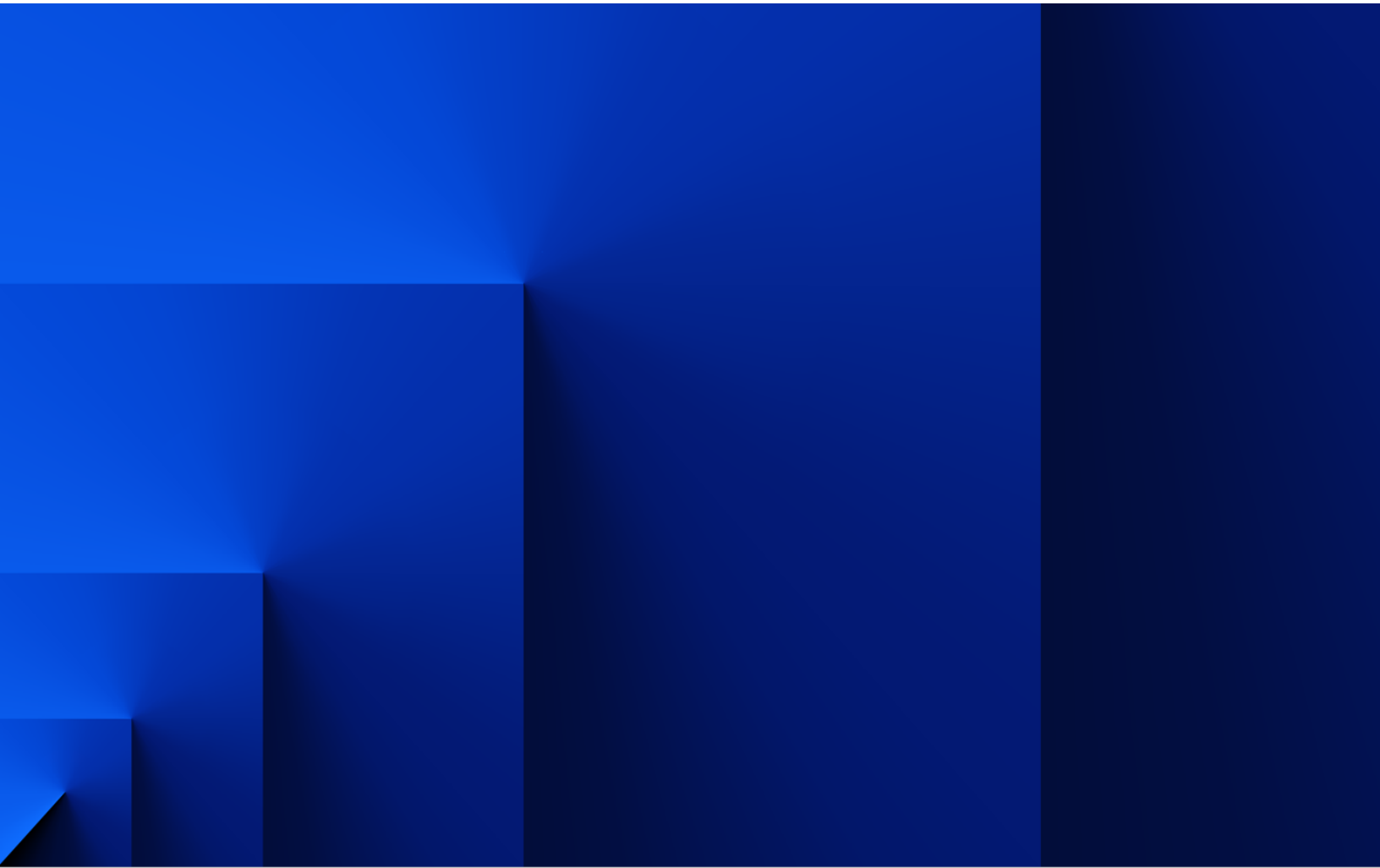
Delivering digital value from investment in digital resilience

Whitepaper

An initiative of the IBM Open Innovation Community



The ‘Why’ of Operational Resilience

The global direction of travel

In recent years, there has been a growing emphasis on operational resilience in the financial services sector with the aim of maintaining financial stability, preserving market integrity, and avoiding customer harm.

