Global Research
& Risk Solutions

CRISIL
An S&P Global Company

RDARR signals

ECB guidelines on optimising risk data aggregation and risk reporting

July 2024

CRISIL GR&RS analytical contacts

Nageswara Ganduri

Director, Quantitative Services
EMEA, APAC Head of Risk Analytics and Regulatory Transformation
nageswara.ganduri@crisil.com

Partha Ray

Associate Director, Quantitative Services
partha.ray@crisil.com

Sanjay Sachdev

Associate Director, Quantitative Services
sanjay.sachdev@crisil.com

Akash Madhani

Lead Analyst, Quantitative Services
akash.madhani@crisil.com

Executive summary

The European Central Bank (ECB) has published its final guide on effective risk data aggregation and risk reporting (RDARR).

The guide, published on May 3, 2024, outlines the prerequisites for banks to effectively manage and aggregate risk-related data and reinforces supervisory expectations based on Basel Committee on Banking Supervision (BCBS) principles, especially BCBS 239. It, however, does not replace the BCBS 239 guidelines.

The regulator emphasises governance and quality of risk data as a supervisory priority.

From the perspective of RDARR, the guide describes the practices, which, in ECB's view, are necessary to identify, manage, monitor, and report the risks banks are exposed to.

The guide focuses on the main deficiencies identified by supervisors, sharing industry best practices and streamlining supervisory activities based on the preconditions deemed essential for enhancing governance and RDARR capabilities of banks.

The seven principles of the ECB

Responsibility of a bank's management body

The management plays a crucial role in overseeing the implementation of strategic objectives, risk strategies, and internal governance norms, including ensuring accountability for risk data quality, allocating resources for risk data aggregation, overseeing remediation programmes, setting clear roles, implementing policies, and ensuring employees possess adequate understanding and skills related to data management, information technology (IT) and financial risks. Further, regular monitoring, training, and ongoing assessment of the knowledge and skills of employees are essential for the effective implementation of risk management practices.

Key requirements

- **Oversight and approval:** The management body, typically the Board of Directors or the senior management team, is ultimately responsible for overseeing and approving the RDARR framework
- **Strategy and implementation:** It approves the overall RDARR strategy, including timelines for implementation and compliance with relevant regulations
- **Resource allocation:** The management ensures adequate resources (financial, human) are allocated for successful RDAAR implementation
- **Alignment with the risk management framework:** It aligns RDAAR with the bank's overall risk management framework to ensure the data gathered supports risk identification, assessment, and mitigation

Key challenges

- **Risk management culture**: Investment banks require a cultural shift to ensure risk management becomes a core priority and is integrated into all business decisions to implement the RDARR framework effectively. This could be challenging in an environment that traditionally prioritises short-term profits
- **Lack of clear ownership and accountability:** Lack of clear delineation of responsibilities across departments for data quality and reporting accuracy could hamper RDARR implementation
- **Insufficient management buy-in:** Management may not fully appreciate the importance of RDARR or its benefits in risk management and regulatory compliance, leading to insufficient resource allocation (both financial and staff) to support RDARR initiatives

CRISIL view

- **Lack of governance:** Clear governance policy frameworks to consistently assess and report risk data aggregation and risk-reporting implementation activities to the Board and senior management are lacking. There is also a lack of clarity on the delineation of responsibility and accountability for data quality, coupled with insufficient authority assigned to staff for the development of a well-defined enterprise data programme
- **Clearly defined roles and responsibilities:** Banks should set policies to delineate the roles and responsibilities of data owners, including ensuring accountability for risk data quality, allocating resources for risk data aggregation, overseeing remediation programmes, setting clear roles and responsibilities, implementing policies, and ensuring employees possess adequate understanding and skills related to data management, IT, and financial risks
- **Monitoring and effective implementation:** Regular monitoring, training, and ongoing assessment of knowledge and skills of employees are critical for the effective implementation of risk management practices

Scope of application

The scope of the application defines the boundaries for the implementation of a data governance framework and specifies the data, reports, models, and legal entities that come under the purview of the framework and the level of control required for each aspect. Management efforts to align the scope with ECB guidelines and subsequently BCBS 239 principles could ensure a comprehensive risk-based approach to data governance for effective risk management.

