Broadridge®

ENTERPRISE

Building resilience across borders

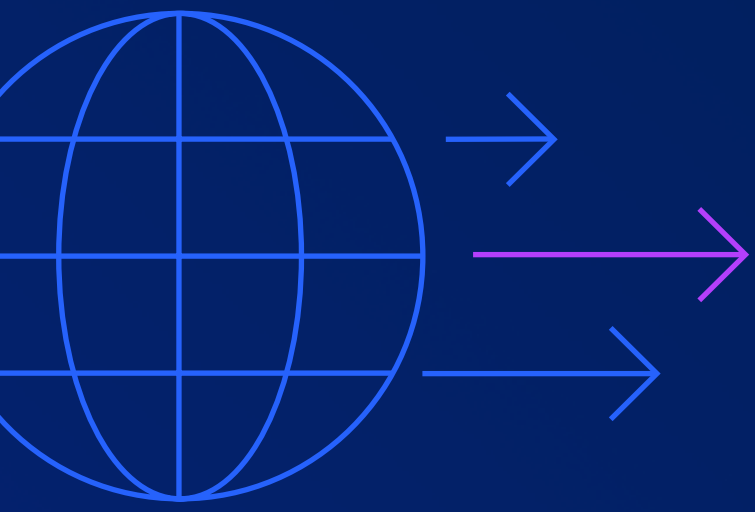
A holistic approach to global operational resilience and navigating the regulatory maze

Produced in collaboration with

Firebrand research

Ready for Next

TABLE OF CONTENTS



FOREWORD – THE NEED TO PREPARE

This report highlights the urgent global need for firms to attain higher standards of operational resilience, and the related regulatory maze that must be navigated across regions. It draws particular attention to the Digital Operational Resilience Act (DORA) in Europe which presents impacted firms with an onerous challenge and a fast-approaching compliance deadline of January 17, 2025.

OPERATIONAL RESILIENCE IS A PRIORITY. ARE YOU AT RISK?

Operational resilience is now firmly established as a critical priority for financial firms in all regions, driven by a fundamental requirement to strengthen trust and security in response to the growing risk of cyber attacks and disruptions – and underpinned by mandatory regulation.

Growing exposure to cyber attacks

Digital innovation and next-gen technologies like GenAI and blockchain are multiplying the scale of attacks and accelerating fraud – causing a dramatic increase in risk.

- Cybercriminals are 300 times as likely to target financial services firms than any other industry, according to Boston Consultancy Group.[1]
- In the next two years, financial firms will boost their investments in cybersecurity by 28%.[2]
- Cyber resiliency is especially challenging for companies in the earlier stages of digital transformation. Nearly half (48%) of Beginners and 29% of Leaders in digital transformation who are deploying next-generation technologies say they are facing cybersecurity challenges.[2]

Frequency of technology faults

Operational outages have also hit the headlines far more frequently over recent years, with firms exposed by both inhouse and third party systems.

- **Multi-industry:** A recent example is the significant Microsoft outage caused by a faulty software upgrade by its cybersecurity provider CrowdStrike in July 2024, impacting firms in all industries, and on a global scale.
- **Financial services:** The central role of market infrastructures, shared platforms and the growing interoperability of technology services mean that an outage in one critical service can have a far-reaching impact on all user firms. The high volume processing spikes during the onset of the global pandemic exposed a number of firms to unexpected system failures and costly downtime, yet this is but one of many examples.

A regulatory imperative that can't be ignored

Responding to the growing levels of threat, regulators in key jurisdictions spanning North America, EMEA and Asia Pacific have understandably introduced new or updated mandatory requirements for operational resilience. However the European Union's (EU) DORA regulation will be particularly challenging for many firms, some of which have yet to commence their readiness programme despite the January 2025 compliance deadline – thereby incurring regulatory risk.

DORA: THE CLOCK IS TICKING, BUT ARE YOU READY?

DORA is widely regarded as the most comprehensive and stringent regulation for operational resilience globally, requiring detailed self-assessment and planning relating to both inhouse technology solutions and throughout the third party technology supply chain. Yet there is a growing sense that many firms remain far from ready, exposing themselves not only to operational resiliency risk, but also to regulatory failure.

- **The industry is under "severe pressure"** to complete the necessary steps before January, according to the Association for Financial Markets in Europe (AFME).[3]

- In a concerning indication of readiness levels, it was noted that **only 4% of network managers are very comfortable** with the sector's operational resilience due to the necessity to examine their whole supply chain of providers, while **34% perceive the operational resilience testing of their custodians to be ineffective,** according to a poll of network managers conducted at The Network Forum Annual Meeting in June 2024.[4]

- **Remember: DORA has extraterritorial reach** – Despite being an EU regulation, DORA requires firms active within EU countries to report on their technology dependencies and resilience plans - irrespective of their headquarters' or providers' location. Further evidentiary requirements of DORA are significantly onerous as they require firms to catalogue and classify all of their provider dependencies, regardless of where those providers are located.

- **Enforcement penalties** – DORA requires EU member states to implement enforcement penalties and measures, which must be effective, proportionate and dissuasive.

- **Reputational damage** is a key risk for financial institutions failing to meet their mandatory resilience obligations, given the industry's heightened focus on trust, security and customer protection. Reputational risk is also an area of exposure for Board members responsible for meeting DORA's requirements relating to ICT resiliency and data protection.

MOBILISING YOUR DORA ACTION PLAN

DORA's January 2025 deadline means that firms must act now to assess the criticality of their information and communications technology (ICT) systems and services, and perform an impact analysis to ensure they can deliver an operating model aligned to DORA's compliance requirements.

DORA requires a full review of internal and third party systems and service provider data. This in turn means the creation of a comprehensive ICT Risk Management Framework and Digital Resilience Strategy including a full suite of ICT Risk Management Policies covering incident reporting and response, as well as third party ICT Risk Management. More detailed information is available in this report.