The Basel Committee on Banking Supervision (BCBS) recognized in 2021 that more work was needed to strengthen banks' ability to withstand operational risk-related events, such as pandemics, cyber incidents, technology failures, and natural disasters, all of which could lead to significant operational failures or disruptions in the financial markets.

In particular, the COVID-19 pandemic that began in 2020 brought operational resilience into the spotlight; and since 2022, geopolitical developments, stress in energy markets and infrastructure, and high-impact climate change events have continued to highlight the need for operational resilience.

Operational resilience in this context is focused on the ability of firms - and the financial sector as a whole - to absorb and adapt to shocks and disruptions, rather than exacerbate them. The expectation of prudential supervisory authorities - such as the European Central Bank (ECB) - is that firms and financial market infrastructures have robust plans in place to continue delivering important business services, irrespective of the cause of a given disruption.

Scenarios of disruption include man-made threats such as physical and cyber-attacks, IT system outages, and third-party supplier failures (3rd/4th party risk) as well as natural hazards such as fire, flood, severe weather, and pandemic.

Because it incorporates proactive measures for mitigating the risk of a disruptive event in the overall design of operations and processes, operational resilience is more forward-looking and broader in scope than simply being another name for business continuity and disaster recovery capabilities.

Digital Operational Resilience Act

DORA - the European Union’s big bet

The Digital Operational Resilience Act (DORA) is a landmark piece of legislation in the European Union (EU), designed to help fortify the operational resilience of the financial sector, making it fit for purpose in the digital age. DORA seeks to facilitate the operational robustness of financial institutions and service providers, in a context where it is important to foster trust and support economic growth in a rapidly evolving digital landscape.

Digital operational resilience under DORA addresses a financial entity's ability to maintain its operational integrity from a technological perspective by having the appropriate controls in place to manage its Information and Communication Technologies (ICT) capabilities.

This whitepaper highlights key aspects of DORA and sheds light on a possible path forward for financial institutions to seek both compliance and long-term digital business value from their investments in digital operational resilience.

“We live in uncertain times. Banks and other companies that provide financial services in Europe already have plans in place for their IT security, but we need to go one step further. Thanks to the harmonized legal requirements that we adopted today, our financial sector will be better able to continue to function at all times. If a large-scale attack on the European financial sector is launched, we will be prepared for it.

Zbyněk Stanjura, Minister of Finance of Czechia

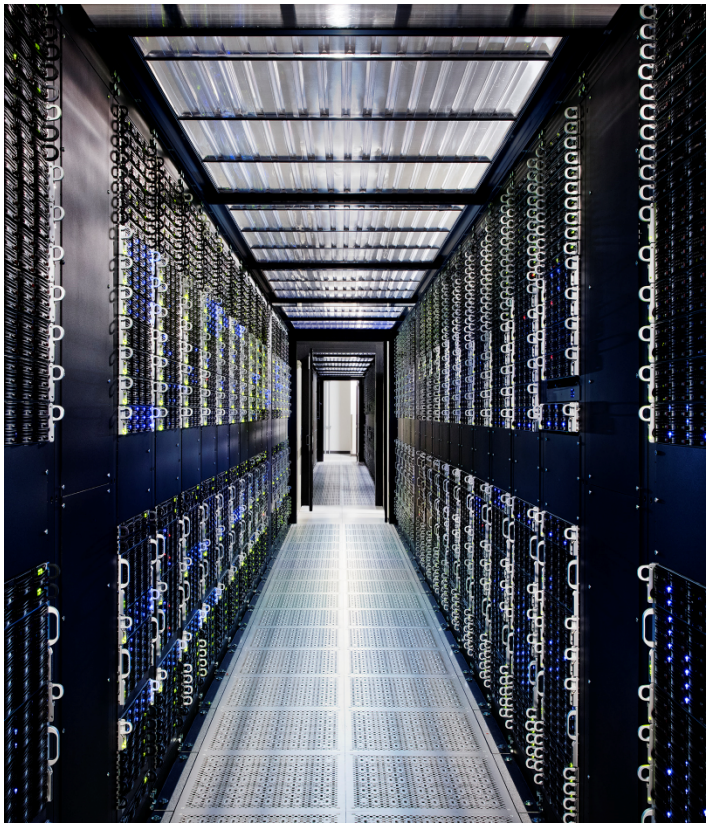
Digital disruption is inevitable...

