Position Paper

of the Association of German Banks (BdB) on understanding, interpreting and opportunities in implementing the RDARR Guide

Lobbyregister-No. R001458
EU-Transparenzregister-No. 0764199368-97

Berlin, 5 May 2026

bankenverband

Introduction

The implementation of the BCBS 239 principles under the ECB's RDARR Guide has become a central topic in supervisory practice over recent years. In particular, the further specification of requirements regarding the scope of application, data lineage and the handling of end-user computing (EUC) has led institutions to reassess and, depending on their starting point, further develop their existing data management and reporting structures. Recent supervisory reviews and feedback from major European institutions indicate that the RDARR Guide, in parts, sets out a highly ambitious target state, of which the practical implementation is largely shaped by the interpretation of individual terms, the depth of review and the expectations of the supervisory authorities. As a consequence, divergent interpretations and operational approaches are key drivers of implementation effort, complexity and prioritisation conflicts within institutions.

Against this background, private banks consider it essential that the implementation of the RDARR Guide balances its core objectives – namely sound management decisions based on reliable data quality, transparent and traceable data flows, and robust governance – with a consistent, risk-based and economically sustainable approach. This paper is intended as a principle-based interpretation guide for RDARR, with a particular emphasis on proportionality, relevance and operational sustainability as core elements of effective implementation. In this context, a clearly defined and transparently derived scope of application, an insight-driven approach to data lineage, and proportionate, risk-oriented management of EUCs are critical.

For internationally active banking groups, particularly those headquartered outside the EU, additional challenges arise. These include differences in jurisdictional frameworks, group-wide governance models and the operational allocation of responsibilities between group and local entities. In such environments, RDARR implementation must be embedded into existing group structures in a manner that ensures consistency while remaining operationally feasible.

The purpose of this paper is to set out private banks' understanding of key interpretative questions under the RDARR Guide, based on practical implementation experience, and to outline supervisory-compliant approaches for addressing identified challenges. Where illustrative examples are used, they are explicitly intended to support the application of the underlying principles and should not be understood as prescriptive or exhaustive requirements. The paper focuses on principle-based interpretation related to the scope of application, data lineage, and EUC. In doing so, it aims to support structured dialogue with supervisory authorities, facilitate peer exchange among institutions and contribute to greater clarity, proportionality and operational feasibility.

RDARR scope of application

Basic principles of RDARR scoping

The ECB's RDARR Guide deliberately defines the scope of BCBS 239 beyond traditional risk reporting, following an impact and usage-oriented approach. The decisive factor is no longer solely the formal regulatory classification of a report, model or dataset, but its actual relevance for internal management, decision-making, supervisory assessment and external reporting. As a result, the scope should not be understood as a static "checklist", but as the outcome of a structured process that prioritises material risk impact and the practical use of information.From the perspective of private banks, this approach requires a structured, transparent and proportionate determination of scope that takes supervisory objectives into account while avoiding an undifferentiated "everything-in-scope" approach. A one-size-fits-all approach would neither reflect the impact-oriented logic of the RDARR framework nor the principle of proportionality. It would also risk shifting the focus from meaningful insights to excessive implementation effort with limited supervisory or management value. The purpose of an appropriate scoping concept is therefore twofold. Firstly, it is to determine the scope of application of BCBS 239 by identifying the relevant reports, metrics, models and group entities to which the principles apply. Secondly, it is to define how this scope is managed in the course of implementation along the risk data aggregation, in particular with regard to the depth and granularity of requirements such as data lineage.The RDARR Guide explicitly allows for flexibility at both levels, in particular with regard to the depth and granularity of requirements such as data lineage, noting that 'implementation choices should be fit for purpose, well-documented and focused on providing the necessary information for steering the institution and managing its risks' (ECB RDARR Guide, 2024). What is crucial is a consistent and transparent methodology that can be applied on an institution-specific basis, appropriately documented and clearly justified vis-à-vis the supervisory authorities.Proportionality is a key element of this approach. Not all data elements along the data aggregation require the same level of data lineage granularity, automation or control environment. Instead, a phased and risk-based implementation is necessary, reflecting the relative importance of the underlying data for management and supervisory purposes.In determining the approach, existing governance, control, and audit mechanisms must be duly taken into account. RDARR implementation should build on existing structures, rather than establishing parallel or redundant frameworks. This is particularly relevant for annual financial statements and related financial reporting: From the perspective of private banks, such information clearly falls within the RDARR scope of application, given its central importance for external stakeholders. At the same time, in areas such as financial reporting, data is already subject to mature governance and assurance mechanisms driven by other regulatory requirements. From the perspective of private banks, RDARR implementation in these areas should therefore be proportionate and risk-based, building on existing control environments where they are effective, rather than requiring parallel documentation or controls that do not materially enhance data quality or supervisory insight. Where these mechanisms are demonstrably effective and