Requirements ahead of January 2025

At minimum, a financial firm's DORA action plan, in advance of January 2025, should include a detailed health check to assess the criticality of its systems and services, including a review of how closely aligned its existing ICT governance frameworks are with DORA's requirements. An impact assessment must be created that includes:

- Identifying important business services that, if disrupted, could cause harm at a client or market level

- Setting impact tolerances for each important business service, and taking actions to remain within them

- Identifying and mapping the people, processes, technology, facilities and information (including those of suppliers) that support important business services

- Developing internal and external communications plans in the event of disruption

- Maintaining an updated self-assessment document detailing how the firm has assessed its regulatory compliance requirements

Successful long-term compliance with DORA will require multiple further components, as covered within this report.

RESOURCING FOR DORA – IS THERE A SHORTFALL?

Faced with the urgent need to attain higher levels of resiliency within a mandated regulatory deadline, firms have an opportunity to evaluate the services of their external partners and service providers, including their ability to deliver the advantage of experienced resources and proven technology based on a mutualised, shared service pricing model.

Professional services

Firms lacking the capacity to resource their DORA resilience projects internally, or experiencing a shortfall of specific domain expertise, can turn to specialist third party support services to help achieve the highest level of protection, for example through:

- Detailed and well-informed assessments of ICT frameworks
- Validation of risk controls
- Insightful recommendations to rectify areas of vulnerability

When assessing their options, firms should take note that specialist professionals can attain Digital Operational Resilience Act Trained Professional status, a certified qualification evidencing a quantifiable understanding of the subject matter.

Tools and technology

It is of fundamental importance that firms establish multiple lines of defence to identify, manage and address ongoing ICT risk. Core to this is firms' ability to mirror their mission-critical technology functions in back-up environments that are the regulatory-prescribed distance away from their primary site, and that they can meet their prescribed recovery time objectives (RTOs) in the event of a cyber attack or outage. Firms need to be confident that their inhouse and third party service providers can meet these requirements to the required standard, and seek further outsourcing back-up if needed.

Another key technology consideration is the need for multiple layers of data protection, as DORA builds on the important focus of preventing the compromise of critical data assets in as robust a manner as possible. Cyber vaults play an important role in achieving this by providing an immutable and system-isolated copy of critical production data that is secure in the event of a cyber incident or outage.

FOREWORD FOOTNOTES

[1] Boston Consulting Group, 2019. Reigniting Radical Growth
[2] Broadridge, 2024. Digital Transformation & Next-gen Technology Study
[3] DORA Compliance: Untangling Key Hurdles to Implementation, AFME, May 2024
[4] Poll of Network Managers at The Network Forum Annual Meeting, June 2024

EXECUTIVE SUMMARY

The financial services industry is facing a global challenge to improve its operational resilience across all major markets and industry stakeholders:

1. **Strengthening operational resilience across financial services sectors:** Operational resilience is critical for financial firms to minimise the risk of cyber attacks and disruptions, and to enable efficient and effective recovery. Regulators in key jurisdictions are focused on the topic of operational resilience - several regulators in the US market, Canada, European Union (EU), UK, South Africa, Japan, Hong Kong, Singapore and Australia have introduced new or updated requirements or proposals in this area.

2. **The Digital Operational Resilience Act (DORA) covers many financial services sectors:** The EU, through regulations such as DORA, mandates that almost all types of financial firms implement robust measures to manage and mitigate operational and system risks. DORA requires firms to strengthen their operational risk management and governance frameworks, which presents a significant challenge for many as they adapt to its comprehensive requirements.

3. **Firms need to get ready for DORA now:** Although impacted financial firms must be compliant for DORA in January 2025, it will take months of preparation in order to meet their obligations, especially when it comes to a full systems review and service provider data reporting. Buy-side firms in particular may need to build in extra time to query information received from their outsourced service providers.

4. **Enforcement action is likely:** Regulators are prioritising operational resilience over many other areas. They are likely to be strict on non-compliance in order to demonstrate the importance they place on cybersecurity and operational risk reduction.

5. **Third party providers and inhouse IT will come under increased pressure:** The emphasis of regulators is on ensuring that critical systems of all kinds, including those of service providers, have received the necessary investment resources to provide operationally resilient environments. This necessitates a full review of the supply chain for these services, including nth party dependencies, regardless of their headquarters' or providers' location or regulatory jurisdiction.

