A Guide to a Better Understanding of Operational Resilience

By John Thackeray

Operational resilience is a set of techniques that allow people, processes and informational systems to adapt to changing patterns. It is the ability to alter operations in the face of changing business conditions. Operationally resilient enterprises have the organizational competencies to ramp up or slow down operations in a way that provides a competitive edge and enables quick and local process modification.

A resilient enterprise is able to recover its key business services from a significant unplanned disruption, protecting its customers, shareholders and ultimately the integrity of the financial system. Enterprise operational resilience is about more than just protecting the resilience of systems; it also covers governance, strategy, business services, information security, change management, run processes and disaster recovery. Avoiding disruption to a particular system that supports a business service contributes to operational resilience.

Operating Environment and Regulators influence

The operating environment for financial firms has changed significantly in recent years, with many adverse and material events becoming a near certainty. Regulators now want operational resilience to be something that boards and senior managers are directly engaged with and responsible for through governance and assurance models. As a result, regulators are keen on promoting the principles behind having an effective resilience program and its benefits for firms, customers and markets. In July 2018, the UK's financial services regulators (The Bank of England, The Prudential Regulation Authority [PRA] and Financial Conduct Authority [FCA]) brought the concept of operational resilience into the limelight, with the publication of a joint discussion paper, Building the UK Financial Sector's Operational Resilience.

The key requirements noted in the Discussion Paper include:

► Governance: the paper has emphasized the importance of operational resilience in the Boardroom. Accountabilities and responsibilities for senior management will need to be clearly defined, set against an unambiguous chain of command.

► Business Operating Model: must be properly understood, including key business services and the people, systems, processes and third parties that support them, with accountabilities agreed.

► Risk appetite and tolerances: organizations will need to understand and clearly articulate their operational risk appetite and impact tolerance for disruptions to key business services, through the lenses of impact to markets, consumers and business viability.

► Planning and communications: organizations will need to have meaningful plans with emphasis placed on the performance of these plans. Supplemented by proposals for them to be tested not only by the organizations themselves but by partnership with their contributing stakeholders.

► Culture: There must now be a shift in mind-set towards service continuity and a continuous improvement approach, by embedding a 'resilience culture' which reinforces and promotes resilient behaviors.

The Operational Offense

I would suggest five critical actions firms should be taking to support and evolve their approach to operational resilience.

- **Identify your critical services –** Discovery. The enterprise should begin by documenting its business services and mapping them to the underlying technology (cloud infrastructure, data centers, applications, etc.) and business processes (disaster recovery, cyber-incident response plans, etc.).
- **Understand impact tolerance –** Assessment. These underlying technologies and processes are then assessed against Key Performance Indicators (KPIs) or Key Risk Indicators (KRIs). This assessment is used to create a risk score for each business service

which is then reviewed against agreed impact tolerances. Firms need to estimate through the use of scenarios the extent of disruption to a business service that could be tolerated. Scenarios should be severe but plausible and assume that a failure of a system or process has occurred. Firms must then decide their tolerance for disruption – i.e., the point at which disruption becomes no longer tolerable.

- **Know your environment –** Using the assessment, a remediation plan is developed which gives priority to the business services with the largest disparity between risk score and acceptable impact tolerance. Having been communicated to the regulators, and aligned with their expectations, the remediation plan is then funded and executed, and the business service is reassessed for resilience. This should incorporate, third parties, who are the second biggest root cause of operational outages – after change management.

- **Operationalize the program –** The operational resilience program must be able to evolve with the business as it changes. Firms should understand what external or internal factors could change over time and what trends could impact the key business services identified, and adjust their resilience plans accordingly. An important step in the process is testing, which is also prioritized by the risk materiality of key business services. Testing and simulating disruption events can advance the enterprise from informed assessments to demonstrating capabilities to stakeholders and regulators.

- **Robust and coherent reporting –** For boards and senior management, risk metrics and reporting provide an important insight into the effectiveness of the operational resilience program. Develop clear and transparent stakeholder communication plans. Having a robust communication policy and strategy is an essential part of any resilience program, using all forms of media and engaging with all stakeholders.

Conclusion

Operational Resilience is essentially an upgrade that moves Operational Risk management from passive to active. Operational, the poor sibling of

credit and market risk, has stepped into the limelight, and, like Cinderella, now needs an upscaling and upgrading of both resources and vision to make this happen. Given the number of pressing regulatory programs, it will be curious to see how firms weave this requirement into their infrastructure and mindset.

John Thackeray is the founder and CEO of Risk Smart Inc. Over his long career, he has held many risk positions, including CRO posts where he interacted and engaged with US and European regulators. He frequently contributes articles on his risk insights to the Financial Executives Networking Group (FENG).