before the provision of their services to customers is affected - this is known as impact tolerance.

Scenario testing is encouraged in order to evaluate the impact tolerance and adjustments will need to be made to increase that tolerance where it is found to be too weak.

UK financial regulators realise that it is not possible nor an efficient use of resources to attempt to make every component of a regulated firm's business completely resilient to operational disruption. They therefore recognise that firms will need to prioritise their most important business services.

The important differentiator of Operational Resilience to operational risk for example is its requirement to focus on the outcome of how a regulated firm's customer base can continue to be served. Managing the risk, which may lie in the quality of IT systems used or security used within them for example, is a key component of achieving that outcome.

This outcome-based approach requires firms to start its assessment of that risk with the customer as the front line and to work back from there into the firm's back end infrastructure, looking at its systems and processes along the way.

Q3 As an organisation with a very strong technology & data law division, how do you see Reed Smith influencing and advising customers around the Digital Operational Resilience imperative?

The advantage that we have at Reed Smith is that we act for 48 of the top 50 banks in the world. Banks are really at the heart of this new area of regulation - Operational Resilience or OpRes as we shorten it to. They are the best example of where OpRes will apply, but it doesn't just apply to banks, it applies to other types of financial services organisations, as well as financial market infrastructures such as payment systems. However, in this instance I'll focus on banks. By virtue of having a client base we see a lot, we get to gauge how customers are responding to new regulations, how they're preparing for them, and how they're responding to those regulations once in force. We can see if they are maintaining a level of compliance for example.

Those kinds of insights are hugely valuable, the kind you don't get in other sector-specific organisations as people seem more reluctant to share information than in banking. I'm often asked by bank clients "what are others down the street doing?". We obviously don't identify who's doing what, but we can parlay the sentiment of what's happening elsewhere. That sentiment is often of interest to those keen to get a sense of what the competition is up to, particularly if they feel underprepared themselves and want to be reassured that their competitors are in the same boat.

Q4 What areas are Reed Smith best positioned to help customers with, in the context of DORA?

When I was talking about that end-to-end activity within a bank, I highlighted pieces that fall under the remit of legal and compliance. At Reed Smith, we're a law firm focused on legal and compliance solutions - we probably lean more towards legal than compliance and yet we are extremely well versed in regulatory-induced projects.

Part of the mapping exercise I spoke about earlier will involve looking down a firm's supply chain and assessing the contractual relationship that binds the firm to its supplier.

The problem at looking at the contracts however is that they are likely to have been negotiated over many months, without consideration for Operational Resilience or other regulations that govern a regulated firm's engagement of third party suppliers.

At Reed Smith, our forte is uplifting those contracts to comply with Operational Resilience requirements, as well as other outsourcing and third party risk management rules such as the EBA Outsourcing Guidelines and the UK PRA's equivalent rules on outsourcing.

On the periphery of all that, there are other areas where we can help to establish an end-to-end approach to OpRes projects - such as mapping the relationships the bank has with third party organisations and establishing the nature and extent of these relationships.

This involves looking at the contract, looking at how it has evolved over the years, looking at how easy it is to negotiate changes to that contract and engaging with the third party supplier. We are also talking in the context of banks that have thousands of relationships, meaning it's very difficult to put every third party supply relationships under a microscope. Sometimes you have to standardise the approach; establish a project to map numbers and data and overlay that approach over those, rather than the specific details of each relationship.

And yet, what we've seen as particular failures in these types of projects is where banks over-commoditize by imposing a new contractual amendment on them without any explanation. This isn't feasible - we don't live in that much of a faceless world. All of us in financial services work within a relationship matrix and those relationships are based on humans getting to know each other, and therefore we need to put the human touch into these projects.

Q5 What's your personal perspective on the growing importance of Digital Operational Resilience at board level?

That's an easy one. Operational Resilience is viewed by the UK financial regulators as no less important than financial resilience. This sentiment really underscores the incredible significance of OpRes - framing it as important as something that was created as a result of the 2008 financial crisis. So if that doesn't capture boardroom attention, I don't know what will. Also, DORA will have far-reaching implications for financial services organisations by tackling pervasive issues, such as cyber risk, which by their very nature will affect the whole of a regulated firm's business. It therefore merits sharp focus at a board level.

Q6 Do you have any predictions for how institutions will navigate the future Digital Operational Resilience roadmap?

I think they will navigate the road ahead with difficulty because quite frankly, they haven't quite adopted the right mindset yet. Regulated firms who fall within the scope of the Digital Operational Resilience Act (DORA) within Europe and the equivalent rules in the UK are still tussling with the outsourcing and third party risk rules, such as the EBA Outsourcing Guidelines.