THE GLOBAL REGULATORY PICTURE

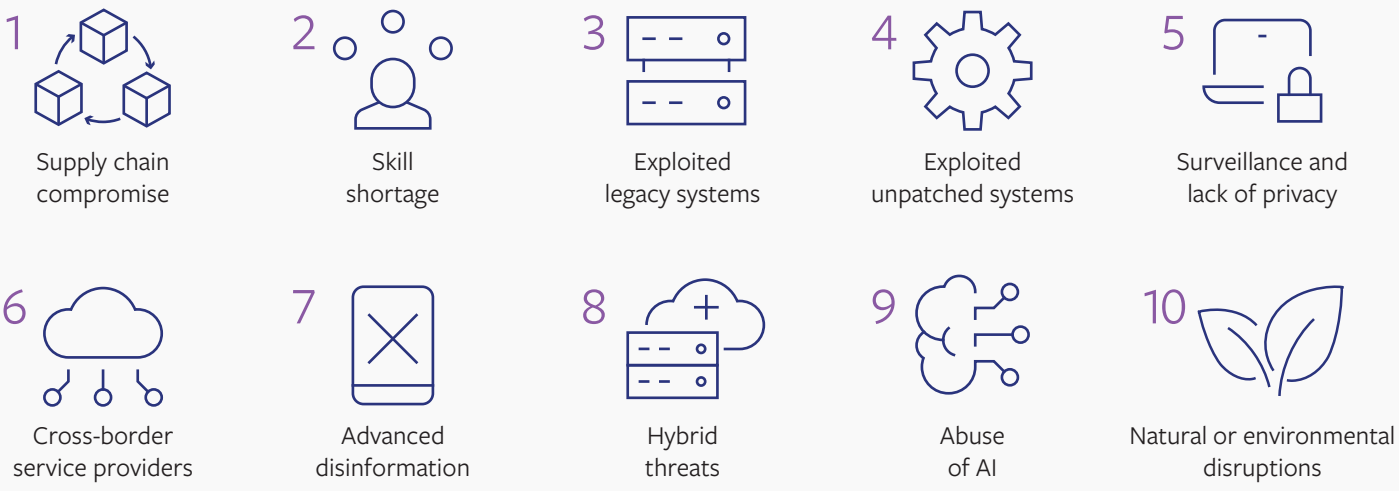
There is a heightened industry focus globally on operational resilience, particularly as it relates to cybersecurity and in the wake of the increased prominence of operational outages and ransomware attacks, particularly in the financial sector. The Digital Operational Resilience Act (DORA) and similar regulations across the globe are targeted at addressing the industry's best practices in operational resilience and risk mitigation in light of these developments, especially as the global geopolitical outlook continues to worsen. Regulators are beginning to work with cybersecurity-focused bodies to close the information gap when it comes to understanding attack vectors and sharing threat information internationally.

The new requirements are to take into account the increasingly digital nature of numerous industries, including financial services, and the increased sophistication of cyber crime. The variety and volume of cyber attacks has increased over time as cyber criminals have become more organised and well-funded by crime syndicates and nation states. The increasing prevalence of weather-based disruptions due to climate change are also under regulatory focus as regulators continue to model industry-level climate risks. Operational outages have also hit the headlines far more regularly over recent years such as a significant Microsoft outage caused by a faulty software update by its cybersecurity provider CrowdStrike in July 2024.[1]

According to the International Monetary Fund (IMF), the financial sector has faced more than 20,000 cyber attacks over the past 20 years, causing $12 billion in losses. The European Union Agency for Cybersecurity (ENISA) catalogues the rising cyber threats across the region as shown by the graphic below based on its predictions looking out to 2030.[2] These threats can be considered to be global, given that cybercrime is generally borderless and these criminals target a range of different market participants along the financial services supply chain. The increasing use of artificial intelligence (AI) by cybercriminals is also concerning from both a threat volume and increased sophistication standpoint.

Regulators are keen to understand the dependencies and potential related systemic risks within the financial services sector as it becomes increasingly reliant on information and communication technology (ICT) tools and systems. The increased industry adoption of AI is also on the regulatory radar as many of the AI providers are already within the ICT category due to their role as cloud technology providers, which could add to concentration risk. These and other next generation technologies must therefore be implemented responsibly by financial institutions, taking into account new cyber risks and potential supply chain dependencies in the longer term. The Microsoft CrowdStrike outage in July 2024 presented a perfect example of these concerns realised in a global context.

ENISA'S TOP 10 FORESIGHT CYBERSECURITY THREATS FOR 2030



Cybersecurity and cyber hygiene have also become a financial institutional priority from a risk mitigation, reputation and competitive standpoint. Broadridge's 2024 Annual Digital Transformation and Next-Gen Technology Study indicates that financial services firms are already facing significant challenges in addressing their cyber risks. Nearly half (48%) of the Beginners and 29% of the Leaders in digital transformation who are deploying next generation technologies indicate that they are facing such cybersecurity challenges (see the chart below).

The global move to shorten the settlement cycle is another important factor to consider that will impact the realm of operational risk and resilience. Many firms have ageing systems in their back offices that are in need of retirement and therefore could pose risks from an operational risk perspective if put under increased volume and scalability challenges. Bank own-builds and significantly customised vendor platforms also pose key person risks as the IT teams that built them near retirement and are therefore unable to continue to update them in line with market and security threat requirements.

PERCENT OF FIRMS REPORTING CHALLENGES ADDRESSING CYBERSECURITY RISK

Source: Broadridge 2024 Annual Digital Transformation & Next-Gen Technology Study

DORA is far from the only regulatory regime change related to operational resilience globally, though it is one of the most stringent and will impact firms outside of the boundaries of the European Union (EU) due to its extraterritorial nature. The below graphic highlights the global view of existing and incoming regulation related to operational resilience. There are numerous regulatory proposals and incoming regulations across the major markets.

In Canada, the Office of the Superintendent of Financial Institutions previously issued an advisory regarding Technology and Cyber Security Incident Reporting, mandating financial institutions to report significant cyber attacks, as well as updates to its E-21 Guideline in order to ensure that financial institutions implement operational resiliency measures in their processes and systems. South Africa's banking authority issued a new proposed operational resilience directive in April 2023 with a view to introducing the new rules by December 2024[3] based on the Basel Committee on Banking Supervision's (BCBS's) principles from 2021.

The US market has seen numerous proposals related to operational resilience over the last couple of years across the various segments of the market including proposals made by the Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC).

In July 2023, the SEC adopted final rules requiring companies subject to SEC reporting requirements under the Securities and Exchange Act of 1934, as amended, to disclose material cybersecurity incidents on Form 8-K and provide enhanced disclosure of cybersecurity risk management, strategy, and governance in annual reports beginning with annual reports for fiscal years ending on or after 15 December 2023.[4]

In the UK, the Bank of England, Prudential Regulation Authority (PRA) and Financial Conduct Authority (FCA) have added new rules related to critical third-party dependencies within the financial services sector. The three regulatory authorities issued a consultation on the topic in December 2023[5] and financial institutions must also now comply with new operational resilience requirements by 31 March 2025. The FCA is currently monitoring how firms are preparing for the new rules[6], which include

THE GLOBAL VIEW OF OPERATIONAL RESILIENCE REGULATION

new reporting requirements for disruptions and annual self-assessments for third party providers. They also introduce a new set of granular operational risk and resilience requirements for providers of mission critical systems, including supply chain risk management and incident management requirements.

