Rethinking operational resilience as a business mandate
Imagine a global bank unable to process its wholesale payments, or a cyber-attack locking down all the ATMs of a retail bank in its top revenue market, or a universal bank having to prioritize which of its retail bank and capital markets businesses to restore first. Breakdowns of critical business services do not just impact revenues, profit, and reputation, they may durably damage relationships and have cascading impacts on broader market participants and communities.

This is why the financial services (FS) industry needs to think about operational resilience¹ in terms of not only preventing disruption, but being prepared to continue and restore business services. To do so, firms need to elevate their traditional business continuity planning and disaster recovery (BCP/DR) to a more strategic, holistic set of capabilities.

¹ UK regulators define operational resilience as “the ability of firms, financial market infrastructure (FMIs) and the sector as a whole to prevent, respond to, recover and learn from operational disruptions.”
There is an increasing sense of urgency around operational resilience

The concept of operational resilience is not new to the FS industry, with long-established guidance and BCP/DR practices. However, increasing complexity, accelerating technological change, uneven maturity of BCP/DR and increasing regulatory attention are driving a need for strengthened operational resilience.

Disruptive events over the last 20 years – such as September 11 and Hurricanes Irene and Sandy – have led FS firms and financial market utilities (FMUs) to develop BCP/DR practices that focus on preventing the disruption of IT systems supporting business services. However, this approach has often resulted in a level of resilience that is insufficient for the challenges of today’s environment.

Increasing complexity of financial services

With globalization, increased competition, and resulting cost and margin pressures leading to more outsourcing, offshoring, and automation, FS firms are now more interconnected and complex than ever before. In addition, key services offered by FS firms rely on multiple providers across the value chain. For example, ecommerce transaction processing typically involves service providers related to payment gateways, payment processing, card networks, settlement and funds transfer at a minimum. Similarly, the trade life cycle relies on multiple providers for financing, brokerage, trade execution, clearing, settlement, pricing and valuation, custody and reporting. With such dependencies and interconnectedness, a breakdown at any one step could disrupt the entire chain.

Accelerating pace of technology change

As the FS industry is testing and adopting disruptive technologies, new risks are emerging. For example, risks of malicious actors locking or encrypting data are forcing institutions to rethink how to recover critical business data. Similarly, the rapidly increasing use of cloud service providers expands the perimeter and creates challenges for security controls designed in simpler times for in-house data centers.

Uneven maturity of operational resilience across the industry

Significant progress has been made in operational resilience since the financial crisis through enhanced risk management, stress testing, capital planning and liquidity management. While these efforts have generally improved financial resilience, traditional BCP/DR activities have in some firms received less attention and focused on maintaining existing capabilities as opposed to continuously improving in maturity and depth. Generally speaking, few firms have a good handle on the mapping of their business services to the people, products, and technology assets that support them. Even fewer have specific plans for reconstructing data in the eventuality of a disastrous event beyond expected recovery point objective targets. Many are unable to failover their entire data center should the need suddenly arise. Some institutions, however, have been making continuous progress in these areas and have set a higher standard for “best practice.”
Regulatory attention and guidance

All of these drivers for FS firms to enhance operational resilience capabilities are not going unnoticed by regulators. A discussion paper published in July 2018 by UK financial regulators put this topic at the forefront for large global financial institutions and provided valuable perspective on regulatory expectations for operational resilience. The paper discusses focusing on key business services rather than just systems and processes, defining impact tolerances for business services and assuming that disruption will occur rather than simply focusing on minimizing the possibility of disruption.

Given the critical role of US FS firms in the global financial system, we expect US regulators to focus both on business continuity fundamentals and the enlarged scope of operational resilience, especially for the largest and most complex firms. We would expect them to ask questions such as: How do you know which business services are critical and based on what criteria? What governance tools and processes do you have in place? How do you make decisions about resource allocation for operational resilience?

In essence, what is your framework for operational resilience?
The bar for operational resilience has risen

A new framework is necessary to develop continuity and restoration capabilities for critical business services and go beyond current BCP/DR practices.