consistently integrated into the overall data management framework, the introduction of additional RDARR-specific measures is generally not necessary.

Reports in scope

The identification of relevant reports is carried out using a structured, multi-stage process that considers both, the institution's internal management logic and supervisory expectations. The objective is to establish a robust and transparent basis for defining the scope of application of the BCBS 239 principles. The starting point is the identification of key risk types based on the institution's own Risk Appetite Framework (RAF). The RAF provides a common reference linking the business model, risk profile and management logic, and serves as the foundation for further analysis.

The decision whether a report is included in scope or deliberately excluded is based on clearly defined criteria assessed from three analytical perspectives. These perspectives illustrate how the underlying scoping principles may be applied in practice.

The first perspective is internal management relevance. Reports are considered in scope if the data they contain is regularly used at board or key management committee level, contribute to the management of the institution's risk appetite or inform assessments of significant or emerging risks. What matters is their effective use for decision-making purposes. It is therefore irrelevant whether a report is used on a standalone basis or embedded in higher-level reporting, provided it is independently relevant for management decisions.

The second perspective is supervisory relevance. Reports are in scope if they are used by supervisory authorities to assess the financial soundness and stability of an institution, in particular aggregated, non-statistical supervisory reports such as COREP and FINREP. By contrast, reports or report components that serve purely statistical purposes and are highly granular or technical in nature should, in the opinion of private banks, be excluded from the RDARR scope.

The third perspective addresses financial and external reporting. Financial reports that contain risk or performance-relevant information and are publicly disclosed should be included in scope where they are material from a management or risk perspective and have the potential to create reputational or capital market risks. The objective is to ensure that externally published information is consistent, complete and reliable.

Particular importance should be attached to the consistent inclusion of management-relevant KRIs that are used internally and/or disclosed externally. This intersection between internal management and external reporting represents a core application of RDARR and should be clearly reflected within the scope.

Models in scope

Risk models are not considered in isolation within the scope but are consistently assessed along the data lineage. Models whose outputs are used in management-relevant reports or KRIs should therefore be considered within the scope of application, with the depth and granularity of requirements applied in a risk-based and proportionate manner. From the perspective of the banking industry, a separate, standalone scoping assessment for models does not add meaningful value, as the relevance of a model is already determined by the integration of its outputs into key management and reporting processes.

Accordingly, regulatory models (e.g. IRB or FRTB models), key Pillar 2 models such as stress tests, models for economic capital or liquidity stress, as well as central accounting and risk models, for example in the context of IFRS 9 are considered in scope where their outputs are used for management or supervisory purposes. Responsibility for identifying the relevant model outputs lies with the respective model owners, while technical integration is carried out in line with existing governance structures.

Data governance/data ownership

Firms should identify and assign responsibilities to roles such as Data Owners, or equivalent positions, within their data governance framework. A Data Owner is a designated individual or unit accountable for the definition, integrity, and governance of a defined scope of data, ensuring that appropriate standards for accuracy, completeness, and consistency are established and maintained in line with regulatory requirements and internal policies. Data Owners are accountable for the integrity of the data within their remit through collaboration with, and support from, clearly assigned roles responsible for data quality management, controls, and stewardship.