Other jurisdictions, such as the Monetary Authority of Singapore (MAS) and Australian Securities and Investments Commission (ASIC), have implemented similar regulations.

In Japan, the government introduced the Economic Security Promotion Act in May 2022 to reduce the country's dependence on third party providers outside of its direct jurisdiction. The rule is much broader than financial services, but it will impact the sector.

Much of the global regulation, including DORA, reflects the Financial Stability Board's (FSB's) operational resilience guidelines[7] and therefore has some common ground for international firms to bear in mind:

- **Legacy systems and complex inhouse builds could spell big trouble:** Firms that have systems in place that aren't regularly being patched and updated in line with industry standards are likely to come under increased regulatory scrutiny. If firms have lifted and shifted these systems into a cloud environment rather than rearchitected them, the risks are even greater in the event of a cyber attack. Key person risk and internal resource constraints will also be a core consideration and likely burden for firms as they prepare to address their inhouse system readiness for the new operational resilience demands.

- **Recognise the global nature of third-party risk management:** The global nature of the markets is emphasised as any regulation is likely to be extraterritorial. Very few firms will have all of their critical third-party providers and supply chain providers located in one regulatory jurisdiction, which means firms need to understand how each of the jurisdictions compare when it comes to the evaluation of key dependencies.

- **Critical third parties are about more than size:** The size of the provider isn't the only important factor in these assessments, it's also how impactful the service or technology is to the day-to-day running of a firm's operations. The critical providers to that technology or service are also extremely important to evaluate, especially if the provision of that system is dependent on one particular cloud provider, for example.

- **The importance of regular and timely reviews and communication:** This is not a 'one and done' exercise and regulators are being encouraged by the FSB to conduct regular assessments of industry compliance when it comes to monitoring and evaluating their critical services, both inhouse and via third party services. The timeliness of notifications when incidents happen, as dictated by the various requirements in each jurisdiction, is also a focus of the supranational regulator.

- **Test, test and test again:** Business continuity plans and cybersecurity drills must be regularly reviewed and tested to ensure they keep up to date with current operational and technology set-ups, and with the latest cyber attacks.

- **Systems from front to back office are in scope:** Given the nature of operational resilience regulation, it is important to note that critical systems reside across the spectrum of functions within a firm and thus a comprehensive review is necessary to understand where operational risk management and cybersecurity deficiencies lie.

Regulatory changes are only one reason why firms need to focus on improving their resilience; the impact of significant downtime on clients, brand reputation and sometimes the market as a whole can be severe. Financial services as an industry is built on a foundation of trust and part of maintaining that trust is continuously proving resilience and risk mitigation. Supporting business continuity is contingent on understanding the existing estate of systems, services and data and technology environments across an enterprise and identifying any potential weak points as cyber threats evolve. Recovery time objectives (RTOs) that have been established by market practices and regulations need to be achieved to maintain compliance and minimise disruption.

THE CHALLENGES AHEAD

One of the challenging areas of compliance will be determining the criticality of internally built systems and third-party providers and the supply chain of vendors on which these systems and services rely. Regulators are required to examine criticality at both the firm level and the industry level, the latter of which is determined by the number of financial institutions that are dependent on a particular service or technology. These industry-level or systemically risky third parties will come under direct regulatory scrutiny.

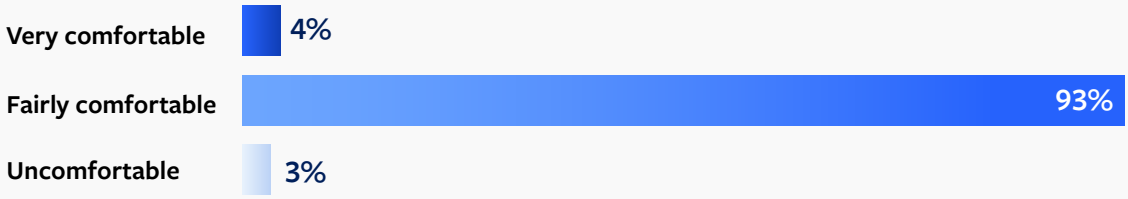
Smaller firms with fewer resources to commit to operational risk mitigation and compliance, and that don't fall below regulatory thresholds, may face more challenges from an implementation standpoint.

As noted by a Firebrand Research interviewee in operations at a buy-side firm, if a firm's critical inhouse platform relies on a smaller vendor for the conversion of data from PDF into digital form, then that vendor could potentially fall under the scope of DORA compliance. The potential for small providers that lack cybersecurity accreditations to come under scrutiny is of concern for all firms.

DORA's technical standards emphasise the need for firms to have a detailed understanding of the dependencies and operational risks within their home-grown technology stack. Not only should these systems be regularly stress tested from an operational incident and cybersecurity perspective, they must also be assessed from a long term support and governance perspective. If the provision of a particular function is dependent on technology that is only supported by a small number of individuals within an organisation, that key person risk must be understood and mitigated. This also means firms may need to add third party providers into the mix as a backup for business continuity purposes.

Operational resilience overall is an area that needs to be improved, regardless of specific regulatory requirements, to meet changing client expectations in this area. According to a poll of network managers at The Network Forum Annual Meeting in June 2024, there is some perceived room for improvement in the sector's overall operational resilience (see chart below). Only 4% of network managers are very comfortable with operational resilience due to the necessity to examine their whole supply chain of providers, including fourth and fifth party services that sit behind their outsourcing arrangements with custodians. These individuals are charged with conducting due diligence on all of their providers and DORA adds to the burden of data that must be collected and maintained over time.