We view the evolving state of operational resilience as an opportunity to not only meet regulatory requirements, which in itself constitutes a call to arms, but to foster a broad-based reexamination of organizations, operations, processes, and the technology environment. Key to setting this new standard is the idea that critical business services must have a path to restoration and continuity even if the timely recovery of supporting systems cannot be achieved.

With critical business services at the center of the renewed focus on operational resilience, new frameworks will require significant involvement from senior management as well as multiple business lines and functions. It will also involve creating or enhancing tools and processes for operational resilience that drive strategic decision making.

### Operational resilience framework

1) **Organization and governance**
   - Elevated stature, scope, and understanding
   - Structure, roles, and responsibilities
   - Policies and procedures

2) **Tools and processes**
   - Critical business services identification
   - Mapping of processes and systems to business services
   - Impact tolerance definition
   - Scenario design and impact assessment

3) **Decisions and strategies**
   - Strategic investment
   - Contingency plans
   - Internal/external communication plans
   - Periodic testing of plans
1) Organization and governance: Drive resilience from the executive level and engage the entire firm

Elevated stature, scope and understanding: As with most significant undertakings in financial services, change is not durable without executive support. Firms have traditionally handled operational resilience through technology-centric BCP/DR programs that have not sufficiently involved business leaders and often failed to prepare for the business consequences of system disruptions. Business leaders and lines of business must no longer be “recipients” of the work performed by the business continuity teams: they need to be the drivers for resilience. To do so, they need to help guide dialogue with the board on topics such as risk appetite and evaluation, remediation activities, and policy changes or trade-offs between major initiatives. They need to also help technology and operations teams understand 1) which business services are critical and why, and 2) their expectations for continuing those services so they can manage impacts on key stakeholders once a disruption occurs.

Structure, roles and responsibilities: Accountability for operational resilience is often scattered across silos with BCP/DR officers buried in organizational layers and tasked with performing the role on a part-time basis in addition to their primary responsibilities. However, a strong operational resilience program requires more robust governance which can be accomplished in a number of ways. For example, organizations can 1) create an executive role such as chief resilience officer to be a peer to business line heads and the chief information officer with direct visibility into resilience-related activities and budgets, 2) align a number of high-profile, executive-level resilience officers to business units, and 3) tie resilience capabilities to the performance of key stakeholders. The functional design matters as well – firms need to design clear cross-functional roles and accountabilities with the product lines and groups such as technology, operations and risk.

Policies and procedures: A well-developed operational risk management program should have business processes along with risk and controls mapping that can be leveraged for operational resilience. In addition, specific policies and procedures should be developed and/or revised to support new practices to systematically design, build and test business services restoration capabilities.

2) Tools and processes: Determine critical services, impact tolerance, and recovery preparation

Critical business services identification: As a foundation of operational resilience, firms must reconfirm the list of critical services for their businesses and operations (e.g., payments, settlements). As a starting point, many firms can leverage the significant work done as part of RRP programs to help identify critical operations and services, mapping interdependencies within the firm as well as critical outsourced services and vendors. Doing so not only prevents the multiplication of conflicting definitions of what is critical to the business, but also avoids significant duplication of efforts and enables operational resilience to gain momentum more quickly.

Mapping of processes and systems to business services: Identifying relationships and dependencies between internal and external business services, operational processes and technology assets has always been difficult. While there is a wealth of information, for example from process documentation and IT asset databases, quality and usability are often limited. However, many firms’ recent investments in customer journey maps, lean process design, and IT hygiene efforts have resulted in valuable artifacts and improved data that can be leveraged for operational resilience efforts. Innovative tools such as graph databases and natural language processing can also accelerate business process mapping.

Impact tolerance definition: For each critical business service, firms must identify their impact tolerance, namely – how much downtime is acceptable should services be completely disrupted and unavailable? While the industry is still developing consensus on what criteria should define impact tolerances, FS firms should pilot the development of their own criteria specific to their clients, counterparties and relative importance to the financial markets.