A core tenet underpinning digital operational resilience is that firms in the financial services sector must seek to prevent and also prepare for inevitable ICT-related disruptions and have measures in place to respond, recover, and limit the impact of the occurrence.

One approach to digital operational resilience is to first prioritize a firm's critical functions and then understand with a high degree of granular precision the process and technological interconnections and interdependencies involved in delivering what is coming to be known as the '**minimum viable bank**'.[1]

The principles of robust digital operational resilience focus on:

1. **Establishing effective ownership** at the level of the Board and senior management
2. **Identifying critical functions** and all related activities necessary for the minimum viable bank to maintain its operations
3. **Setting impact tolerances** for these services
4. **Testing** the firm's ability to stay within those impact tolerances during severe and plausible scenarios, and
5. **Continuously reviewing and learning** from how the firm responds to disruptive events to incorporate lessons learned and iteratively enhance operational resilience over time.



Policymakers and supervisory authorities in the EU are making it abundantly clear that they are expecting financial services leaders to take ownership of their firms' digital operational resilience and prioritize their actions and investments based on the potential impacts of disruption to themselves and the financial stability of the sector at large.

The DORA recitals call out increasing customer trust as a target objective of the regulation, which is why there can be a strong enterprise logic for financial entities to anchor their investments in digital operational resilience to an expectation of delivering business and customer value, in addition to regulatory alignment.

While DORA encapsulates a comprehensive digital resilience framework, the 5-pillar structure (covering ICT risk management, ICT-related incident reporting, digital operational resilience testing, ICT third-party risk, and information sharing) can easily lend itself to a siloed 'per pillar' approach characterized by isolated 'tick-box' initiatives.

Firms opting for a "check the box" approach to DORA compliance may deliver on regulatory expectations. However, from a strategic business perspective, they are arguably leaving untapped value and a chance to revitalize their digital transformation on the table.

In choosing to make digital operational resilience an enterprise-wide business objective, firms increase the odds that their investment in relation to DORA will measurably shift the dial on building transformational digital capabilities that serve the business.

[1] https://apexassembly.com/wp-content/uploads/2021/01/IBM_Cyber_Resiliency_-_Recovering_from_a_Cyber_Attack.pdf

...getting digital value is a choice

While much financial regulation relies on high-level, broadly stated principles, portions of DORA are prescriptive and set out specific rules on ICT risk management, incident reporting, digital operational resilience testing, ICT third-party risk management, and information sharing.

Despite the detailed, rules-based nature of many of the requirements, financial institutions still seem to have leeway to determine how strategic and business-centric they want to make their approach to implementing the regulation.

"Between stimulus and response, there is a space. In that space is our power to choose our response." -*Viktor Frankl*

The suggestion here is that if firms approach DORA with a mindset that positions it as a key enabler of the resilience and dependability that can drive customer satisfaction, digital trust, and loyalty, the budgets dedicated to DORA won't simply disappear into the 'black hole' of compliance spend. Rather, they may serve to fund horizontally aligned priorities that have clear traceability back to valued business outcomes, while also enabling the pace of project execution that most digital initiatives lack.