Key requirements

- **Models in scope:** Scope should include all key internal risk management models. This includes Pillar 1 regulatory capital models (such as internal ratings-based (IRB) approaches for credit risk), Pillar 2 risk and capital models, and other key risk management models (such as IFRS 9 collective provisions models and value-at-risk models). Input data used for model development and the resulting model outputs (e.g., exposure at default, probability of default, or loss-give-default estimates) are part of the guidelines
- **Materiality-based approach:** The ECB's guidelines emphasise a material risk-based approach to data governance. The scope of the application should reflect the approach by focusing on data elements and processes critical to risk management. Data associated with high-risk activities and large exposures to complex calculations should be accorded the highest level of attention and control within this framework
- **Granular definition of data elements:** A well-defined scope explicitly identifies specific data elements that fall under its control, including customer, product, risk exposure, and financial performance data. Granularity in defining data elements enables targeted implementation of data quality controls and facilitates easier identification of data gaps or inconsistencies

Key challenges

- **Integration with legacy systems:** Management efforts to implement data governance controls across various legacy systems may be challenging due to incompatible architecture and data formats. The key lies in finding cost-effective solutions to integrate legacy systems into the scope of application and ensure consistent data quality management practices
- **Alignment with business needs:** The scope of the application should not solely focus on regulatory compliance but align with internal business models. The challenge lies in balancing a risk-based approach with practical data requirements of various business functions within banks
- **Evolving regulatory landscape:** Regulatory reporting requirements could change frequently, making it difficult to dynamically adapt to new data demands. The challenge lies in establishing a process for regularly reviewing and updating the scope to reflect changes in regulatory expectations
- **Wide range of products and instruments:** Banks deal with a vast array of financial products, ranging from derivatives and structured products to complex securities. Collection and aggregation of risk data for all these instruments could be a challenging and demanding task

CRISIL view

- **Data landscape assessment:** Banks should start conducting a comprehensive in-house data landscape assessment to identify all data elements, sources, and uses. This assessment helps prioritise data based on its criticality to risk management and regulatory expectations
- **Leverage regulatory reporting requirements:** Banks should utilise existing regulatory reporting requirements as a starting point for defining the scope. They should ensure the framework encompasses all data elements and processes to fulfil these requirements in an accurate and timely manner

- **Develop a phased implementation approach:** Banks should implement the scope in phases, starting with the most critical data elements and processes to facilitate the implementation process and demonstrate early wins that justify further investments in data governance
- **Maintain dynamic scope:** Banks shall set up a committee that would continuously monitor the appropriateness of previously identified key reports and models

Effectiveness of data governance

Clearly defined roles and responsibilities for ensuring data quality across business, internal control, and IT functions within the internal control framework are essential for effective data governance.

Key requirements

- **Define data requirements:** Banks are advised to establish comprehensive data quality requirements by formalising them in internal policies that cover processes, roles, responsibilities, and decision-making, subject to regular management review and approval
- **Data governance framework:** Essential elements for an effective data governance framework include designated data owners overseeing key risk indicators and critical data elements, and a central data governance function issuing policies and overseeing implementation
- **Independent validation:** A validation function to ensure RDARR processes are functioning as intended, and an internal audit function to handle independent reviews of data governance, RDARR capabilities, and data quality as well as segregation of duties and appropriate organisational arrangements are crucial to ensure the effectiveness and independence of these functions

Key challenges

- **Legacy systems**: Major investment banks often have complex IT infrastructure built over time, leading to data residing in disparate systems (silos). Integration of these silos to create a unified data source for BCBS 239 compliance could be a complex and expensive process
- **Implementation challenges:** Implementation of a data governance framework requires significant investments of resources, including time, money, and personnel. Banks may be tempted to prioritise short-term cost savings over the long-term benefits of improved data quality. This could lead to a minimalistic approach to data governance, ultimately hindering its effectiveness
- **Weak data quality controls**: A data governance framework is only as effective as the data quality controls it promotes. If the existing controls are weak or inadequate, data quality issues will persist. This could involve a lack of data validation processes and insufficient data cleansing procedures. The guidelines lay significant emphasis on the need for granular and accurate data, but ensuring consistency in data definition formats and quality across various systems remains a challenge

CRISIL view

- **Implementation challenges:** Despite recognising the essential nature of data governance frameworks in effective risk management, some banks still struggle to implement them effectively. Many banks view these frameworks as an added expense with limited immediate return on investment (ROI). This short-sighted perspective leads to underinvestment in resources and a minimalistic approach to implementation
- **Leverage technology:** Banks should leverage technology, utilise automation tools to streamline data governance processes, reduce manual intervention, automate data cleansing tasks, identify data anomalies, and monitor key performance indicators (KPIs) related to data quality to minimise associated costs
- **Track progress:** Banks should establish clear metrics to track the effectiveness of this initiative and regularly review progress, identify gaps, and implement corrective actions where necessary

Integrated data architecture

The ECB and BCBS 239 principles emphasise the importance of robust and integrated data architecture to support effective RDARR. This architecture serves as the foundation for data collection, storage, management, and analysis, ensuring data quality, consistency, and accessibility for risk management functions.