Many of them haven't achieved the level of compliance that is required by the end of this calendar year (2021).

For those organisations to then be confronted with additional rules that are even more sophisticated; more pervasive; require a deeper look under the bonnet;, in order to achieve a particular outcome (which itself may require a compliance mindset change) is going to be a very steep learning curve.

The UK PRA realises this and announced in a speech earlier this year that it does not foresee firms will have done all the work required by its deadline of the end of March 2022. It does however expect them to have completed a compelling gap analysis to the extent that it can identify where its major shortcomings lie and therefore which areas need more work.

Q7 What are your thoughts on how the Digital Operational Resilience landscape is evolving across the NY, HK, SG, and UK markets? Have you identified any noteworthy nuances in different jurisdictions?

I have.

The US banking regulators issued a paper at the end of 2020 on how the largest and most complex domestic banking organisations can achieve Operational Resilience. The difference here from what we are seeing in the UK and Europe is that the US financial regulators did not issue any new regulations on OpRes but rather than brought together the existing regulations, guidance and common industry standards in one place to assist in the development of comprehensive approaches to OpRes.

Hong Kong has a similar view to the US regulators but is considering whether additional rules are required in order to implement the Principles for Operational Resilience issued by the Basel Committee on Banking Supervision back in March of this year (2021).

Singapore's rules on OpRes have focused on managing a safe working environment during the pandemic. Although Singapore has had in place Technology Risk Management rules covering similar concerns to OpRes since 2014.

Closer to home, from a pure terminology perspective there is a difference. Whereas the Europeans use the term "Digital Operational Resilience", we in the UK simply refer to Operational Resilience or OpRes. This follows the same terminology used by the Basel Committee's Principles for Operational Resilience. These principles obviously apply to banks only whereas the UK OpRes rules and DORA have a wider scope. In particular, DORA will for the first time put major ICT service providers within the scope of supervision of the European Supervisory Authorities.

The UK is ahead of the Europeans in this area by already having issued its Operational Resilience rules (not digital), which will come into effect at the end of March 2022.

Coincidently, those rules come into effect at the same time as the UK version of the outsourcing and third party risk rules. This goes back to my point about how difficult it will be for firms to navigate these rules. With a catalogue of different rules coming at the same time - different levels of sophistication and complexity - it's going to be challenging for organisations to get to grips with all of this at once.

The UK is ahead of Europe however only in terms of issuing the rules, not in preparedness. In terms of preparedness of financial institutions in Europe, I think they've struggled to achieve compliance with the EBA Outsourcing Guidelines, just as the UK institutions have. With a little longer to go until DORA is introduced, I think they've got some much-needed breathing space and time to digest the EBA Outsourcing Guidelines before moving on to some more sophistication, as DORA ultimately is. I do think this phase of recalibration will prepare them to absorb and bed in the effects of DORA. Whereas if a UK regulated firm took the current rules literally, I think they would be a rabbit in headlights.

The Five Pillars of Digital Operational Resilience

While it can be difficult to prepare for a regulatory framework that we don't fully understand, with constraints that aren't yet fully defined, enough is known at this current juncture about the impending DORA regulation to begin setting the foundations for a pre-emptive compliance strategy. What we do know is that DORA will introduce an unprecedented framework of cybersecurity oversight for technology service providers, with a particular emphasis on cloud computing and 'mission critical' operational functions.

While this is a lot to absorb, think of DORA as just one stop on the road to Digital Operational Resilience. The following five-pronged approach helps light the way for enterprises navigating this new ground and supports the compliance strategies of enterprises.

"UK firms need to be closely compliant to the European Commission DORA legislation, to support innovation, resilience and security in their European jurisdictions."

Jamie Merritt, CEO at Accourt Payment Specialists

01

Building DOR awareness

With any new piece of impending legislation, there is a necessary discovery phase that will inform the direction of compliance strategies. But first, you need to figure out the scope of work required, allocate resources accordingly, and acknowledge the opportunities that come with enhanced DOR. This 'education' piece is the bedrock for getting it right, and to build an understanding of possible regulatory outcomes, as they pertain to your individual company's current modus operandi.

"True resilience needs to start with the operations strategy and filter down through the organisation."

Rachel Saunders, Client Director at Moorhouse (an Expleo company)

02
Training and coaching

Ensuring internal personnel are completely up to speed on the implications of DORA for their business is very important. This means coming up with a development programme that is informed by industry and regulatory experts, to help staff become attuned to new procedures that will underpin a strategy of compliance. They'll need to be well versed in the new incident classification standards, new terminology and acronyms related to the new legislation. For the staff that will shoulder the responsibility for testing and monitoring, bespoke tutelage will be required, as will bespoke AML (Anti-Money Laundering) training and coaching - and relevant checks will need to be in place to gauge monitoring effectiveness. These staff members will be the eyes and ears of the company in the resilience arena, and should be trained comprehensively to spot system weaknesses that could undercut overall operational resilience.