By investing in the foundational digital capabilities that underpin the sustainability of their future business models (such as next-generation data capabilities to power artificial intelligence (AI), data privacy and cybersecurity, and infrastructure modernization), DORA can help firms in the financial services sector become digitally resilient by bringing siloed digital initiatives into a cohesive transformational motion that is strategically and operationally impactful.

Experience has shown us that digital technologies can only really shift the dial on delivering business outcomes when firms embrace the challenge holistically and invest in the long game.

For leaders in the financial services sector, this means having the self-directed enlightenment, courage, and staying power to address the many organizational, process, data 'hygiene', and enterprise technical debt issues that have accumulated over the years.

There is no quick fix. DORA requires investments of time, effort, and financial resources as well as consistent focus. But there is upside for firms to having a long-term vision of how resilience serves and enables the business, backed by an implementation strategy that embeds short and mid-term stage gates that can help serve to motivate, guide, and hold accountable those who are entrusted with delivering on this mission-critical endeavor.

Transferable lessons from digital transformation projects

According to research by McKinsey[2], a staggering 70% of digital transformation projects fail, typically due to:

- A **lack of clear goals** and conflicting priorities
- **Insufficiently high aspirations** and low engagement
- **Skill gaps** and poor cross-functional collaboration
- **Inadequate investment** to sustain the change

While it is important to understand why 70% of digital transformation projects fail, in the context of DORA it is far more constructive and impactful to unpack why and how the minority 30% succeed. Because success *is* attainable.

Arguably the most relevant and actionable learning is that the top 30% of successful digital transformation projects are more likely than others to make investments in foundational enterprise technology capabilities – the same capabilities that can supercharge the value that DORA programs deliver:

- **Data capabilities:** building out next-generation data platforms, enabling the pervasive use of artificial intelligence (AI) across the enterprise
- **Cybersecurity and data privacy:** proactively running cyberthreat drills, using next-gen defenses and threat intelligence to respond to emerging attacks in real-time
- **Modernizing infrastructure:** focusing on cloud migration and management, as well as infrastructure automation to improve strategic positioning in an uncertain environment

Furthermore, the research shows that these top performers report gains across the board in terms of achieving the type of positive business outcomes every organization strives for:

- Creation of **new revenue streams**
- Improved **employee experience**
- **Increased revenue** from existing streams
- **Reduced costs**

Macroeconomic conditions are challenging, competition is tough, and margins are tight for financial institutions. DORA could easily be framed as 'yet another' costly compliance obligation on an already-fraught business horizon.

The good news is that within DORA is an opportunity to turn compliance expense into a set of strategic investments aimed at delivering higher performance.

IBM is ready with the skills and technology to help you on your DORA journey and assist you in making the strategic benefits of your investment real for your business.

[2] Source: McKinsey Global Survey on Technology Transformations, April 2022

Making your DORA investment work for you beyond compliance

DORA has several objectives, including to comprehensively address ICT risk management in the financial services sector and to harmonize the ICT risk management regulations that already exist in individual EU member states.

Building the requisite level of digital operational resilience under DORA is mandatory for all financial institutions that fall within the scope of the regulation. With that said, there isn't a one-size-fits-all route to addressing DORA. On the surface, this might seem to complicate matters. However, the flip side is that every organization has the option to map out its specific DORA journey, acknowledging its starting point and making business and risk-informed prioritizations along the way to generate maximum value from its investment.

A snapshot of IBM's extensive portfolio is shown below, illustrating the wealth of enabling technologies that firms can leverage as they build their digital operational resilience and explore innovative ways of combining capabilities to unlock new levels of business performance.

