DECISIONFOCUS

White Paper

Strengthening Operational Resilience: A Unified Approach

In a volatile global landscape, organizations are under increased pressure to remain resilient – not just financial service firms and institutions – but every organization, regardless of size or industry. This paper delves into increased regulatory pressure and how organizations can enhance their operational resilience by leveraging an integrated platforms that unify teams and streamline processes.

DECISION FOCUS

Introduction

In an increasingly volatile and rapidly changing global landscape, organizations are under increased pressure to ensure their operations remain resilient. Disruptions caused by pandemics, geopolitical tensions, economic fluctuations, and climate change are no longer rare events but persistent threats that can significantly impact business continuity. As the financial industry becomes more interconnected and digitized, the repercussions of operational failures can be swift and far-reaching, affecting not only individual firms but the stability of the entire financial system. However, it is important to recognize that operational resilience is not just crucial for financial service firms and institutions—it is essential for every organization, regardless of size or industry.

As a result, operational resilience has emerged as a critical priority for organizations worldwide who are now expected to withstand, respond to, and recover from disruptions while maintaining the trust of their customers and meeting stringent regulatory requirements. The concept extends beyond traditional risk management and business continuity planning, encompassing a holistic approach to managing the myriad risks and challenges that we face today.

This white paper delves into the increased regulatory pressure and how organizations can enhance their operational resilience by leveraging an integrated platforms that unify teams and streamline processes. By doing so, they can proactively manage risks, comply with evolving regulations, and meet the rising expectations of their customers. We will explore the regulatory landscape driving these changes, the specific challenges faced by organizations, and the critical role of technology in shaping operational resilience strategies. Finally, we will highlight how a unified approach can help institutions navigate these complexities and achieve a robust resilience framework.

Regulatory Pressures

Operational resilience has become a top priority today for organizations and regulatory authorities worldwide, with new regulations coming into effect in a matter of months. The regulatory guardrails are important to ensure that financial services organizations have the necessary measures in place to withstand, respond to, and recover from operational disruptions.

The Basel Committee on Banking Supervision (BCBS) published the Principles for Operational Resilience (POR) in 2021, which aims to strengthen the ability of banks to "withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets."

The regulations that are coming into force now have been many years in the making. The efforts from regulatory authorities around the world, including the Australian Prudential Regulation Authority, the European Commission, the Financial Conduct Authority, the Hong Kong Monetary Authority, the Monetary Authority of Singapore, and others, began even before the COVID-19 pandemic, which tested the resilience of global organizations.

Globally, regulatory bodies such as the Basel Committee on Banking Supervision have issued principles aimed at enhancing operational resilience. These principles emphasize the need for robust risk management frameworks, effective governance, and comprehensive incident response strategies. In regions like Europe, the proposed Regulation on Digital Operational Resilience (DORA) is nearing finalization, highlighting the critical importance of digital and cyber resilience.

In the UK, new rules on operational resilience came into force on March 31, 2022, with firms expected to complete mapping and testing by 2025. The US has also prioritized operational resilience, with the SEC and banking regulators issuing guidelines and consolidating materials to strengthen resilience practices. Similar initiatives are seen in Canada, Australia, Hong Kong, Singapore, and other jurisdictions, each tailoring their approach to their unique regulatory landscapes.

United Kingdom

In the UK, the Bank of England (BoE), the Financial Conduct Authority (FCA), and the Prudential Regulation Authority (PRA) published the final policies on operational resilience, FCA policy statement (PS21/3) and PRA policy statement (PS6/21) in 2021.

Organizations have until 31 March 2025 to set up the measures and processes required to be compliant with the new rules. The Policy Statements 21/3 and 6/21, Building Operational Resilience and Operational Resilience: Impact tolerances for important business services respectively, require organizations to:

- Identify important business services
- Set impact tolerances for important business services
- Perform mapping and testing to ensure they remain within impact tolerances for each important business service
- Map dependencies and resources to important business services
- Conduct scenario testing
- Implement governance structures
- Undertake self-assessment to test the ability to deliver important business services

PS21/3 applies to banks, building societies, insurers, PRA-designated investment firms, Recognized Investment Exchanges (RIEs), organizations within the enhanced scope of the Senior Managers and Certification Regime (SMCR), and authorized and registered entities under the Electronic Money Regulations 2011 or Payment Services Regulations 2017. PS6/21 applies to UK

banks, building societies, and PRA-designated investment firms; and UK Solvency II firms, the Society of Lloyd's, and its managing agents.