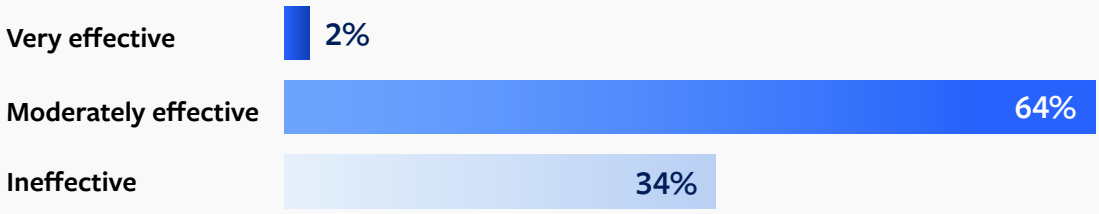
NETWORK MANAGER LEVEL OF COMFORT WITH SECTOR'S OPERATIONAL RESILIENCE



A Firebrand Research network manager interviewee notes that the requirements of DORA are significantly challenging because of the pressure to receive information from these providers and to potentially renegotiate contracts within a compressed timeframe at the end of 2024. While operational resilience up until this point has largely been about identifying alternative providers in a business continuity incident, DORA requires much more emphasis on resilience and security testing with existing systems, regardless of whether they are internally supported or via third party providers. To this end, network managers would like to see more proactive preparation and resilience testing from their custodians as highlighted in the chart below. Just over a third (34%) believe that the current effectiveness of their operational resilience testing is ineffective and the majority (64%) believe it is only moderately effective.

Given the global nature of the operational resilience regulatory push, firms should look beyond compliance with individual pieces of regulation and try to tie together their projects across multiple locations. By adopting a more centralised and coordinated approach such as introducing operational resilience health assessments across their business lines, firms can reduce the costs and complexity of compliance in the long term.