In globally operating banks, it is not necessary for all data owners to be located within the local entity. They can be strategically positioned in other parts of the global organisation, enabling them to fulfil their responsibilities effectively under appropriate governance structures. To ensure proper local oversight, it is crucial to establish suitable mechanisms, such as reporting lines or outsourcing arrangements, to oversee the duties of data owners.

Data lineage

Data lineage is a central element of supervisory expectations within the framework of BCBS 239 principles and the RDARR framework. Its objective is to ensure the flow of data from its source through processing to final reporting is transparent. Supervisory authorities expect institutions to be able to demonstrate the origin, path of processing and use of risk data. The aim is to achieve high data quality, consistency and traceability, enabling well-informed decisions at all levels. Private banks fully support

this objective. At the same time, practical experience shows that data lineage in itself does not mitigate risk; rather, it is the effective use of data lineage – resulting in controlled data and controlled data usage – that constitutes the relevant risk mitigant. Accordingly, the scope and depth of data lineage implementation must be proportionate to the institution's size, complexity and risk profile, and that the data lineage must remain usable and maintainable in day-to-day operations.

A key aspect of interpretation concerns the starting point for documenting data lineage. From the perspective of private banks, data lineage should begin at the point where data enters a controlled, persistent system that forms part of the reporting-relevant data flow. In the case of globally operating banks, it should be recognised that data lineage may include systems distributed globally and not necessarily specific to the entity in question. Extending lineage documentation to earlier preparatory or transient steps should be driven by materiality and risk considerations, where this provides demonstrable supervisory or management value. Extending this to upstream workflow, pre-trade or preparatory process steps would significantly increase the effort required, without regularly providing proportionate additional insights. This is because risk profiles, management information, and regulatory reporting typically relate to completed transactions that affect the balance sheet or the institution's risk position.

In complex data landscapes, a fully attribute-level, entity-specific and comprehensively tool-based implementation entails significant cost, maintenance effort and complexity risks. It also carries the risk that the additional insights sought through data lineage documentation may not materialise due to the sheer volume of information and technical heterogeneity. In practice, expectations regarding fully automated, end-to-end tooling solutions have at times been set too high and cannot yet be considered a market-wide standard.

Against this background, private banks consider the fit-for-purpose principle to be essential. Fit for purpose means that data architecture, taxonomies and data lineage must be designed and documented so that they provide the information necessary for steering the institution and managing its risks within the defined scope of application. Documentation should therefore be purpose-driven and proportionate: data lineage should only be captured where it serves a clearly identifiable supervisory or risk management objective. Lineage that does not contribute to steering, risk monitoring or reporting within scope does not need to be documented.

Data lineage should be documented for reports in scope to the extent necessary to clearly demonstrate data origin, path of processing, and responsibilities, but not necessarily at attribute level – as this does not generate additional insights or may even reduce transparency due to information overload. Decisions on the appropriate level of granularity should be based on clearly defined, risk-based criteria. Institutions may apply different methodologies to determine where enhanced documentation, quality assurance, or governance is warranted, depending on materiality and use. Possible implementation options may include, for example, the identification of Critical Data Elements (CDEs) or relevant datasets to focus attention on decision-relevant data flows. This approach should be understood as illustrative and not as mandatory or prescriptive mechanisms. It is equally important to assess whether relevant

