KPMG

Regulatory Alert

Regulatory Insights for Financial Services

February 2024

Heightened Risk Standards: Focus on Data Management (& BCBS 239)

KPMG Insights:

- ***Governance:*** *Sufficient involvement across the Board, senior management, and three lines of defense in the risk data aggregation and risk reporting (RDARR) framework (e.g., roles/responsibilities, review/challenge; policies, standards, procedures; metrics, risks, controls).*
- ***Data universe and tiering:*** *Adequacy of the scope and breadth of data, metrics, models, reports covered by RDARR, including classification and tiering.*
- ***Data lineage:*** *Ability to trace and report on the relationship between data outputs and business processes, authoritative sources, systems of record, and systems of origin.*
- ***Data management and quality:*** *Standardized processes and controls around access, authorization, use, privacy, security, and sharing; accuracy of data and controls to measure and manage risk exposure and reporting.*

Regulators are intensifying their scrutiny of financial services companies' data management and data governance practices over risk management data, from aggregation capabilities to internal risk reporting practices. This focus on RDARR (risk data aggregation and risk reporting) is part of the regulators' increasing supervisory and enforcement activities in areas of both financial and non-financial risk.

Supervision and Enforcement

Financial service companies are expected to both demonstrate and sustain elements of "Heightened Standards"—regardless of size and complexity. Four areas of heightened supervisory focus relating to risk data aggregation and reporting include:

Area of focus	Description
Governance	— Involvement of the Board and senior management in 'business as usual' processes and the adequate and proper definition of requirements around RDARR and how they align to BCBS 239 principles. — Involvement of key internal functions and the adequacy and presence of an independent validation unit within data processes. — Clearly defined and formalized documentation of the governance model (i.e., roles, responsibilities, and accountabilities for the board, management, and across all 3 lines of defense (LOD); policies, standards, and procedures), including mapping, ownership, and ongoing testing and monitoring of controls. — Assessment of data risks associated with RDARR, with associated data risk taxonomy and minimum control requirements.
Data Universe and Tiering	— The scope of the "data universe" including types of data and risk reports covered by the RDARR standard (e.g., models; metrics; regulatory, compliance and risk reporting). — Data classifications, tiering, and risk ratings based on sensitivity, integrity, availability, and criticality.
Data Lineage	— Level of process automation and coverage of the entire data flow (e.g., to consolidate data from different business units / subsidiaries) as well as the accuracy and granularity of the data. — Ability to trace and report on the relationship between data outputs and business processes, systems of record, and systems of origin.
Data Management and Quality	— Data management processes and controls (e.g., standardized data controls around access and authorization, quality and integrity, capture and usage, privacy and security, and sharing with third parties; understanding of data sources;) aligned with the data risk taxonomy and shown to be sustainable through a regular and robust control testing function. — Data quality issue management and reporting (e.g., measurement of data risk exposures for key RDARR metrics and reporting).

Examples of recent data management-related enforcement actions related to risk management data require:

- Establishing a data governance framework, operating model and management oversight, policies, procedures and standards, data literacy and training program.
- Establishing the enterprise-wide adoption of foundational capabilities for data quality, risk aggregation, and reporting.
- Improving data management and reporting practices to facilitate accurate risk and regulatory reporting.
- Addressing previously identified deficiencies related to adequate governance, data quality management for risk metrics, and model risk management.

Regulatory Issuances

Recent regulatory issuances related to data management and governance for risk management data include:

Agency	Activity	Description	KPMG Regulatory Alert
BCBS	Progress Report on Principles for effective risk data aggregation and risk reporting	A progress report assessing 31 G-SIBs and their adoption of BCBS 239. The report indicates that although banks have made some notable improvements, weaknesses and challenges persist in fragmented IT landscapes and deficient risk data aggregation and reporting capabilities. Further, the report urges FS regulators to increase/intensify their supervision and enforcement in order to promote widespread RDARR compliance.	n/a
FDIC	Proposed guidelines on corporate governance and risk management standards	Proposed new corporate governance and risk management guidelines outlining expectations for board and management responsibilities regarding risk management. Specifically, the proposal sets the expectations for "covered institutions" to implement risk management programs that contain policies and procedures designed to ensure that their risk data aggregation and reporting capabilities are appropriate to their business size, complexity, and risk profile and support supervisory reporting requirements.	Expanded Risk Governance and Management: FDIC Proposed Guidelines
OCC	Policies and procedures	New policies and procedures to implement when considering supervisory and enforcement actions against banks subject to Heighted Standards that exhibit or do not correct "persistent weaknesses". The Heightened Standards for risk governance frameworks address RDARR expectations for financial institutions to have "policies supported by appropriate procedures and processes, designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the covered bank, and to support supervisory reporting requirements".	Bank Supervision: OCC "Persistent Weaknesses"

For more information, please contact Rob Westbrook, Brian Radakovich, or Pedro Calado.

Contact the author:

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

kpmg.com/socialme