Knowing what we know about digital investments that deliver transformational value, we suggest that firms focus on increasing their digital operational resilience by accentuating their mastery of foundational capabilities in 4 key domains:

Data - Operations - Risk Management – Automation & AI

By reimagining how smart combinations of technology can enhance the orchestration of their data, operations, risk, and automation capabilities - and backing them with the right talent and processes to bring digital will and digital skill to their implementation - financial institutions can seek to sustainably address DORA *and* enable their business ambitions by focusing on:

- Embedding security & stability across the ICT estate
- Proactive and prioritized risk mitigation
- Continuous monitoring & rapid response to threats
- Adaptive business continuity and data recovery
- Interoperability and technical optionality
- Reinforced, streamlined governance
- Enhanced operational & strategic decision-making
- Resource allocation prioritized according to business service criticality

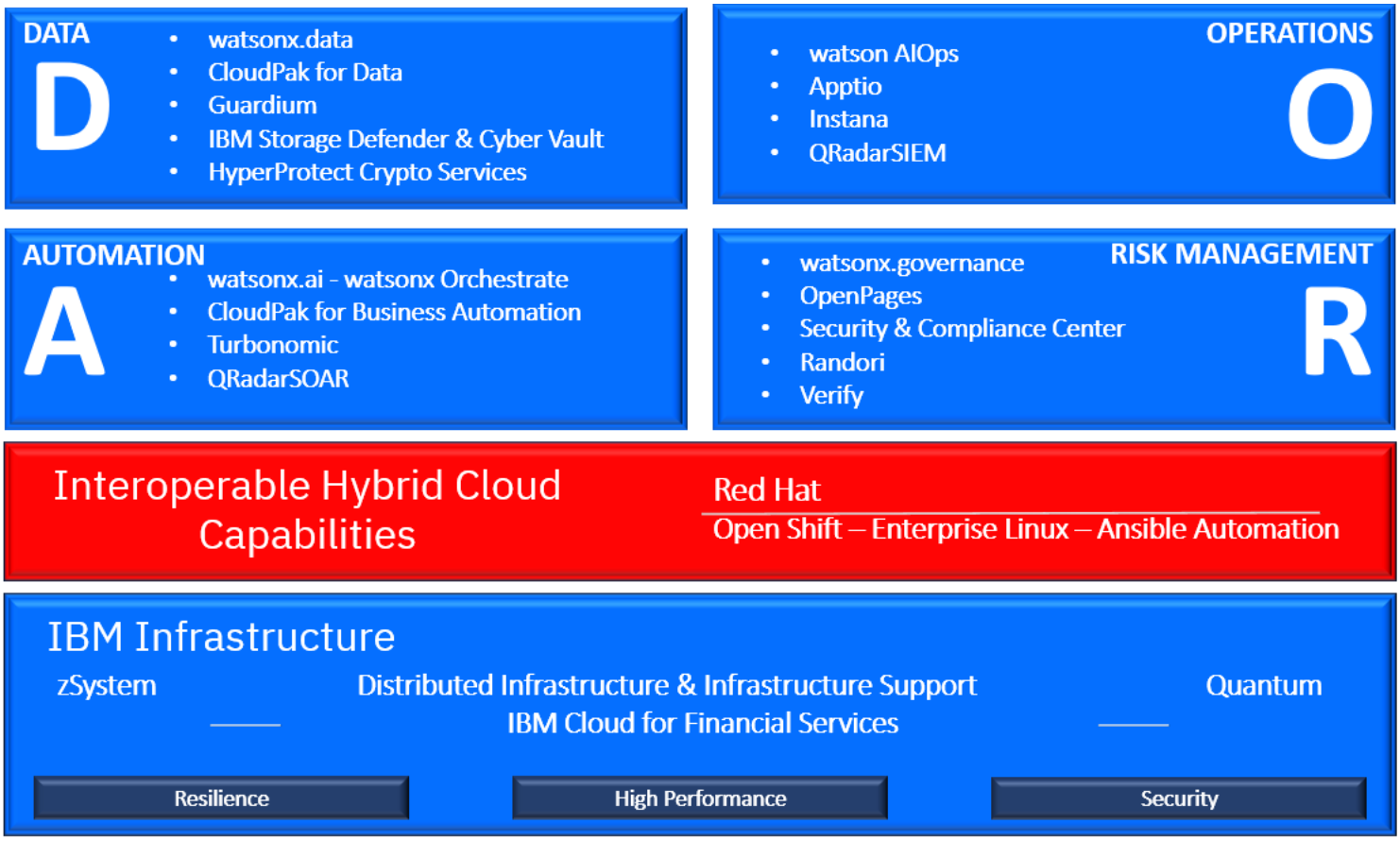


Figure 1 - Building digital resilience capabilities and business value with IBM Technology