It includes data taxonomies covering legal entities, business lines, risks, reports, key risk indicators, critical data elements, and applicable models. Data taxonomies should have uniform definitions, ownership and validation rules, and complete data lineages. Implementation should be well-documented, fit-for-purpose, and focus on providing necessary information for effective risk management and decision-making.

Key requirements

- **Unified data source and storage:** Basel guidelines recommend a unified data source or centralised data repository to store all risk-related data. This central repository eliminates data silos and facilitates easier data access for risk reporting and analysis. A unified data source also simplifies data lineage tracking, enabling banks to trace the origin and transformation of data elements through various systems
- **Integration with business systems:** The data architecture should seamlessly integrate with various business systems across the bank, including front-office, back-office, and risk management systems. This integration ensures timely and accurate data capture from source systems, eliminating the need for manual data entry and reducing the risk of errors. Integration strategies could involve data application programming interfaces (APIs), data warehouses, and data lakes
- **Data definition and taxonomy:** Banks should have uniform data definitions and glossaries with clear data ownership

Key challenges

- **Integration of legacy systems:** Integration of modern data architecture with legacy systems could be challenging due to incompatible data formats and architecture, necessitating significant efforts to adapt legacy systems or migration of data to the new architecture. The cost and complexity of integration could be a significant hurdle in implementing a unified data platform
- **Data governance and ownership:** Implementation of integrated data architecture requires clear data governance and ownership structures, including clearly defined roles and responsibilities for data quality management, data access control, and data security. The challenge lies in ensuring all stakeholders understand and comply with data governance policies and procedures
- **Data taxonomy mismatch:** Sometimes, data definitions and taxonomies are not fully integrated between the first and second lines of defence, leading to inconsistency in critical data lineage

CRISIL view

- **Enhance the data governance framework:** Banks should reassess their data governance framework, policies, and procedures, along with their IT capabilities, and ensure they cover the scope and capabilities set above. Integrated data architecture is a pre-condition for many other principles. Additionally, banks have to consolidate data categorisation approaches and structures as well as integrated data taxonomies
- **Change management and transformation:** Banks should implement a comprehensive change management and transformation initiative to address potential resistance from various business units regarding data standardisation and integration. Effective communication strategies are crucial for gaining buy-in from key stakeholders and ensuring the smooth adoption of the new data architecture

Group-wide data quality management and standards

Group-wide policies and processes are crucial within the overall risk management framework to ensure effective data quality controls and remediation of material issues, while also transparently addressing limitations and risks.

Key requirements

- **Data quality management processes:** These processes should encompass several key aspects, including the implementation of data quality controls covering accuracy, integrity, completeness, and timeliness, the introduction of automation where possible, as well as the definition and measurement of data quality indicators with documented processes for breach resolution
- **Data quality monitoring and reporting:** Banks should include an up-to-date register of data quality issues with severity assessments, root cause analyses, impact analyses, and remediation processes. Additionally, integration of end-user computing applications into data quality management, documentation and control of manual workarounds, and consideration of data quality risks in internal assessment processes are essential components

Key challenges

- **Legacy systems:** Many banks often have complex IT infrastructure built over time, leading to data residing in disparate systems (silos). Integration of these silos to create a unified data source for regulatory compliance could be a complex and expensive process
- **Weak data quality controls:** A data governance framework is only as effective as the data quality controls it promotes. If the existing controls are weak or inadequate, data quality issues will persist. This could involve a lack of data validation processes and insufficient data cleansing procedures. The guidelines emphasise the need for granular and accurate data, but ensuring consistency of data definition formats and quality across various systems remains a challenge

CRISIL view

- **Data governance committee:** Banks should establish a dedicated data governance committee for overseeing data quality management efforts. This committee should comprise representatives from various business units and IT departments. The committee could drive data quality initiatives, monitor performance, and ensure adherence to data quality standards
- **Data quality management tools:** Banks should leverage technology, utilise data governance automation tools to streamline processes, reduce manual intervention, automate data cleansing tasks, identify data anomalies, and monitor KPIs related to data quality to minimise associated costs
- **Track progress:** Banks should establish clear metrics to track the effectiveness of this initiative and regularly review progress, identify gaps, and implement corrective actions where necessary

Timeliness of internal risk reporting

Timely internal risk reporting is essential for effective risk management based on accurate, complete, and timely data presented to the right stakeholders. The ability of banks to produce timely reports primarily depends on the frequency of reporting and the time taken to produce the reports. The ECB expects banks to calibrate their reporting frequency and production timeline, which can help take appropriate actions based on changing internal risk appetite metrics for effective risk management.