PERCEIVED EFFECTIVENESS OF OPERATIONAL RESILIENCE TESTING

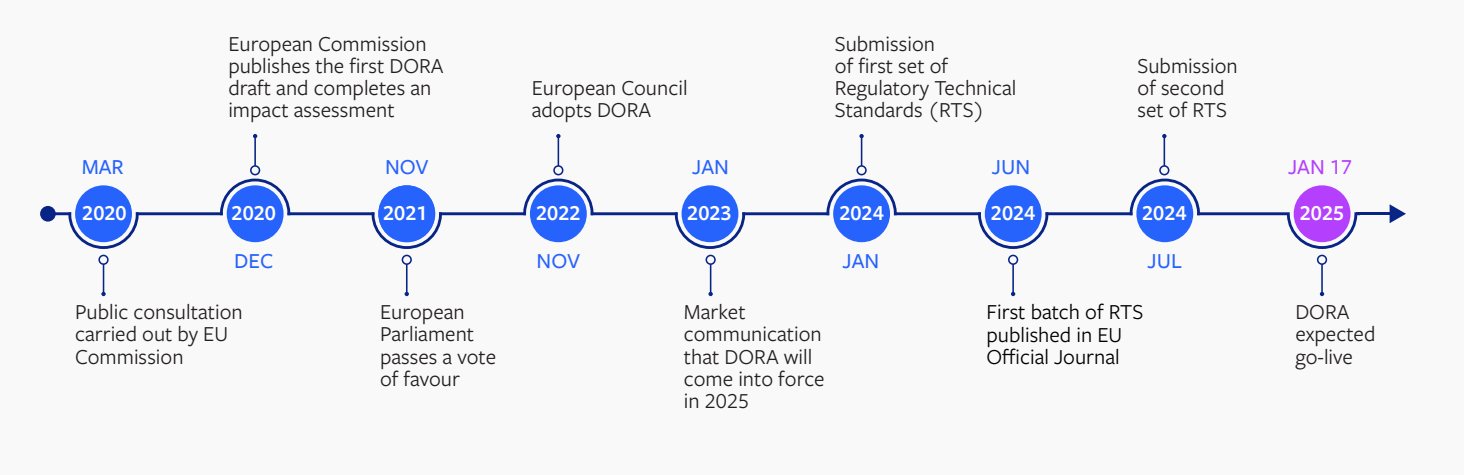


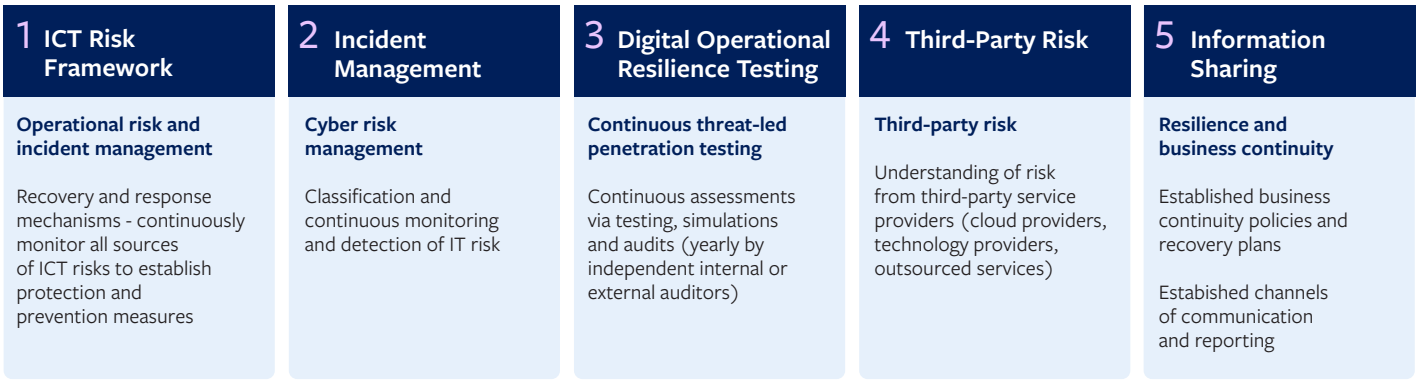
DORA: WHAT YOU NEED TO KNOW

The European Union is focused on improving the industry's operational resilience as part of its overall digital strategy, which is part of the regional government and European Commission's plans for competitive growth over the next decade. The Capital Markets Union (CMU) plan hinges on all member states adopting common standards and market practices to reduce cross-border friction and to improve the attractiveness of the EU market. To this end, the regulation harmonises the existing patchwork of compliance requirements related to operational resilience across the EU markets and establishes EU-wide standards for digital operational resilience testing. DORA also reflects the global regulatory push to better address cybersecurity and business continuity planning in the event of operational outages.

DORA came into force on 16 January 2023 and the regulatory text has been translated into two batches of policy mandates and technical standards by the European-level regulatory bodies as per the timeline below. The regulatory requirements, which include new governance and reporting requirements, apply from 17 January 2025. This leaves only six months between the publication of the last batch of policy mandates in July 2024 and implementation for the wide range of financial institutions in scope.

The industry has already raised concerns to EU-level bodies such as the European Securities and Markets Authority (ESMA) that the timeline is tight between the publication of the supporting legislative texts and the implementation date. The Association for Financial Markets in Europe (AFME) notes in its DORA paper[8] that the industry is under "severe pressure" to complete the necessary steps to meet the requirements before January. The European Cloud User Coalition (ECUC) in its feedback on DORA suggests that the implementation deadline should be moved out to 17 January 2028[9] to allow for sufficient time for the industry to prepare. However, given the strategic importance of operational resilience to the EU agenda, a delay of three years is unlikely.





The major components of DORA can be broken down into five separate categories as displayed in the diagram above. The overall aim is to ensure that financial institutions of all kinds understand and identify the potential risks within their operating environments and mitigate these risks by establishing more rigorous business continuity plans. The focus is on critical services that could have an impact on the overall operational resilience of a financial institution and in a wider context, on the stability of the financial markets.

As a result of DORA's focus on supply chain risk, there is also a strong extraterritorial component to the regulation. DORA requires firms active within EU countries to report on their technology dependencies and operational resilience plans regardless of their headquarters' or providers' location or regulatory jurisdiction. This essentially means that a firm with operations in the EU will need to comply, irrespective of where it is incorporated or located. The regulation also brings designated ICT providers under the remit of European regulators from an oversight and enforcement perspective.

DORA provides a harmonised framework for operational resilience risk management, incident classification and reporting, which requires firms to understand and regularly evaluate the criticality of their software, hardware and services. The Regulatory Technical Standards (RTS) establish requirements for firms to be able to demonstrate their governance of their critical services via regular testing, consistent metrics and tolerance setting for each critical service. Regulators will therefore expect firms to conduct regular reviews of these classifications, metrics and tolerances and to adjust them appropriately as risk profiles change.

The RTS also establish prescriptive requirements for the detection, monitoring and notification of IT security breaches within a certain timeframe. These will be familiar to firms that currently comply with the General Data Protection Regulation (GDPR), but they extend the remit of breach notifications from personal data to any type of data or when a firm's services are impacted more generally. The RTS require firms to meet prescribed RTOs when handling an operational outage or cybersecurity event. The main requirements of DORA therefore comprise:

- **Strategic executive ownership and responsibilities:** Board-level responsibilities related to the governance and oversight of ICT resiliency and data protection.
- **Prescriptive ICT risk management framework requirements:** New standards for the management of ICT services and providers, and business continuity planning.
- **A full system review:** Firms need to understand all of their internal and external system dependencies, including people, processes and technology.
- **Incident management and reporting:** Specific processes for the reporting of ICT related incidents using prescribed templates.
- **Stress testing requirements for firms and their providers:** The establishment of an annual operational resilience testing process including threat-led penetration testing.
- **Enhanced due diligence for critical service providers:** Oversight throughout the lifecycle of the vendor relationship including assessment of the full supply chain of providers' underlying critical services.

THE COMPLIANCE OUTLOOK

Overall, DORA has a huge number of requirements that touch nearly every part of a financial institution's business. It builds upon long-established guidelines for the management of outsourcing relationships, for example, and reflects the regulatory assumption that most firms have in place robust governance and control frameworks across their entire service provider community. The emphasis is not on pushing responsibility and liability onto these providers, it is very much on requiring financial institutions to take ownership of these relationships. To this end, firms must conduct regular data and system criticality assessments alongside stress testing exercises. They need to provide evidence that they have established the appropriate governance and compliance controls, which will move further toward near real-time visibility on these controls over time.

Firms struggling to fund internal system updates and upgrades will need to take a long hard look at their ongoing capacity to meet changing industry operational resilience requirements. Cybercriminals are well-funded and increasingly professionalised in their manner of operating with 'as a service' cyber attacks such as ransomware as a service available for use across the black market. Keeping ahead of cybercrime dynamics as well as the changing requirements of clients necessitates a significant amount of IT and operational investment. Operational resilience is a persistent requirement and the stakes will only get higher as cyber risks, climate and operational risks increase over time.

EU regulators are also working with bodies such as ENISA to determine how to establish a hub for secure information sharing amongst relevant authorities from a cyber threat perspective in particular. The sharing of this information internationally is a likely next step and this is why reporting standards and operational resilience data definitions are expected to evolve further as other regions build out their own reporting requirements. This means that firms must expect further refinements to the DORA regime over time, especially when it comes to reporting. DORA will not be a 'one and done' exercise.

