International Journal of Engineering, Science and Mathematics
Vol. 9 Issue 05, May 2020
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

RISK DATA AGGREGATION AND RISK REPORTING ROLES AND PRINCIPLES

Author Correspondence:
Sowmya Tejha Kandregula | Data Governance Leader
Brambleton, Virginia | sowmyateja@gmail.com

Abstract:
The financial crisis of 2007-08 highlighted the fragile state of risk data and risk reporting capabilities of banks (and) financial organizations globally. In response, the Basel Committee on Banking Supervision (BCBS) issued the regulation BCBS 239 – "Principles for Effective Risk Data Aggregation and Risk Reporting" directing banking (or) financial organizations to strengthen their risk data aggregation capabilities and risk reporting practices.

The BCBS239 regulation focuses on the need for robust Risk Data Aggregation and Risk Reporting (RDARR) governance, architecture, and infrastructure. The requirements address risk data accuracy, integrity, completeness, timeliness, and adaptability. The above-mentioned regulation also focuses on risk reporting accuracy, comprehensiveness, clarity and usefulness, frequency and distribution.

A strong data governance environment translates into reliable and timely data which is critical for any banking (or) financial organization in achieving its strategic objectives. For instance:

- Country Codes: accuracy in the application of Country Codes is essential for a banking (or) financial organization to perform analysis by country and regional groupings to assess exposure, market share, limits, profitability, and the management of concentration risk.

- SIC Codes: accuracy in the application of SIC Codes is essential for risk analysis by industry groupings and the management of concentration risk as well as banking (or) financial organizational sector limits.

Keywords:
Risk Data Aggregation, Risk Reporting, BCBS 239, Data Accuracy, Data Integrity, Data Governance.

Importantroles for the accountability of Risk Data:

1. **Business & Corporate Support Segment Oversight Groups (e.g. Data Offices)** – The function accountable for the presence of controls to measure, monitor and govern the accuracy, completeness, and timeliness of CDEs (Critical Data Elements) data produced by Data Originators, Inputters and Transformers within their Business or Corporate Support Segment. These oversight groups are also responsible to ensure their data control processes are aligned to relevant enterprise-wide policies and standards.
2. **Data Champions –** Those who lead data governance and represent a banking (or) financial organization's Business and Corporate Support Segments relative to the review and feedback of data-related policies and standards and coordination of the resultant impact assessments, as necessary.
3. **Business Term Owners** – Groups/individuals within a banking (or) financial organization; accountable for establishing and maintaining the definitions and valid values for data. Business Term Owners are accountable for the maintenance of CDE data definitions that they own.
4. **Data Originators, Inputters and Transformers** – Those accountable for the validity and accuracy of their data, which usually means the persons that created it. This includes those who select or input data. This role also includes those that manipulate or otherwise transform data (which would effectively result in the creation of new data).
5. **Data Sterwardship Roles** – Those responsible for managing, measuring and monitoring data quality and acting in a data stewardship capacity
6. **Data Custodianship Roles –** Typically teams who are responsible for the applications, databases, tools, and services required to keep data intact and available to users.

- **Risk Chief Data Office (Risk CDO)** – Should act as a second line of defence capacity, the Business & Corporate Support Segment Oversight Group (Data Office) for Group Risk Management (GRM) which includes risk data strategy & governance as well as operations.
- **Risk CDO-Risk Data Strategy & Governance** – The data governance office which includes the role of effective challenge and oversight for data.
- **Risk CDO-Risk Data Operations** – Those who have oversight for monitoring data quality, remediation and reconciliation; and
- **Report Producers** – Those who use data for risk analysis and/or the development and production of CRR`s (Critical Risk Reports) – Group Risk Management (GRM), Corporate Treasury (CT).

Risk Data Aggregation and Risk Reporting Principles:

1. Risk data is a valuable and vital enterprise asset
2. Accountability for risk data lies with those who create and/or transform it
3. The Board and Senior Management must be advised of material gaps or limitations of risk data aggregation and reporting
4. Decisions related to risk data, risk reporting, and supporting infrastructure should be transparent and balance business value and risk management priorities
5. Risk data should be accurate, timely and complete and available to support business decisions in normal and stress or crisis situations
6. Risk reports should be accurate, timely and comprehensive and appropriately reflect the organization's risk profile
7. Risk reports should provide insight and value to an organization, support sound decision making and meet the needs of report consumers

Roles and Responsibilities:

This section outlines the key accountabilities for the governance of data. Effective implementation and management of data and risk reporting controls requires collaborative and ongoing partnerships among all Business and Corporate Support Segments and follows the three lines of defense governance model as depicted below:

1st Line of Defence	2nd Line of Defence	3rd Line of Defence
• Business & Corporate Support Segment Oversight Groups (e.g. Data Offices) • Data Champions • Business Term Owners • Data Originators, Inputters and Transformers • Data Stewardship Roles (Business) • Data Custodianship Roles (Technology)	• Risk CDO – Risk Data Strategy & Governance • Risk CDO – Risk Data Operations • Policy and Standards Owners	• Internal Audit • External Audit

1st Line of Defense:

User Group	Description	Role – examples	Responsibilities
Business & Corporate Support Segment Oversight Groups (e.g. Data Offices)	The function accountable for oversight over data or those who own and manage either Front Office applications in Business Segments or the Risk Ledgers	Business & Corporate Support Segment Oversight Groups (e.g. Data Offices)	• Establish control processes to measure, monitor and govern the integrity of data over which they have oversight responsibility • Ensure their data control processes are aligned to relevant enterprise-wide policies and standards • Ensure that Business & Corporate Support Segment-specific data standards are in place and are aligned to the enterprise-wide policies as appropriate
Data Champions	Those that represent their respective Business and Corporate Support Segments in the Enterprise Data Governance Council (EDGC)	Data Champions from Business and Corporate Support Segments	• Represent their Segment in the Enterprise Data Governance Council to lead the prioritization, monitoring, and governance of the overall investment in data and information management • Establish and maintain an effective data governance organization within their area and ensure clear accountability and stewardship for data and its controls • Act as the focal point of contact and liaison for material concerns and issues related to data aggregation and reporting • Provide input into the prioritization and resolution of data-related issues by ensuring appropriate resourcing and focus, in particular, in times of stress • Support the planning and execution of change management activities in their respective areas and leverage authority and influence to assist with data efforts in achieving their intended outcomes

			• Champion the alignment and adoption of data-related policies, standards, and architecture • Champion the establishment of data mindfulness and strong risk conduct across their Business Segment or Function
Business Term Owners	Those who establish and maintain definitions and valid values for data elements	Policy or Methodology groups within Business Segments	• Establish the definition and valid values for data elements and other business terms which they own • Establish rules, standards or guidelines related to assigning the appropriate value of the term based on an assessment or process • Responsible for resolution of issues and questions related to the definition of a term • Ensure that data definitions are in place and are maintained and comply withestablished standards
Data Originators, Inputters and Transformers	Those who assign, input or transform data (e.g. SIC, BSC, BRR)	• Account Managers (e.g. CAM) • Business Service Centres • Operations Groups • Credit Adjudicators (e.g. CAG) • Corporate Treasury	• Accountable for the quality, accuracy, and completeness of the data that they assign, input or transform • Responsible for the effective execution of controls in order to support data quality goals
Data Stewardship Roles **(Business)**	Those as appointed by the various Business and Corporate Support Segments to fulfill data stewardship responsibilities	Business Unit Application Sponsor	• Responsible for managing, measuring and monitoring data quality • Support data-related initiatives and ensuring alignment to data policies and standards • Support the remediation of data-related issues • Responsible for maintaining data definitions, lineage and business

			rules for data under their responsibility • Accountable for data security and access controls for their data • Responsible for coordinating data provisioning agreements as appropriate
Data Custodianship Roles **(Technology)**	Those as appointed by the various Business and Corporate Support Segments to fulfill data custodianship responsibilities	Data Owners	• Responsible for the applications, databases, tools, and services (including data security) required to maintain data and allow appropriate access by users • Collaborate with Data Stewardship Roles and application owners to implement data transformations, resolve data issues, and agree on system changes • Ensure appropriate accountability for the ongoing adherence to data policies and standards

2nd Line of Defense:

User Group	Description	Responsibilities
Risk Chief Data Office (Risk CDO)	Risk CDO - Risk Data Strategy & Governance Data governance office with Group Risk Management (GRM) which includes Second Line of Defence role for effective challenge and oversight for data and risk reports	**Policy Owner Role** • Ownership of the RDARR Framework and this Policy • Communicate changes to this Policy to all stakeholders for implementation in systems and/or reporting • Manage alignment of this document to other policies and standards as necessary • Provide subject matter expertise and counsel on RDARR risk management and RDARR-related policies and standards to the Business and Corporate Support Segments, as required. **Effective Challenge Role** • Define and maintain Effective Challenge Model & Criteria • Monitor and manage action log for improvements • Communicate findings to Senior Management, Auditors, Regulators and other key stakeholders
	Risk CDO - Risk Data Operations Data operations area with Group Risk Management responsible for monitoring data quality, data remediation, and risk reconciliation	**Oversight and Monitoring Role** • Measure and report on RDARR-related data quality • Monitor data quality on behalf of GRM policy owners • Monitor the terms of service agreements related to data (e.g. operating level agreements, data provisioning agreements[1]) • Perform the reconciliation function and lead the remediation of risk reconciliation issues • Assess, triage and prioritize issues • Lead and facilitate the analysis and remediation of issues related to data they monitor

Conclusion:

RDARR Risk is a form of Information Management Risk, which is a subset of Operational Risk. Within an enterprise Risk Pyramid, RDARR Risk should be linked to the execution-related risk drivers and it should be within Financial Institution`s influence and control.

This should support the Risk Data Aggregation and Risk Reporting Framework of a banking (or) financial organization and help to communicate key roles and responsibilities for the governance of Critical Risk Data Elements (CDEs) that are used in Critical Risk Reports (CRRs).

Effective RDARR processes and controls better enable banking (or) financial organizations to:

- Aggregate risk exposures and identify concentrations quickly and accurately at the enterprise level, across business lines, and between legal entities,
- Accurately measure its performance against its risk tolerance/appetite, and
- Make effective business decisions with confidence.

Conversely, there are a number of potential critical and negative impacts of inaccurate, inconsistent, incomplete or non-timely risk data and risk reports including:

- Increased capital and liquidity costs due to a lack of sufficient data to classify or reconcile exposures,
- Inability to effectively monitor and manage industry sector and geographic limits,
- Inadvertent exposure to restricted clients, sectors, and geographies,
- Ineffective or delayed reporting in stress or crisis situations,
- Inefficient, time-consuming manual workarounds and punitive defaults to remediate incomplete and inaccurate data in downstream reporting processes, or
- Negative regulatory attention and, in certain cases, administrative monetary penalties.