The supervisory authorities are also working on new requirements aimed at ensuring the operational resilience of the UK financial services firms when dealing with critical third parties (CTPs).

European Union

Regulators in the EU have enforced a new regulation aimed at strengthening the "digital operational resilience" of the region's financial sector. The entire EU financial services industry is required to be compliant with the Digital Operational Resilience Act (DORA) by 17 January 2025.

Primarily focused on preventing and mitigating cyber threats, the new regulation lays out the requirements for strengthening the security of network and information systems of financial sector organizations in the region as well as critical third parties that provide Information Communication Technologies (ICT)-related services. DORA requirements are categorized under five key pillars:

- ICT Risk Management Framework
- ICT Incident Management, Classification, and Reporting
- Digital Operational Resilience Testing
- Third-Party Provider Risk Management
- Information Sharing

United States

Operational resilience is also a top area of focus for financial regulatory authorities in the U.S. In 2020, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) published an interagency paper that provided guidance to organizations on 'Sound Practices to Strengthen Operational Resilience'.

"Robust operational risk and business continuity management anchor the sound practices, which are informed by rigorous scenario analyses and consider third-party risks. Secure and resilient information systems underpin the approach to operational resilience, which is supported by thorough surveillance and reporting," the paper reads.

In December 2023, the Commodity Futures Trading Commission (CFTC) approved a rule proposal that requires futures commission merchants, swap dealers, and major swap participants to establish, document, implement, and maintain an Operational Resilience Framework. The commission said that the framework should be "reasonably designed" for the identification, monitoring, management, and assessment of risks relating to information and technology security, third parties, and emergencies or other significant disruptions to normal business operations.

Asia Pacific

Regulatory authorities across countries, including Australia, Hong Kong, and Singapore, are also focused on strengthening the operational resilience of organizations:

- **Australia:** The Australian Prudential Regulation Authority (APRA) released the final cross-industry Prudential Standard CPS 230 Operational Risk Management in 2023. The standard aims to fortify the management of operational risks of all regulated entities and improve their ability to respond to business disruptions and manage the risks from the use of service providers.

- **Hong Kong:** In 2022, the Hong Kong Monetary Authority (HKMA) released the new Supervisory Policy Manual (SPM) module OR-2 on Operational Resilience and a revised version of the SPM module TM-G-2 on "Business Continuity Planning" with the objective of implementing the BCBS's Principles for Operational Resilience (POR) issued in 2021. All authorized institutions were required to develop their operational resilience framework along with the timeline to become operationally resilient by May 2023. By 31 May 2026, these organizations need to be compliant with the new requirements and become operationally resilient.

- **Singapore:** The Monetary Authority of Singapore (MAS) built upon its Guidelines on Business Continuity Management, published in June 2003, to introduce principles and practices to strengthen the operational resilience of organizations. The revised guidelines were published in June 2022. Regulated entities were required to meet the new guidelines and develop a BCM audit plan by June 2023, with the first audit to be conducted by June 2024.

As the risk landscape continues to evolve with growing uncertainties, the regulatory focus on operational resilience will only intensify and expand beyond financial organizations to other sectors. Organizations, however, should not view operational resilience as a mere "tick the box" compliance exercise. When done right, a strong operational resilience program can enable organizations to thrive in challenging business conditions and drive business growth and profitability.

Navigating the Landscape of Operational Resilience: Best Practices for the Modern Enterprise

As we transition from theory to practice, it's imperative to recognize that operational resilience is not a monolithic concept, but rather a multifaceted approach that must be carefully tailored to each organization's unique DNA. The risk profile, operational model, and strategic objectives of a multinational corporation will differ vastly from those of a nimble startup or a mid-sized regional player. Consequently, the resilience strategies employed must be as diverse as the organizations implementing them.

Modern customers demand constant access to services. Any disruption can lead to significant reputational damage and loss of customer trust, making operational resilience a critical business priority. Organizations must ensure their services are always available and secure, which requires a proactive approach to identifying and mitigating potential threats.