On the enforcement front, financial penalties for firms regulated by DORA have not been set within the RTS and it will be up to each EU member state to determine appropriate administrative sanctions and remedies for violations of the regulation. The EU-level regulators have indicated that these penalties and measures must be effective, proportionate, and dissuasive. While DORA does not specify criminal penalties for infringements, EU member states are also free to provide for such penalties in their national law. The reputational damage of such a penalty on a financial institution is another significant aspect for consideration, given the industry's focus on trust and security.

A Firebrand Research interviewee that works as asset manager operations head notes that DORA can be seen as an extension of regimes similar to the UK's Senior Manager and Certification Regime (SMCR), which holds individuals accountable for noncompliance. The Board responsibility for instilling and maintaining more rigorous operational process governance across the organisation is of significant concern for C-suite executives that are aware of DORA's requirements. There are potential benefits from DORA from a better process governance, oversight and operational risk reduction stand-point, but the reputational risks are high for both individuals and their organisations.

As well as the tight timeline for compliance, one of the greatest DORA-related challenges is the lack of awareness across the C-suite executive community about the importance of meeting these new requirements. Large European banks, insurers and asset managers may have a better understanding of these obligations due to their visibility in the region, but many smaller firms and those headquartered outside of the jurisdiction have some catching up to do.

CREATING YOUR ACTION PLAN FOR RESILIENCE

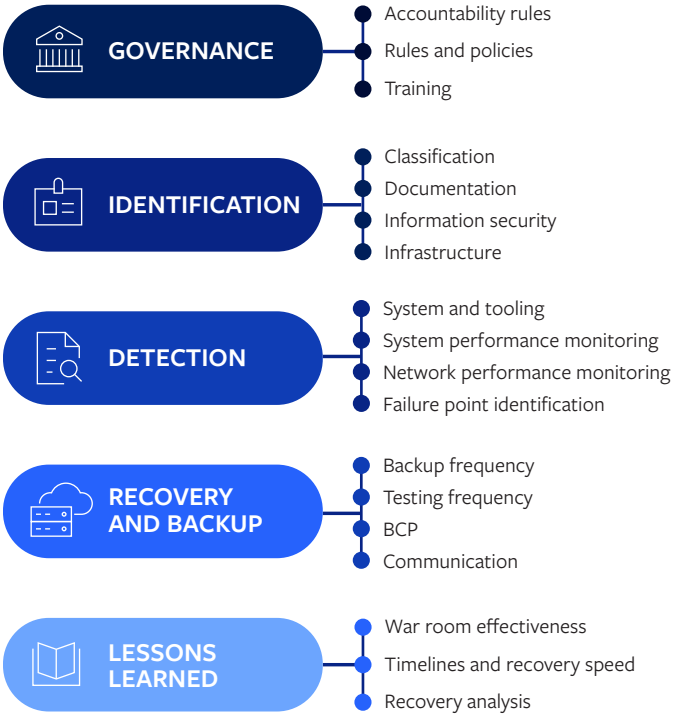
Although impacted financial firms must comply with DORA in January 2025, it will take months of preparation for firms to get ready to meet their compliance obligations, especially when it comes to a full internal and third party system review and service provider data reporting. Buy-side firms and smaller sell-side firms working with large partners in particular may need to build in extra time to assess and potentially query information received from their outsourced service providers. Regulators are prioritising operational resilience over many other areas, which means they are likely to come down hard on noncompliance to prove a point back to the industry about the importance of cybersecurity and operational risk reduction.

Firms will need to keep a close watch on their changing critical system supply chain dependencies over time and report this information regularly to regulators. This necessarily requires the support of these firms' third party providers, which is dependent on the vendors' ability and willingness to comply. AFME has noted in its regulatory response to ESMA[10] that this could prove challenging, especially for non-European providers that consider themselves out of direct scope of the regulation. The evidentiary requirements of DORA are significantly onerous as they require firms to catalogue and classify all of their provider dependencies, regardless of where those providers are located.

Ahead of the January deadline, firms need to conduct a health check on their organisations to assess the criticality of their systems and services and to review how closely aligned their existing ICT risk governance frameworks are with DORA's requirements. The impact assessment should include:

- Identifying important business services that, if disrupted, could cause harm to clients or market integrity, threaten the viability of firms or cause instability in the financial system.
- Setting impact tolerances for each important business service, which would quantify the maximum tolerable level of disruption they would tolerate within the context of each functional area.
- Identifying and mapping the people, processes, technology, facilities and information (including those of suppliers) that support important business services.
- Taking actions to be able to remain within their impact tolerances through a range of severe but plausible disruption scenarios including developing a testing plan and carrying out scenario testing.
- Developing internal and external communications plans for when important business services are disrupted.
- Maintaining an updated self-assessment document detailing how the firm has assessed its compliance with the regulatory requirements.

As highlighted in the graphic below, there are several stages to DORA compliance ranging from the governance and identification of operational risks, through to detection of and recovery from an operational outage. The final stage is applying lessons learned from these events back into improving the effectiveness of a firm's operational risk and resilience programme.



Successful long term compliance with DORA will therefore require multiple components including:

- **Conducting regular reviews:** Focus on assessing existing critical system technology and service dependencies and the resilience of all technology and services environments on a regular basis, regardless of whether they are on premises or on the cloud, or internally or externally provided.

- **Installing multiple layers of data protection, including cyber vaults:** DORA builds on the ongoing regulatory focus on data protection and cybersecurity, and is all about preventing the compromise of those critical data assets in as robust a manner as possible. Cyber vaults are an important asset for firms' business continuity management by providing them with an immutable and system-isolated copy of critical production data. This data is therefore secure if a system is attacked during a cybersecurity incident or impacted by a severe operational outage.

