REPRINT

R&C risk & compliance

OPERATIONAL RESILIENCE

REPRINTED FROM:

RISK & COMPLIANCE MAGAZINE

JUL-SEP 2020 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

KPMG

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

MINI-ROUNDTABLE

OPERATIONAL RESILIENCE

PANEL EXPERTS

Paul Fagone
Principal, Financial Services Regulatory & Compliance Risk
KPMG LLP
T: +1 (214) 213 3560
E: paulfagone@kpmg.com

Paul Fagone leads KPMG's capital markets practice within the regulatory risk and compliance network. He has over 25 years of experience predominantly working at the intersection of electronic trading and risk analytics. His primary focus has been on the design and delivery of operational risk measurement and management strategies and machine learning enhanced surveillance analytics.

Brian Hart
Principal, Financial Services Regulatory & Compliance Risk
KPMG LLP
T: +1 (917) 287 4512
E: bhart@kpmg.com

Brian Hart leads KPMG's financial services regulatory and compliance risk network in the US. In that capacity, he supports clients across the financial services and regulatory sectors to devise and implement large scale programmes that combine driving commercial benefits – lower cost, greater scalability and effectiveness of compliance and risk management programmes – while improving alignment with regulatory expectations and improved risk-taking.

R&C: To what extent has operational resilience become a top priority for financial services regulators in the US? What factors are behind this trend?

Fagone: Prior to recent events associated with coronavirus (COVID-19), the dialogue between global regulators and leading financial services institutions increasingly focused on operational resilience as a core capability. This has been driven by a number of important factors. First, the interconnected nature of global financial services institutions and the utilities that support those firms. Second, the increasing reliance on third-party providers and a need to understand how those risks are assessed, managed and mitigated. Third, the direct harm to consumers caused by a number of high-profile events, such as data breaches and service disruptions, that increasingly highlight the fragility and susceptibility to disruption of the financial service infrastructure. Disruptions caused by COVID-19 will only reinforce and strengthen the resolve of the regulatory community in terms of focusing on operational resilience. We expect that in the postmortem of the impacts of COVID-19, regulators will focus resources on understanding the operational resilience capabilities of the financial institutions that operate within their respective mandates.

R&C: How are bank examinations – and related results – shaping the regulation of operational resilience? Are any new requirements for financial institutions (FIs) likely to emerge from these processes?

Hart: Discussions between some global regulators and leading financial services institutions have touched on the need to incorporate some degree of commonality in terms of the way in which firms define and assess critical services in order to facilitate cross bank comparisons. Some regulators have focused, among other things, on transparency in the rationale behind service level definitions, a clear articulation around the approach for setting impact tolerances, clarity around the manner in which plausible yet severe scenarios are defined and simulated, and linkage between scenario results and how they impact investment decisions around key controls. If history is any guide, leading practices as derived from on the ground discovery through examinations will likely influence their collective thinking. Perspectives are likely to evolve as they are exposed, through the examination process, to competing operational resilience models. With that said, we would expect, over time, that firms will be required to converge on some global standard.

R&C: What options and solutions are available to help FIs enhance their

internal controls, end-to-end testing and management reporting?

Fagone: There is no single vendor platform that encompasses all aspects of operational resilience in financial institutions. One approach is to collaborate with firms to build a strawman that fits into overall strategies and objectives. That said, there are several principles that are important to strengthen the overall integrity of an operational resilience programme. First, utilise data-driven approaches to prioritise service level definitions. Use simple, readily available drivers like trading volume, deal volume and number of accounts to help define services at the appropriate level of detail for your business. Second, leverage simulations and other modeling techniques to assess the impact of service disruptions to augment purely tabletop exercises. This typically yields far more meaningful results that can be replicated with significantly less effort. Finally, design operational resilience reporting intended to enable investment prioritisation and service remediation and enhancement. Incorporating some degree of these principles into your operational resilience framework significantly enhances the utility and value derived from the programme.

R&C: With cyber security now a key area of focus for operational resilience, how important is it for FIs to maintain their IT systems and remediate identified concerns? How can they improve in this area?

> "The dispersion of the workforce displaced by stay at home orders has significantly increased the surface area of the IT footprint and exponentially increased the threat of intrusion and data leakage."
>
> *Brian Hart, KPMG LLP*

Hart: Recent events associated with the COVID-19 environment have highlighted the significant risks associated with cyber threats and the vulnerabilities of IT infrastructure and architecture. The dispersion of the workforce displaced by stay at home orders has significantly increased the surface area of the IT footprint and exponentially increased the threat of intrusion and data leakage, as employees access critical infrastructure through home networks, personal computers and personal cellular phones. With that backdrop, the priority of the cyber threat

has risen on the list of key concerns to address as scenarios like COVID-19 demonstrate. Firms that planned for and are able to execute against a resilience plan that incorporates the mitigation of cyber threats will likely fare better in the long term.

R&C: What steps should FIs take to keep pace with a changing risk environment and regulatory developments?

Fagone: Many firms in the financial services industry are taking a wait and see approach in terms of establishing an operational resilience framework and operating model. This is quite understandable given the high-level guidance provided by and lack of common implementation standards across global regulators. That said, it is to firms' significant advantage to start working through foundational elements of an operational resilience framework by collecting the measures and metrics that can help define and prioritise service offerings, establishing a governance model that considers the end to end delivery of critical services, formalising key definitions like critical services, impact tolerances and thresholds, and thinking through the plausible and severe disruptors that can impact the ability to deliver critical services and designing scenarios that model that disruption. These elements are useful, regardless of when and how the global regulatory community converges on common standards and can be rightsized when those standards emerge.

"It is to firms' significant advantage to start working through foundational elements of an operational resilience framework."

Paul Fagone, KPMG LLP

R&C: To what extent does operational resilience need to be considered when implementing new or revised products or undertaking strategic partnerships?

Hart: Operational resilience should be a key consideration in the upfront due diligence process associated with any new business offering or material change to an existing business model. Understanding potential disruptors from an end to end perspective and the manner in which those potential disruptors will be controlled is a critical input into the return on investment (ROI) discussion.

That said, a comprehensive operational resilience framework that incorporates robust service taxonomies, common control definitions, clarity around impact tolerances and thresholds, as well as structured testing and assessment processes, will facilitate a relatively smooth and straightforward onboarding into a business-as-usual operational resilience operating model.

R&C: What are your expectations for operational resilience in the coming months and years? What more should FIs be doing to address this issue, and satisfy the growing demands of regulators?

Fagone: It is clear that global regulators will continue to focus on operational resilience as a discipline. How that will manifest in terms of the rulemaking process is less certain. That said, firms should, at a minimum, focus on the following. First, assigning accountability for end to end services that align to a functional model for how the business is actually managed. In certain jurisdictions, such as the UK, Hong Kong and Singapore, this is already a requirement. Second, enhancing and extending business continuity and disaster recovery planning capabilities which typically exist within silos to apply more broadly across end to end services. Third, enhancing governance protocols to address operational resilience issues. Finally, rationalising and converging on a common set of operational taxonomies – service level, risk and control inventories – across the business, information technology, risk and compliance and other key stakeholders to manage both the implementation and ongoing maintenance costs of an operational resilience programme. R&C