Key requirements

- **Defined reporting frequency:** Banks should establish a clear and documented reporting frequency for various risk categories. The frequency should be based on the nature, complexity, and potential impact of the risk being reported. For instance, high-impact or rapidly evolving risks may require more frequent reporting (daily, weekly), while less impactful or stable risks could be reported on a less frequent basis (monthly, quarterly)
- **Reporting timelines:** The time needed to produce a risk report has a similar impact on the effectiveness of risk management: the longer it takes to produce an internal risk report, the longer the period in which the risk situation remains unclear and the higher the likelihood of delayed reactions. For internal risk reports in normal situations, the ECB expects the report to be available in 20 days. The production time is dependent on the materiality and volatility of the key risk indicators to be reported
- **Ad-hoc reporting:** Banks should adopt flexible and ad-hoc reporting capabilities to meet any crisis-like situation, such as Covid-19, which help make informed decisions and ensure process and infrastructure readiness to generate such reports at short notice while meeting regulatory compliance expectations

Key challenges

- **Data availability and accessibility:** Timely reporting hinges on the availability and accessibility of accurate data. Challenges could arise from data silos, inconsistent data collection practices, or delayed data updates from various departments. Overcoming these challenges requires data governance initiatives to promote data quality and establish efficient data collection processes
- **Manual reporting processes:** Reliance on manual data collection and report generation could significantly delay the reporting process. These processes are prone to manual errors and inconsistencies in data capture and reporting formats. Automation of data collection and report generation is essential for timely reporting
- **Lack of interconnectivity between IT systems:** Unaligned IT solutions and legacy systems could hamper the reconciliation of risk data of banks and the timely production of accurate reports

CRISIL view

- **Assess reporting needs:** Banks should identify the information needs of various stakeholders (risk management, senior management, etc.) and tailor reporting content accordingly. They must focus on relevant and actionable information to reduce reporting complexity and promote timely analysis by decision-makers
- **Risk assessment methodologies:** Banks should cultivate a culture that emphasises the importance of timely and accurate risk reporting and encourage open communication on risk identification and reporting of potential issues promptly

Effective implementation programmes

Well-defined programmes that address key requirements and challenges and promote best practices are crucial to effectively implement Basel or ECB guidelines.

Key requirements

- **Executive sponsorship and leadership commitment:** Securing a strong leadership commitment is paramount, while executive sponsorship could foster data quality within the bank. Leaders need to actively champion such programmes by allocating resources and providing ongoing support for their implementation
- **Clear programme roadmap:** The programmes should have adequate project management and governance support, including sufficient measures and metrics to control project execution risks and adequate material, financial and human resources. The implementation plan should clearly define remedial actions, targets, milestones, roles, and responsibilities and suggest intermediate actions to mitigate weaknesses if applicable
- **Progress reporting:** Periodical reporting on the progress of the programmes, including analysis of impediments, delays, and other factors, should be in place. The implementation plans should clearly define remedial actions, targets, milestones, roles, responsibilities, and, if applicable, intermediate actions to mitigate weaknesses that require a longer implementation time to be fully addressed

Key challenges

- **Resource constraints and budget limitations:** They could hamper the implementation of these guidelines. The programmes could be resource-intensive, requiring dedicated personnel, technology investments, and ongoing management efforts. Banks need to secure sufficient budget allocation and identify resources (personnel and technology) to support the programmes

CRISIL view

- **Data governance committee:** Banks should establish a dedicated data governance committee to oversee data quality management efforts. The committee should comprise representatives from various business units and IT departments. It could drive data quality initiatives, monitor performance, and ensure adherence to data quality standards
- **Data management training programmes:** Training should be provided to the relevant personnel across the bank, with the training programme focusing on data governance principles, best practices, and the role of users within the data framework
- **Data quality management tools:** Banks should leverage technology, utilise data governance automation tools to streamline processes, reduce manual intervention, automate data cleansing tasks, identify data anomalies, and monitor KPIs related to data quality to minimise associated costs
- **Monitoring and effective implementation:** Banks should establish clear metrics to track the effectiveness of the initiative. They should regularly review progress, identify gaps, and implement corrective actions where necessary

How CRISIL can help

CRISIL brings a strong combination of risk and data management expertise, best practice guidelines, and solution accelerators.

