

Regulatory Alert

Regulatory Insights for Financial Services

February 2024

Heightened Risk Standards: Focus on Risk Frameworks, Processes, and Controls

KPMG Insights:

- **Risk Framework:** Heightened regulatory scrutiny built on established prudential risk frameworks and comparisons to 'peers'.
- **Risk Governance:** Expanded internal controls and non-financial risk management breadth/depth of supervisory and enforcement actions.
- **Issues Management:** Expectation for enterprise-wide review/application of identified risks to risk assessments/RCSAs, expansion of mitigating controls, and robustness of end-to-end processes.
- **Sustainability and Continuous Improvement:** Need to demonstrate continuous improvement and sustainability of processes in such areas as internal controls, data management, change management, issues management.

As part of the current focus on heightened risk governance and risk management practices, the financial services sector is experiencing high regulatory intensity in the area of non-financial risk management, inclusive of a focus specifically on Internal Controls and Operational Risk.

Supervision and Enforcement

In keeping with established prudential regulatory frameworks, financial services regulators expect a

company's risk governance framework to fully incorporate policies and standards, credible challenge and demonstrable evidence of dynamic risk assessment in support of the design, effectiveness, and sustainability of risk controls. Key regulatory areas include (see table on following page):

Regulatory Area	Key Areas of Focus, Including:	KPMG Regulatory Insights
Governance	<ul style="list-style-type: none"> — Reclarification of roles, responsibilities, and accountability for all three lines of defense. — Talent management, covering skills development, recruitment, succession planning, and compensation/performance programs. — Stature afforded risk functions (e.g., autonomy, empowerment, visibility). 	Key Ten Regulatory Challenges of 2024 <ul style="list-style-type: none"> — Risk Standards
Risk Framework	<ul style="list-style-type: none"> — Risk appetite approved by the Board, including company’s risk culture and quantitative risk statements (measured against earnings or capital). Risk appetite clearly connected to the risk assessment programs. — Data governance, quality, and utility of risk limits, set and measured (with clear metrics/limits) at enterprise, concentration, and front-line unit levels. Clear transparency and escalation reporting to management/board of risks and of early warning of elevated risk. — Communication, and periodic review and monitoring, of the risk appetite and the enterprise, concentration, and front-line unit risk limits. 	<ul style="list-style-type: none"> — Risk Sustainability — Data
Internal Controls	<ul style="list-style-type: none"> — Content and quality of the controls inventory (e.g., right/key controls, quality of controls). — Adequacy/coverage/effectiveness of controls testing (including timeliness to remediate identified gaps). — Integration of control testing with risk assessments, and demonstration of actions taken (e.g., enhancements) based on failures and/or risk assessments. 	
Data Management	<ul style="list-style-type: none"> — Deficiencies in data, data outputs, or reporting (e.g., data quality, timeliness, accuracy, traceability, metrics, models). — Data management, including access controls; practices related to collection, retention, disposal; third-party governance/agreements; and reporting capabilities at the lines of business and enterprise levels. — Ability to train, recruit, and retain, skilled talent resources to identify, measure, manage data risk management processes. 	
Issues Management	<ul style="list-style-type: none"> — Completeness and quality of issues inventory. — Governance over the issues management lifecycle (e.g., planning, implementation, closure). — Identification and resolution of issues (distributed across the three lines and across risk tiering) and associated testing, critical challenge, and validation of sizing, mitigation, and resolution. — Demonstration and validation of sustainability. 	
Change Management	<ul style="list-style-type: none"> — Processes for identifying, managing, challenging, approving, and monitoring changes due to new products, activities, processes, and technologies. — Evidence of sustainable processes and effective risk coverage, including metrics. — Periodic review and changes in the risk management framework to reflect industry developments and changes to the company’s risk profile as a result of internal and external factors (e.g., new products, M&A, negative news, systems changes, regulatory changes). 	

Regulatory Issuances

The financial service regulators have stated that outstanding supervisory findings are increasing across entities of all sizes and that operational risk issues – including governance, internal controls, IT and

cybersecurity, and third parties – are among the most cited supervisory issues. The agencies have further identified these operational risk areas as part of their top supervisory priorities for 2024 along with companies’ efforts to remediate previous supervisory findings, including:

Agency	Activity	Description	KPMG Regulatory Insights
FRB	Supervision and Regulation Report	Operational risk identified as a supervisory priority or 2024 for banking entities of all sizes; specific areas include governance and controls, third party management, novel activities, and fintechs.	FRB Reports: Supervision and Regulation; Financial Stability
OCC	2024 Bank Supervision Operating Plan	Risk-based supervision will focus on: <ul style="list-style-type: none"> — Change management, where change to leadership/staffing, operations, risk management frameworks, and business activities are “significant”. — Operations, including products, services, third-party relationships with unique, innovative, or complex structures (e.g., AI, fintechs). — Incident response, data recovery, threat detection/remediation, third-party controls, and maintenance of IT assets inventory related to cybersecurity. 	Fall 2023 Regulatory Agendas: Key Federal Banking Agencies
	Semiannual Risk Perspective	One of four key risk themes, operational risk is deemed to be “elevated”; highlighted risks include: <ul style="list-style-type: none"> — Innovative technologies and new products/services that change the operating environment as well as the relationship with legacy technologies. — Management of third parties and other risks commensurate with size, complexity, and risk profile – more rigor to higher risk and critical activities – talent management for sufficient resourcing and subject matter expertise. — Strong threat and vulnerability monitoring, and effective security controls, given increasing sophistication of cyber attacks and geopolitical tensions. 	
FDIC	2023 Risk Profile	“Operational risk remains one of the most critical risks to banks.”	n/a
SEC	2024 Examination Priorities	Information security (e.g., data privacy, access, cyber) and operational resiliency identified as key emerging risk areas. Attention to safeguarding data and assets; risk management/prevention; and event response. Specific attention to clearing agencies, and changes related to the standard settlement cycle.	Examinations: SEC 2024 Priorities

For more information, please contact [Amy Matsuo](#), [Todd Semanco](#) or [Cameron Burke](#).

Contact the author:



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

kpmg.com/socialme



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

All information provided here is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to

provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the facts of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.