KPMG

Regulatory Alert

Regulatory Insights for Financial Services

March 2024

Emerging Regulatory Focus: Operational Resilience

KPMG Insights:

- ***Transverse Risk:*** *Operational resilience transcends all risk pillars, demanding heightened attention to third-party risk management, critical operations, technology services, and cybersecurity.*
- ***Expanding Risk:*** *The probability of operational disruptions and the potential impact of those disruptions is increasing, driven by evolving technologies and interconnectedness with third parties.*
- ***Operational Resilience:*** *Focus on critical operations and core business lines, tolerance for disruptions, rigorous scenario testing, and robust third-party oversight.*

The financial services industry is experiencing significant focus from cross-agency regulators on strong risk management and controls around operational resilience—the ability "to prepare for, adapt to, and withstand or recover from disruptions" (e.g., natural disasters, cyberattacks, technology failures, etc.). Regulators highlight the growing threat landscape, potential failure points, and the link between operational resilience and other areas of non-financial risk management (e.g., third-party risk management (TPRM), critical business capabilities, critical business operations, critical tech services, and cybersecurity).

Federal financial service regulators are assessing how disruptions could affect financial services companies' critical operations and core business lines (e.g., payments, clearing, and settlement) and/or potentially affect systems or data. Learnings are meant to inform potential regulatory requirements and/or expectations, along with learnings informed by global regulators (e.g., UK Prudential Regulatory Authority).

Regulatory considerations include:

Regulatory Area	Key Areas of Focus, Including:
Critical operations and core lines of business	— Critical operations (including related services, functions, and support) whose failure or discontinuance would pose a threat to financial stability in the U.S. — Core business lines (including related operations, services, functions, and support) whose failure would result in a material loss of revenue, profit, or franchise value. — Third parties supporting critical operations and core business lines.
Tolerance for disruption	— Tolerances for disruption set at the enterprise level and for the identified critical operations and core business lines, considering: – Risk appetite for weathering disruption from operational risks given risk profile and capabilities of supporting operational environment (e.g., systems, processes, expertise). – Scenario analysis and recovery maps.

Scenario testing	— Ability to remain within set tolerances through severe but plausible disruption scenarios, including potential risks identified through operational risk management, the internal audit function, business continuity planning, and resolution/recovery planning. — Interconnections and interdependencies within and across critical business operations and core business capabilities and lines of business including third party risks and critical technology services.
Third-party risk management	— Ability to perform critical operations and deliver core businesses within disruption tolerances is not compromised by third-party relationships. — Verification that third parties have sound risk management practices and controls to mitigate disruption consistent with the tolerance level. — Identification of additional/alternative third parties that may be able to assist if the current third party cannot deliver services. — More rigorous oversight of third parties that support higher-risk activities, including critical activities related to critical operations and core lines of business.
Governance and risk management	— Accountability of boards and senior management for operational resilience, including: – Approving the identification of critical operations, core business lines, and disruption tolerances. – Scenario testing and validation. – Periodic, and as needed, review of ongoing surveillance and testing of operational risks and resilience. – Prioritizing investment and cultural changes where needed and driving improvements in operational resilience.
Communications and reporting	— Notification of the appropriate parties in the event of an incident, both internal and external (e.g., internal stakeholders, customers, service providers). — Reporting of the incident and related information to the appropriate regulatory authority, where applicable.
Business continuity management	— Adequacy of contingency and business continuity plans to ensure ongoing operation and limit losses during severe business disruptions. — Identification of the resources (people, processes, technology, facilities, and information) necessary to perform critical operations and deliver core businesses within defined disruption tolerances. — Disaster recovery and business continuity testing with third parties associated with critical operations and core business lines when possible.
Operational risk management	— Integration of risk management systems into organizational structures and decision-making processes, with a focus on reducing the likelihood of operational incidents and limiting losses in the event of business disruption. — Risk identification and assessment approaches that adequately capture business processes and their associated risks, including technology and third-party risks.

Operational resilience has been an ongoing topic of regulatory concern but has become more prominent on regulators' agendas as the threat landscape continues to evolve and expand. Additional examples of regulatory focus on operational resilience include:

Regulatory Issuances		
Federal Financial Institutions Examination Council (FFIEC)	November 2019	Information Technology Examination Handbook was updated with a revised booklet on Business Continuity Management focusing on financial institutions' risk management around the availability critical products and services.
Federal Banking Regulators (FRB, FDIC, OCC)	October 2020	Jointly issued a paper titled "Sound Practices to Strengthen Operational Resilience," which integrated existing guidance, common industry practices, and the work of the BCBS's Operational Resilience Group.
	November 2021	Jointly adopted the Computer-Security Incident Notification Rule to bolster cyber defenses (see KPMG Regulatory Alert, here).
	June 2023	Issued interagency guidance on TPRM. (See KPMG's Regulatory Alert, here.)
	November 2023	FRB Supervision and Regulation Report, identifies operational resilience, including cybersecurity, novel banking, and information technology risks as an element of the 2024 supervisory priorities for governance and controls for large banking organizations. (See KPMG Regulatory Alert, here.)
	November 2023	OCC highlights operational resilience as a supervisory priority in the context of continued evolution and volatility of cyberattacks (OCC 2024 Bank Supervision Operating Plan) and also as an identified risk as it relates to the adoption of new technologies and innovative products in response to increasing demand for digitalization, including on-premises and critical third-party technology architecture (OCC Semiannual Risk Perspective Fall 2023).
Commodity Futures Trading Commission (CFTC)	December 2023	Issued a proposed rule that would require futures commission merchants, swap dealers, and major swap participants to establish operational resilience frameworks designed to "identify, monitor, manage, and assess risks to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations." The framework would include three components (information and technology security program, third-party relationship program, and business continuity and disaster recovery plan) and be supported by requirements around governance, training, testing, and recordkeeping. (See KPMG Regulatory Alert, here.)
Securities & Exchange Commission (SEC)	May 2023	Issued a proposed rule on clearing agency resiliency, recovery, and wind-down plans, which would require clearing agencies to identify and describe several elements in their resiliency and recovery planning (e.g., critical services and continuity, related service providers, adverse scenarios, triggers, risk thresholds, and criteria around implementation of recovery plans); Final rule is expected in the fall of 2024. (See KPMG's Regulatory Alert, here.)
	December 2023	Identified both information security (e.g., data privacy, access, cyber) and operational resiliency as top examination priorities in 2024. (See KPMG Regulatory Alert, here.)

For more information, please contact Amy Matsuo, Prince Harfouche, or Rachel Hynes.

Contact the author:

Amy Matsuo
Principal and National Leader
Regulatory Insights
amatsuo@kpmg.com

kpmg.com/socialme