Scenario design and impact assessment: Developing a diverse set of disruption scenarios, including ones in which systems fail to be recovered, is central to developing critical business service restoration capabilities and refining impact tolerances. Business stakeholders and support teams can work together and model how to bring back services in each scenario and thereby understand which prerequisites are necessary to do so. Assessing the impact of disruptions and establishing overall measures of resilience will help build visibility into both absolute resilience levels and the evolution of resilience. In general, before starting to add new metrics, it is best to take stock of what is currently available (e.g., second/third line reporting, audit, compliance, technology, business continuity, operations) and focus initially on improving where possible.
3) Decisions and strategies: Embed operational resilience tools and preparation into business-as-usual (BAU) decisions and strategies

Strategic investment: Operational resilience tools and recovery preparation inevitably result in a wealth of information about critical business services, key underlying applications and processes, and impacts of disruption. This information can and should be a valuable input for investment decisions in areas such as staffing, third party support and technology. Stakeholders can drive investments to the most critical or risk-prone business services and use impact tolerances to understand where more preparation is needed.

Contingency strategies and plans: Fundamentally, contingency strategies should be driven by the objective of restoring and continuing critical business services within their defined impact tolerance. Firms can consider multiple solutions for doing so, including using backup technologies, following alternative operational procedures, or relying on external service providers. Each of these contingency strategies must have appropriate governance and contractual frameworks to be immediately implemented in the event of a disruption. For example, a bank might develop the contractual framework and operational capabilities to clear positions through an alternate service provider should it forecast its inability to do so using its own platform.

Internal/external communication plans: Beyond restoring critical services, firms must be prepared to communicate through disruptions with internal stakeholders, critical staff, and impacted customers. In addition, elevating the stature and visibility of operational resilience will require communication and awareness programs that extend from the business teams to supporting technology and operations teams.

Periodic testing of plans: Both recovery and restoration scenarios will require testing and a continuous improvement program. In particular, service restoration “muscle memory” will need to be acquired over time, and will necessitate sustained commitment from business teams and ongoing executive sponsorship. As maturity increases, we expect scenarios to be rotated both to confirm operational resilience capabilities and to identify unknown dependencies and single points of failure. It will be essential for firms to not shy away from conducting full failover of their production systems and developing the capability to run for an extended period of time (several weeks) from an alternate location, with the understanding that such a capability should be built up over time. In the past, BCP/DR tests have often been conducted with the assumption they would be successful. In the future, we view a healthy mix of success and failure as a sign of a healthy operational resilience program.

Financial institutions have achieved significant progress in enhancing their risk management capabilities and their overall financial resilience over the decade since the financial crisis, but there is still substantial work to be done to improve operational resilience – particularly given the industry’s increasing complexity and pace of technological change.

Although regulators in the UK and US are increasing focus on operational resilience and may issue guidance or requirements, financial institutions would be wise to proactively drive improvements to their operational resilience programs. Critical system and business service disruptions must be seen as not just a technology issue, but a business risk with potentially long-range consequences.
For a deeper conversation, please contact:

Adam Gilbert  
PwC Principal, Global Regulatory Leader  
adam.gilbert@pwc.com  
(646) 471-5806

Gail Vennitti  
PwC Principal, Custody Banking Leader  
gail.vennitti@pwc.com  
(646) 207-7052

Julien Furioli  
PwC Principal, Resilience Leader  
 julien.furioli@pwc.com  
(646) 247-0608

Corey Booth  
Strategy& Principal, Technology Strategy Leader  
 corey.booth@pwc.com  
(917) 561-7268

Pranjal Shukla  
PwC Principal, Banking Resilience Leader  
pranjal.m.shukla@pwc.com  
(646) 471-2733

Ertem Osmanoglu  
PwC Principal, US Financial Services  
Cybersecurity & Privacy Leader  
ertem.osmanoglu@pwc.com  
(646) 634-8297

Sandrine Mottin  
PwC Director, Digital and Technology Innovation  
sandrine.y.mottin@pwc.com  
(914) 424-7230

Follow us on Twitter @PwCUS

Thank you