PUTTING RESILIENCY PRINCIPLES INTO ACTION FOR FINANCIAL INSTITUTIONS

While operational resilience first took center stage after the 2008 financial crisis, it's seen consistent focus in the years since, and after the initial COVID-era forecasts and disruptions, has again come into the limelight. The focus has shifted toward anticipating disruption and learning from it, rather than simply preventing it (a no longer realistic undertaking), and to the necessity of operational resilience in the financial services sector particularly. Finextra Research, the world's leading specialist financial technology (FinTech) news and information source, recently partnered with BMC to explore the five considerations for financial services businesses to consider when building operational resilience.

Per the report, in imagining "a culture fortified with technology and digital tools that enable them to be ready for impending changes," worldwide institutions are devising strategies based in existing regulatory guidance around risk management and governance, as well as output developed by global standard bodies, such as the Basel Committee and the Financial Stability Board. Key to the type of planning necessary for anticipating and weathering disruption are three specific stages:

1. Assessing vital business functions
2. Setting levels of tolerance that those functions can withstand, and
3. Testing the tolerances at regular intervals

In identifying and protecting themselves from threats and potential failures, as well as responding, adapting to, and recovering from disruptive events, financial institutions must undertake five major

steps described briefly here.

Risk identification and technology mapping: This is a challenging yet crucial step for financial institutions—after all, it's not uncommon for a single business service to extend across multiple technologies and third parties. But the process can be assisted with tools to identify operational risk like event data, self-assessments, event management, a control monitoring and assurance framework, and others. Ensuring accurate mapping and securing data that is ensured by strong governance and robust verification and validation procedures is paramount.

Assessing and testing business service tolerance: After establishing tolerance levels, firms should then be prepared to assess and test their systems against dynamic scenarios in regular and repeatable ways. Technology for accurate business forecasting, cloud migration simulations, robust assessment of risks and vulnerabilities, and the reliable breakdown of future updates and releases should be included when attempting to generate consistent and precise inputs for scenario testing.

Understanding response and recovery for system failures: To maintain trust with customers as well as with regulators and other affected entities, plans to manage immediate response and recovery to failures are critical. Having alternative strategies for business continuity in the event of a downed system, such as multi-cloud service management arrangements, can help protect a financial institution's critical applications and data with backup and recovery capabilities. Building on and improving AIOps strategy with big data and machine learning to automate IT operations processes can help predict and find the root cause of complex failures, allowing a faster time to recovery.

Strengthening security and governance: Digital transformation has caused financial services to be more reliant on third parties, and has contributed to their interconnectivity as well. While this has enabled many consumer-friendly services and innovations, it has also opened firms up to additional cybersecurity threats, which are increasingly difficult to identify and remediate. One breach can impact many organizations and thousands of customers. Accordingly, governance requirements continue to become more complex and rigorous. Tools for vulnerability management and compliance with regulatory demands can help ensure protection against threats and adherence to new protocols.

Training in communications and ensuring visibility: Defining and rehearsing communications plans and procedures for recovery from service interruption is crucial to operational resilience, and should include planning for surge capacity, stakeholder service-dependency mapping, and customer redress. Further, clear communication involves holistic, shared information about technology assets and the services the technology supports. Automated tools to improve visibility across the enterprise ensure information is collated and presented in a systematic and consistent manner. To further foster adjacencies and strengthen operational resilience, firms should consider intelligent, automated workflows to reduce the inefficiency and security weaknesses that impede resilience.

To learn more about the five steps to ensure financial services resiliency and the strategies that can help you identify and evaluate the tools for interpreting and applying regulatory guidance in the face of the increasingly digital interconnectedness, read the full impact study here.