03
Vetting third-party providers

Many financial institutions lean on the services of third-party vendors to support the customer journeys and bolster their overall service offering. While leveraging a network of service providers can be wholly beneficial, it also reduces an institution's ability to control their operational fate, so it's important to create a register of all third party providers. When key points of the customer journey are outsourced, it's so important to know where the reliance lies. It would be advisable to conduct an impact assessment to uncover the level of reliance on this outsourcing, ie: is this substitutable? And more importantly, what would happen if that outsourcing was compromised or decommissioned? Properly gauging the rigour of these vendors and identifying any vulnerabilities is a must when it comes to executing a firm DOR strategy. Ultimately, you want third-party organisations with the technical acumen, esteemed industry standing and repertoire of tools to enable fast-tracked, regulatory-compliant DOR.

04
Robust testing

Then, unvarnished assessments of internal testing structures and processes will need to be conducted. Some aspects of DORA will mandate technical testing, so you need to fully appreciate the implications of this on your systems and staff. How are you going to do it, and who's going to do it? How regularly will testing be carried out and how will the results be delivered? Finally, and crucially, what actions will be taken on the end-results? These are just some of the key questions to ruminate on. The security and integrity of system architecture is fundamental to any compliance effort, and as we know, system outages are black marks on a platform's permanent record - undercutting credibility in the eyes of customers. Given the high stakes, it's worth the time and due diligence in establishing a sound set of testing procedures.

05
Reporting mechanisms

With a revamped testing framework in place, establishing a best-in-class reporting framework is the next port-of-call in the compliance game. This is about excellence of execution, and consolidating new standards for reporting requires expert guidance. There's also going to be a whole new set of reporting vernacular to get used to. Tightening up the communications around incident occurrences, and getting those processes better established will be paramount. Then we'll help you come up with a clear plan for managing reporting internally before it goes externally to the regulator. Once a regular reporting structure has been established, it will be easier for enterprises to meet reporting requirements with minimum disruption to operations.

"Changes to the EU and UK's regulatory landscape will impact an organisations senior management team who will be responsible and accountable for monitoring, approving, reviewing, and setting the direction of an organisation's risk management framework."

Angus Panton, Banking & Financial Services Director at Expleo

About the Authors

Angus Panton

Business Unit Director

Expleo is a global engineering, technology and consulting service provider that partners with leading organisations to guide them through their business transformation, helping them achieve operational excellence and future-proof their businesses. Expleo benefits from more than 40 years of experience developing complex products, optimising manufacturing processes, and ensuring the quality of information systems. Leveraging its deep sector knowledge and wide-ranging expertise in fields including AI engineering, digitalisation, hyper-automation, cybersecurity and data science, the group's mission is to fast-track innovation through each step of the value chain. Expleo boasts an extensive global footprint, powered by 15,000 highly-skilled experts delivering value in 30 countries and generating more than €1 billion in revenue.

+44 (0)7800 581350
angus.panton@expleogroup.com
expleogroup.com
@ExpleoGroup
@ExpleoGroup

Howard Womersley Smith

Partner

At Reed Smith, we believe that the practice of law has the power to drive progress. We know your time is valuable and your matters are important. We are focused on outcomes, are highly collaborative, and have deep industry insight that, when coupled with our local market knowledge, allows us to anticipate and address your needs. You deserve purposeful, highly engaged client service that drives progress for your business.

https://www.linkedin.com/company/reed-smith-llp/
reedsmith.com/en

About the Authors

Justyn Trenner

Director

QA Financial is an independent research, information and analytics provider. QA Financial's focus is on software quality assurance and the drivers of improved software risk management at financial firms. Based in London, QA Financial caters to a global audience and runs networking events in major financial centres in Europe, North America and Asia, as well as online seminars and conferences.

+44 (0)7703 162363

justyn@qa-financial.com
info@qa-financial.com

www.qa-financial.com

@QA Media

Jamie Merritt

CEO

Accourt is a leading provider of strategic and operational consultancy services to the payments industry worldwide.

Accourt specialises in addressing issues affecting the payments community. Our unique blend of experienced industry specialists and local market intimacy has positioned us as the advisor of choice for market leaders across the industry.

+44 (0)7880 958880

jamie.merritt@accourt.com


QA Financial

expleo

accourt
PAYMENTS SPECIALISTS

ReedSmith