Quick-start Guide

Building digital operational resilience in alignment with the requirements and objectives of DORA is far from a 'one-and-done' compliance task. Success requires bold leadership, consistent focus, and disciplined implementation.

Supervisory authorities expect that firms will continually build their capabilities and improve over time to optimize an enterprise-level balance between security, risk, and resilience that will support prudential objectives including financial stability, as well as strategic business outcomes.

While it is important to avoid letting perfection be the enemy of 'good enough', the date for implementation is looming large on the horizon and firms need to both progress at pace *and* be intentional about how they orchestrate their efforts internally so that all the relevant stakeholders and contributors are aligned in the same transformational motion, delivering on objectives that everybody is fully committed to.

TOP TIPS for BUILDING ENTERPRISE MOMENTUM

- **Get started and iterate –** if your organization is behind the curve in terms of preparation and readiness, prioritize and focus on building momentum
- Put in place an **end-to-end governance process** for planning, executing, reporting, and tracking-to-closure with clear identification of roles and responsibilities.
- **Take the time to identify the critical and important functions and Crown Jewel apps** of your organization and establish an enterprise-wide consensus that is agreed upon as an 'unarguable' foundation for moving forward.
- **Identify, document, and map the necessary people, processes, information, technology, facilities, and third-party service providers** required to deliver each of its critical or important functions - this exercise should be undertaken collaboratively across the business to ensure comprehensive service-chain mapping of IT assets and dependencies.
- **Prioritize to focus on the most critical services and technology components first and consider limiting scope and complexity in the early stages** of capability-building around digital operational resilience; build in additional stressors and complicating factors as organizational maturity increases.
- **Set clear objectives** with radical clarity about the outcomes sought and use these to help manage any potential scope creep; this includes an articulated and accepted expectation about the level of ownership and accountability in the business for delivering results.
- **Engage broadly** to get feedback from a diverse group of internal subject-matter experts from different parts of the organization during the development of scenarios to help ensure they are plausible, fit-for-purpose, and feasible to test with available methods and resources.
- **Actively involve senior management** by making them a sparring partner so that they can provide appropriate challenge and endorsement of the overall strategy and chosen tactical approaches.

- Make sure that there is a **standard, repeatable, and applied mechanism** for documenting and communicating risks, dependencies, assumptions, and decisions, particularly for topics where no 'ideal' solution is immediately available.
- **Leverage opportunities to engage with peers**, industry bodies, supervisors, and policymakers to share learning and feedback, sanity-check decisions, and measure internal progress relative to the rest of the sector.

We are here to support your DORA journey and assist you in empowering your business success

Leveraging the combined experience and expertise of IBM Consulting and IBM Technology, we are already working with financial institutions across the EU to deliver strategy formulation and program design in line with DORA objectives, as well as hands-on implementation of process, governance, training, and technical actions in many of the areas covered by DORA specifications (including cybersecurity, testing, business continuity, ICT incident response and recovery plans, etc.).

Customer conversations are revealing that many financial institutions only apprehend the full magnitude of DORA once they mobilize their internal teams and break ground on their DORA program.

The time to act is now. The more time passes, the more constrained the implementation options will become.

By starting early there is more room for firms to aim higher by taking a holistic approach to DORA and making digital operational resilience the foundation of your digital business strategy.