The best practices we're about to explore should be viewed not as a prescriptive checklist, but as a flexible framework—a set of guiding principles that can be adapted, scaled, and customized to suit the specific needs and contexts of various organizations. These practices

have been distilled from the experiences of industry leaders, the insights of risk management experts, and the latest research in organizational resilience:

1. **Implement Comprehensive Risk Assessment:** The foundation of operational resilience lies in understanding your risks. Conduct regular, thorough risk assessments that cover not only internal operations but also external factors and third-party dependencies. This process should identify potential threats, vulnerabilities, and their potential impact on critical business functions.

2. **Establish Clear Recovery Objectives:** Define clear Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for each critical business function. These metrics will guide your recovery efforts and help prioritize resources during a disruption. Remember, the goal is to maintain business continuity with minimal impact on stakeholders.

3. **Develop and Test Business Continuity Plans:** Create detailed business continuity plans that outline steps to be taken during various disruption scenarios. However, don't stop at planning - regularly test these plans through simulations and drills. This practice helps identify gaps and ensures that your team is prepared to execute the plans effectively when needed.

4. **Invest in Robust Technology Infrastructure:** Leverage technology to enhance your operational resilience. This could include implementing cloud-based solutions for data backup and recovery, using virtual data rooms for secure document sharing, or adopting AI-powered predictive maintenance systems. The right technology can significantly reduce downtime and accelerate recovery.

5. **Foster a Culture of Resilience:** Operational resilience should be ingrained in your organizational culture. This involves regular training for employees, clear communication of resilience strategies, and encouraging a proactive approach to identifying and addressing potential risks.

6. **Establish Strong Governance and Accountability:** Clearly define roles and responsibilities for operational resilience within your organization. This should include a dedicated team or individual responsible for overseeing resilience efforts, as well as clear escalation procedures during disruptions.

7. **Monitor and Measure Resilience Performance:** Implement Key Performance Indicators (KPIs) to measure the effectiveness of your resilience strategies. These could include metrics like the number of successfully resolved incidents, average recovery time, or the results of resilience maturity assessments. Regularly review these metrics to drive continuous improvement.

8. **Manage Third-Party Risks:** In our interconnected business world, your resilience is only as strong as your weakest link. Conduct thorough due diligence on your vendors and partners and include them in your resilience planning. Consider scenarios where a critical supplier fails and have backup plans in place.

9. **Ensure Effective Crisis Communication:** Develop a clear crisis communication plan that outlines how you'll keep stakeholders informed during a disruption. This includes internal communication with employees as well as external communication with customers, partners, and regulators.

10. **Learn and Adapt from Incidents:** Every disruption, whether major or minor, is an opportunity to learn and improve. Conduct thorough post-incident reviews to identify what worked well and what could be improved. Use these insights to refine your resilience strategies continuously.

Operational resilience is no longer a luxury or an afterthought—it's a fundamental requirement for business sustainability and success in the 21st century. The best practices outlined in this article provide a roadmap for organizations to build and maintain robust resilience capabilities. However, the journey doesn't end with implementation.

True operational resilience is a dynamic, evolving process that requires constant attention and refinement. It demands a shift in organizational mindset from reactive to proactive, from siloed thinking to system-wide awareness. Leaders must champion this shift, embedding resilience into the very DNA of their organizations.

Furthermore, as we look to the future, the concept of operational resilience is likely to expand and evolve. Emerging technologies like artificial intelligence and machine learning offer new possibilities for predictive resilience—anticipating and mitigating potential disruptions before they occur. Blockchain technology could revolutionize supply chain resilience by providing unprecedented transparency and traceability.

At the same time, new challenges are on the horizon. Climate change, geopolitical instabilities, and the rapid pace of technological change all present complex, interconnected risks that will test even the most resilient organizations. Businesses must be prepared to adapt their resilience strategies to address these emerging threats.

Ultimately, operational resilience is not just about surviving crises—it's about thriving in the face of change and uncertainty. Organizations that master operational resilience will be better positioned to seize opportunities, innovate, and drive sustainable growth, even in turbulent times.

Leveraging Technology to Enhance Operational Resilience

The convergence of operational resilience and digital transformation offers a powerful synergy that can elevate an organization's ability to anticipate, withstand, and rapidly recover from disruptions. By harnessing the capabilities of advanced technologies such as artificial intelligence, cloud computing, and the Internet of Things, businesses can create a more dynamic, responsive, and robust operational framework. This article explores the critical role of technology in enhancing operational resilience and why embracing digital solutions is imperative for organizations aiming to thrive in today's volatile business environment.