data flows are already sufficiently evidenced through established business or technical documentation and how any additional lineage documentation can be embedded into a sustainable operating model. In addition, materiality considerations should be applied consistently along the entire data flow, for example allowing for a less granular or simplified documentation of data inputs related to non-material portfolios or exposures. Depending on the institution's risk strategy, alternative approaches may include applying controls at dataset or flow level, or focusing enhanced governance on selected, decision-relevant information. The choice of approach should remain institution-specific, taking into account factors such as the data landscape, control framework and risk profile. To ensure supervisory acceptance of a fit-for-purpose approach, transparent documentation of the underlying criteria is essential. Institutions should be able to demonstrate the criteria by which they have determined the level of detail and how the lineage is integrated into data quality processes, controls and responsibilities. A data lineage that merely fulfils formal documentation requirements, but is neither used in data quality processes nor provides real insights for subject matter experts, does not meet this principle. Data lineage must remain readable, operationally compatible and genuinely useful.

From an industry perspective, existing documentation and established processes should be actively leveraged to avoid duplication of effort and to ensure the ongoing accuracy of the data lineage. Business and methodological concepts, technical specifications such as data models and interface descriptions, as well as existing ETL documentation, can be referenced as supporting evidence, provided that the relationship between business concepts and technical implementation remains transparent and traceable. This approach enables a consolidated view of data flows that meets audit requirements while limiting operational burden, as it builds on documentation already maintained as part of day-to-day operations. Detailed documentation from operational processes can be used as a supplement, without this automatically resulting in a formal requirement to evidence all data paths at the highest level of granularity.

Private banks are committed to high standards of data quality, traceability and clear accountability. At the same time, feasibility and economic sustainability must be appropriately balanced against the benefits. The fit-for-purpose approach ensures that transparency, governance and efficiency are aligned, enabling implementation to remain robust over the long term.

Handling of end-user-computing tools

End-user computing (EUC) tools are an integral part of the operational reality of many institutions. They enable business units to implement requirements efficiently and flexibly, close to business processes, and thereby support adaptability and innovation. In particular in the context of evolving regulatory requirements, specialised analyses or low-volume processes, EUCs often represent an appropriate and cost-efficient complement to central IT systems. Where EUCs are used in management-relevant processes or reporting, they must be appropriately documented and integrated along the data lineage, ensuring transparency over data flows and path of processing.

From the perspective of private banks, the use of EUCs is not an exception to standard processes but rather demonstrates an effective collaboration between business units and IT functions. At the same time, it is acknowledged that EUCs, like any other processing solutions, need to be integrated in a well-defined governance and control framework. The objective is not to eliminate or universally replace EUCs, but to ensure their transparent, controlled and risk-appropriate use in line with supervisory expectations of traceability, data quality and governance.

Accordingly, EUCs should not be categorically prohibited, but managed in a differentiated and risk-based manner. A general objective of prohibition would neither reflect operational realities nor the principle of proportionality and could result in significant efficiency losses as well as reduced adaptability of institutions, particularly in areas requiring flexibility, specialist expertise or rapid implementation. Instead, EUCs should be consciously treated as an integral part of the process and data landscape, with controls and automation strengthened where this is justified by risk considerations and economically meaningful.

The core of such an EUC strategy is a governance framework that provides transparency regarding the availability, use and significance of EUCs. This includes a centralised recording of relevant EUC tools, clear roles and responsibilities for their development, use and maintenance, and proportionate documentation requirements. The aim is to establish a risk-oriented overview that systematically integrates EUCs into management, control and audit processes. A criticality-based approach is key in this context, focusing on end-to-end processes rather than individual tools in isolation. Relevant criteria include financial impact, regulatory relevance, importance for internal management and external reporting, data criticality and functional complexity.

Based on this assessment, the appropriate control environment and degree of automation can be determined. A rigid categorisation is not necessarily required; what matters is that the level of control can be increased on a risk-based basis where necessary, while allowing for alternative or compensating controls where full migration to core IT systems is neither feasible nor appropriate.

Manual or semi-manual EUCs are therefore not only acceptable but, in certain cases, appropriate and necessary. This applies in particular to EUCs with a low-risk profile, infrequent use or a high degree of specialist expertise, where full automation would not be economically or functionally justified. In such cases, a manual approach allows for the targeted use of expertise and preserves the necessary flexibility within business units.