Aiming higher means establishing:

- **Alignment -** based on a holistic and integrated strategy with clear goals and objectives
- **Clarity** - from pervasive leadership direction given by the Board and CEO and relayed by middle-management
- **Focus** – achieved when high-caliber talent is empowered to collaborate cross-functionally
- **Cohesion** - characterized by a shared commitment to agreed goals and an agile governance mindset
- **Momentum** - generated by the disciplined monitoring of progress towards defined target outcomes

Now is the time for leaders in financial institutions to mobilize the full digital will of their enterprise and enable their teams to drive forward in orchestrating and amplifying their digital skills.

Building operational resilience is a team sport. Leveraging a structured methodology, we can tailor our know-how to your ambition, applying renowned advisory and trusted technology expertise to DORA-specific use cases and problem statements.

Contact us today to find out more.

A final word from us to you

As those familiar with DORA know, legislative rulemaking will continue to identify and define DORA requirements. It is imperative that those subject to DORA carefully monitor the rulemaking to help ensure they stay abreast of DORA's evolving obligations.

With its longstanding heritage of supporting financial institutions in delivering their mission-critical business services, IBM is more committed than ever to accompanying financial services clients in the EU as they embrace the digital operational resilience challenge.

We are ready to mobilize the breadth and depth of IBM's extensive technology and service portfolio to empower you with the capabilities to help drive DORA-aligned resilience for the critical, complex, and demanding operations that characterize your business.

IBMers are known for being relentlessly inventive problem-solvers dedicated to every customer's success. Our product, service, and advisory teams are on hand to help you seize the transformational possibilities of DORA. We are here to guide you, learn with you, and co-create with you.

Together, we can weave the many threads of DORA into a value-oriented transformational motion that motivates and aligns your teams and helps position your organization for sustainable resilience and long-term digital business success.

Let's create something that changes everything.

Policy References & Supervisory Frameworks

- BIS Principles for Operational Resilience
- FSI Briefs – Safeguarding operational resilience: the macroprudential perspective
- Bank of England Prudential Regulation Authority Policy Statement | PS6/21 Operational resilience: Impact Tolerances for important business services | March 2021
- Financial Conduct Authority Policy Statement | PS21/3 Building operational resilience: Feedback to CP19/32 and final rules
- DORA Official Text
- Central Bank of Ireland Cross Industry Guidance on Operational Resilience
- APRA Prudential Standard CPS 230 Operational Risk Management
- OCC/FDIC/FRB Sound Practices to Strengthen Operational Resilience
- FFIEC IT Examination Handbook Infobase
- FSB Guidance on Identification of Critical Functions and Critical Shared Services
- Critical Functions Single Resolution Board Approach
- FCA Definition Important Business Service

Further Institutional Resources

- FSB Toolkit for Enhancing Third-Party Risk Management and Oversight (Consultative document)
- ESMA – TRV Risk Analysis: A framework to assess operational resilience
- ESRB – Advancing macroprudential tools for cyber resilience
- TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming
- CMORG Third-Party Lifecycle Management Guidance
- CMORG Sector Response Framework: Core Response Groups
- CBEST Threat Intelligence-Led Assessments

Open Innovation Community Initiative Leaders

Anne Leslie
Cloud Risk & Controls Leader
IBM Technology
anne.leslie@ibm.com

Dr Saritha Arunkumar
WW Cloud Technical Leader – Security
IBM Technology
saritha.arun@uk.ibm.com

Vicky Bunyard-Ford
Director - Account Technical Leaders
IBM Technology
victoria.bunyard@nl.ibm.com

Executive Sponsors

John Duigenan
General Manager - FS Industry
IBM Technology
john.duigenan@us.ibm.com

Barry Brown
Director - IBM Cloud Technical Sales
IBM Technology
barrybro@ie.ibm.com

Expert Contributors

Christophe Appert – IBM Consulting
John Collins – IBM Technology
Rodrigo Hornos – IBM Technology
Dorothee Koppermann – IBM Technology
Juergen Lang - IBM Technology

IBM Cloud
New Orchard Road
Armonk, NY10504

Produced in the United States of America
November 2023