Here's why embracing digital transformation is crucial for robust operational resilience:

1. **Enhanced Risk Identification and Management:** Advanced analytics and artificial intelligence can help organizations identify potential risks more efficiently and accurately. These technologies can process vast amounts of data to detect patterns and anomalies that humans might miss, allowing for proactive risk management.

2. **Real-time Monitoring and Response:** IoT devices and sensors provide real-time data on various operational aspects. This allows for immediate detection of issues and faster response times, minimizing the impact of potential disruptions.

3. **Automated Incident Response:** Automation tools can initiate predefined response protocols instantly when incidents occur, reducing human error and accelerating recovery processes.

4. **Enhanced Communication and Collaboration:** Digital platforms facilitate seamless communication and collaboration among team members, stakeholders, and customers during crisis situations, ensuring a coordinated response.

5. **Scenario Planning and Simulation:** Advanced simulation tools enable organizations to model various disruption scenarios and test their response strategies, helping to identify gaps and improve preparedness.

6. **Data-driven Decision Making:** By leveraging big data and analytics, organizations can make more informed decisions during crises, based on comprehensive insights rather than gut feeling.

The implementation of technology in operational resilience practices represents a fundamental shift in how organizations safeguard their operations, assets, and stakeholders. As we've explored, the benefits of this integration are multifaceted and far-reaching, from enhanced risk identification to data-driven decision-making during crises.

However, it's important to recognize that technology alone is not a panacea. Successful operational resilience requires a holistic approach that combines technological solutions with robust governance, skilled personnel, and a culture of preparedness. Organizations must view digital transformation not as a one-time project, but as an ongoing journey of continuous improvement and adaptation.

As the pace of technological change accelerates and new threats emerge, the organizations that will thrive are those that remain agile, embracing innovation while maintaining a strong foundation of operational resilience. By leveraging technology effectively, businesses can not only weather the storms of disruption but emerge stronger, more efficient, and better positioned for future success.

Tomorrow's Vision for Operational Resilience

The vision for operational resilience in organizations involves seamless integration and collaboration across all business functions. When teams work in a unified manner, using joined-up workflows on a central platform, they can contribute far more effectively to the institution or organization's resilience. This integrated approach enables proactive identification and mitigation of risks, ensuring continuous service availability and security.

With increasing operational risk from economic, geopolitical, and climate change-driven disruptions, resilience is top of mind for business leaders. Decision Focus helps organizations interprets risk, compliance, and operational insights from throughout the organization into a single pane of glass, providing functional guidance for the continuous management of changing risks.

Features of the Decision Focus platform include:

1. **Impact Tolerance Determination:** The platform enables organizations to accurately assess and define their impact tolerances. This crucial step helps businesses understand the threshold at which disruption to a business service would pose a risk to the firm's viability, consumer protection, market integrity, or financial stability.

2. **Visual Process Mapping:** Decision Focus offers intuitive visual mapping tools for key processes and resources, both internal and outsourced. This feature provides a clear, comprehensive view of the organization's operational structure, helping to identify potential vulnerabilities and critical dependencies.

3. **Risk Assessment and Mitigation:** The software includes advanced tools for assessing and mitigating risks to essential processes and resources. This proactive approach allows organizations to address potential threats before they escalate into major disruptions.

4. **Centralized Data Repository:** All resilience data, planning documentation, and testing results are stored in a single, secure repository. This centralization ensures easy access to critical information and promotes better decision-making during potential crises.

5. **No-Code Flexibility:** The platform's no-code design allows for quick and easy adjustments without the need for specialized IT skills. This flexibility ensures that the system can adapt to changing business needs and regulatory requirements.

Decision Focus' operational resilience management platform overcomes the gaps, delays, and overhead imposed by typical organizational and data silos. Chief Operational Officers, business unit leaders, and resilience managers gain the insights required to protect their customers, employees, products, and services from disruption.

About Decision Focus

Decision Focus delivers enterprise SaaS solutions for managing risk, assessing controls, and optimising all aspects of audit. Decision Focus is an intelligent GRC management tool, offering small and large companies and enterprises a scalable, futureproof approach to GRC – for all industries and sectors. It enables organisations to meet the increasing GRC demands - smarter and with fewer resources. As it should be.

Embedding innovation through agile GRC

See how Decision Focus can support your business. Please get in touch to book a demo.

DECISIONFOCUS

decisionfocus.com