Gap analysis and compliance assessment

- Identifying and inventorying all regulatory and management reports within the scope of RDARR. Additionally, identifying all risk data aggregation processes that are required to be governed under BCBS 239 principles
- Conducting a gap analysis against RDARR/BCBS 239 requirements and assessing compliance level for the relevant reports and processes identified in the inventory

Data standardisation

- Use its expertise to leverage guidelines of various industry bodies such as the International Capital Market Association, the Bank for International Settlements, the International Swaps and Derivatives Association, and the Loan Market Association for data standardisation; maintaining data catalogues using tools such as Collibra, Informatica
- Prepare logical and physical standardised target data model templates for finance, risk, and front office
- Use its rich experience in product, risk, and finance business processes and regulatory compliance to identify critical data across front-to-back processes

Data traceability

- Delivered multiple strategic meta-data-driven data lineage solutions for large investment banks
- Reverse engineering from reports and code/SQL scripts to understand the flow of data attributes and document the same
- Extensive experience in handling data lineage tools such as Octopai, Manta, Informatica EDC, Collibra

DQM, remediations, and governance

- Framework to automate management of data quality rules and their metadata, defining data quality management (DQM) metrics and implementing scorecard dashboards
- Successfully delivered multiple configurable DQM platforms for risk calculations, scenario analysis, and reporting
- CRISIL's meta-data management best practices enable the team to quickly perform root cause analysis; drive strategic solution delivery to speed up investigations and remediation

Risk aggregation and reporting

- Experience in delivering automated generation of aggregate level risk data for business lines, and legal entities by asset type, industry, and region; validation and reconciliation of reports
- Experience in implementing aggregation methodologies to handle complex non-additive computations as well
- Flexible and ad-hoc reporting capabilities with our RDARR solutions. Our solutions help banks adapt to any crisis-like situation, such as Covid-19. They help make informed decisions and ensure process and infrastructure readiness to generate such reports at short notice while meeting regulatory compliance expectations
- Delivering risk reporting platforms – both proprietary and tableau, QlikView-based
- Performing reconciliation and checks such as risk vs finance, risk vs scenario, exceptional movements

References

[1] https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.supervisory_guides240503_riskreporting.en.pdf

[2] https://www.bis.org/publ/bcbs239.pdf

About Global Research & Risk Solutions

CRISIL GR&RS is a leading provider of high-end research, risk, and analytics services. We are the world's largest provider of equity and fixed-income research support to banks and buy-side firms. We are also the foremost provider of end-to-end risk and analytics services that include quantitative support, front and middle office support, and regulatory and business process change management support to trading, risk management, regulatory, and CFO functions at the world's leading financial institutions. We also provide extensive support to banks in financial crime and compliance analytics. We are leaders in research support, and risk and analytics support, providing it to more than 75 global banks, and 50 buy-side firms covering hedge funds, private equity, and asset management firms. Our research support enables coverage of over 3,300 stocks and 3,400 corporates and financial institutions globally. We support more than 15 bank-holding companies in their regulatory requirements and submissions. We operate from 8 research centers in Argentina, China, Colombia, India, and Poland, and across several time zones and languages.

About CRISIL Limited

CRISIL is a leading, agile, and innovative global analytics company driven by its mission of making markets function better.

It is India's foremost provider of ratings, data, research, analytics, and solutions with a strong track record of growth, a culture of innovation, and a global footprint.

It has delivered independent opinions, actionable insights, and efficient solutions to over 100,000 customers through businesses that operate from India, the United States (US), the United Kingdom (UK), Argentina, Poland, China, Hong Kong, Singapore, Australia, Switzerland, Japan and the United Arab Emirates (UAE).

It is majority-owned by S&P Global Inc., a leading provider of transparent and independent ratings, benchmarks, analytics, and data to the capital and commodity markets worldwide.

CRISIL Privacy Notice

CRISIL respects your privacy. We may use your personal information, such as your name, location, contact number, and email ID to fulfill your request, service your account, and provide you with additional information from CRISIL. For further information on CRISIL's privacy policy please visit www.crisil.com/privacy.