Ultimately, the decisive factor is not the degree of automation, but the traceability, controllability and robustness of the process. Manual EUCs can also be made audit-proof through appropriate documentation, defined work instructions, the four-eyes principle and existing internal controls. At the same time, this approach allows for the targeted allocation of limited IT and business resources to those EUCs and processes where automation can genuinely deliver significant risk reduction and efficiency gains.

Overall, the approach to EUCs follows the same fundamental principles as other elements of risk data management: proportionality, appropriateness and sustainability. A differentiated EUC strategy enhances the management capabilities of institutions, preserves the necessary agility within business units, and simultaneously supports supervisory expectations regarding transparency, traceability, and data quality. In the opinion of the private banks, a differentiated and risk-based EUC approach represents an established and forward-looking practice that supports supervisory objectives while remaining operationally feasible.

Conclusion

From the private banks' point of view, a clearly defined and impact-oriented scope of application is central to the effective and sustainable implementation of the RDARR requirements. RDARR objectives can only be achieved where the scope of application, the depth of implementation and the intensity of controls are consistently aligned with the actual use and risk impact of data, metrics and reports. A principle-based approach that prioritises proportionality, relevance and operational sustainability is therefore essential to avoid an undifferentiated "everything-in-scope" outcome.

In this context, a structured scoping methodology, transparent delineation, the consistent integration of relevant models along the data lineage and a proportional risk-based approach to lineage requirements provide a sound basis for meeting supervisory expectations in a manner that is both compliant and economically sustainable. The approaches described in this paper illustrate how these principles may be applied in practice and should not be understood as prescriptive or exhaustive implementation requirements. Crucially, institutions must document transparent, risk-based criteria for determining granularity, automation levels and control intensity, while leveraging existing documentation and control mechanisms embedded in day-to-day operations.

For internationally operating banking groups, these considerations are even more pronounced. Complex group structures, heterogeneous IT and data landscapes and distributed governance models between headquarters and local entities require scope definition, data flow traceability and control concepts to be designed and operated consistently across jurisdictions. In addition, handover points within end-to-end processes — such as the interaction between group-wide data standards and locally managed data provision — require clear principles regarding responsibilities, minimum expectations, and evidencing, rather than uniform technical solutions.

From an implementation perspective, it should be noted that European supervisory authorities currently place a very high priority on RDARR compliance, particularly with regard to demonstrating data lineage and governance arrangements. The expectations and audit focus observed by many institutions in this area go beyond those in comparable international supervisory environments. For globally operating banking groups, especially those headquartered outside the EU, this can lead to significant additional coordination, adaptation and evidencing requirements, with tangible implications for investment decisions and resource allocation. In a global environment characterised by broadly comparable risk profiles, persistently higher implementation burdens in Europe may translate into competitive disadvantages unless they are mitigated through a proportional, value-oriented and consistent approach to implementation.

Against this background, the principle-based approaches set out in this paper contribute not only to operational feasibility and supervisory compliance, but also to the competitiveness of the European financial market. An impact-oriented scope of application, a proportional risk-based approach to data lineage, the targeted use of existing controls and risk-based management of EUCs enable institutions to

meet regulatory objectives - including data quality, traceability and robust governance - effectively, without creating disproportionate complexity or costs. In doing so, these approaches help strengthen a framework that supports financial stability and resilience, while also fostering the conditions for a high-performing, innovative and internationally competitive European banking sector.

Published by:
Bundesverband deutscher Banken e. V.

Burgstraße 28
10178 Berlin
Germany

Lobby Register No R001458
EU Transparency Register No 0764199368-97
USt-IdNo DE201591882

Contact:
bankenverband@bdb.de
bankenverband.de

Responsible for content:
Thematic group [Thematic group]
[First name Last name], [Position]
[First name Last name], [Position]

bankenverband