- **Establishing multiple lines of defence for ICT risk management and governance:** While most firms will have third party service provider teams in place, DORA requires them to bolster these teams and provide a wider governance framework across the whole organisation with multiple lines of defence to identify, manage and address ongoing ICT risk.

- **Investing further in attack detection capabilities:** The faster a firm can identify an attack, the quicker it can be addressed. Scanning for vulnerabilities should be table stakes and cyber weaknesses can and do evolve as attack vectors change.

- **Focusing on quick recovery and resolution:** The mirroring of mission critical functions in back-up environments that are the regulatory-prescribed distance away from primary sites is key. While most large banks may have these capabilities well-established, smaller firms and those on the buy-side will more likely need to bolster their capabilities and ensure that providers also meet the more stringent RTOs.

- **Supporting continuous evaluation and monitoring:** Regulators and clients expect firms to conduct regular stress testing exercises with their own inhouse critical systems and with any external critical service providers, at least annually. Business continuity planning also requires adequate oversight and governance on an ongoing basis.

Preparing for DORA and the onslaught of other global operational resilience requirements entails the establishment of a strong governance framework, so that firms are ready to deal with any incident or threat as it arises.

BROADRIDGE'S APPROACH

One of the most important aspects of Broadridge's role in the financial services industry is bringing together the client community to collectively solve regulatory challenges and to mutualise the costs of compliance through a shared services model. The future resilience of the industry is dependent on collaboration and the sharing of best practices, which underlines Broadridge's commitment to its role as a hub for cross-market communication and information sharing.

DEEPLY KNOWLEDGEABLE PROFESSIONAL SERVICES AND TECHNOLOGY SOLUTIONS

Broadridge offers specialised expertise to assess and validate financial organisations' risk and control frameworks, supporting alignment with new and evolving regulatory requirements and mandatory market changes.

Leveraging its extensive in-depth experience in financial services and advanced analytical tools, Broadridge provides thorough evaluations to identify potential vulnerabilities and optimise risk management practices. Its comprehensive approach includes detailed assessments of your current framework, validation of risk controls, and recommendations for enhancing the robustness and efficiency of operational risk management practices.

Broadridge provides SaaS-based solutions that inherently feature resilience and comprehensive reporting capabilities. Through rigorous risk management protocols, data security, and operational processes, and a 24/7 incident management overseen by a dedicated team spread across multiple geographic locations and time zones, Broadridge strives to provide clients with the highest level of protection against adverse market events.

Broadridge has also launched a set of enhanced cyber recovery (Immutability and Repave) solutions to bolster financial organisations' operational resilience as cyber attacks become more sophisticated and prevalent. By deploying secure immutable storage, these solutions create unalterable, point-in-time copies of the entire system infrastructure, including the operating system, third-party software, application software, and critical data. In the event of a cyber incident, these secure, cyber-resilient copies can be swiftly restored to enable faster and easier system recovery. As a result, this advanced solution mitigates the impact of a cyber attack, enhances business continuity against an evolving threat landscape, and helps get ahead of regulator and Board questions on cyber recovery. Broadridge is also engaged with large global firms on collaborative assessments to design firm-specific recovery playbooks that improve preparedness.

FOOTNOTES

[1] Blue Screens Everywhere Are Latest Tech Woe for Microsoft, Wall Street Journal, July 2024
[2] ENISA Foresight Cybersecurity Threats for 2030, ENISA, March 2023
[3] Principles for operational resilience, South African Reserve Bank Prudential Authority, April 2023
[4] Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, SEC, July 2023
[5] Operational Resilience Critical Third Parties to the UK Financial Sector, Bank of England, PRA and FCA, December 2023
[6] Operational resilience: insights and observations for firms, FCA, May 2024
[7] Enhancing Third-Party Risk Management and Oversight, FSB, December 2023
[8] DORA Compliance: Untangling Key Hurdles to Implementation, AFME, May 2024
[9] ECUC´s Positions on DORA, ECUC, June 2024
[10] DORA - Draft RTS (Second Batch), ESMA, March 2024

ABOUT BROADRIDGE'S RESEARCH PARTNER FOR THIS REPORT: FIREBRAND RESEARCH

We're passionate about capital markets research

Our expertise is in providing research and advisory services to firms across the capital markets spectrum. From fintech investments to business case building, we have the skills to help you get the job done.

- The voice of the market
- Independent
- Built on decades of research
- Practical not posturing
- Diversity of approach
- Market research should be accessible

For more information visit www.fintechfirebrand.com or email contact@fintechfirebrand.com

CONTACT BROADRIDGE

Contact us at **Broadridge.com** or email global@broadridge.com for more information.

David Turmaine
Head of International Consulting Services,
Broadridge

Maria Siano
Head of Strategy, EMEA and Asia Pacific,
Broadridge

The content of this paper represents the view of Firebrand and Broadridge. Nothing in this paper constitutes any legal advice.

Broadridge Financial Solutions (NYSE: BR), a global Fintech leader with over $6 billion in revenues, provides the critical infrastructure that powers investing, corporate governance, and communications to enable better financial lives. We deliver technology-driven solutions that drive business transformation for banks, broker-dealers, asset and wealth managers and public companies. Broadridge's infrastructure serves as a global communications hub enabling corporate governance by linking thousands of public companies and mutual funds to tens of millions of individual and institutional investors around the world. Our technology and operations platforms underpin the daily trading of more than $10 trillion of equities, fixed income and other securities globally. A certified Great Place to Work®, Broadridge is part of the S&P 500® Index, employing over 14,000 associates in 21 countries. For more information about us, please visit broadridge.com.

Broadridge.com

© 2024 Broadridge Financial Solutions, Inc., Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

Ready for Next

240830-EN-00695-MK-CP-CO-WP