EUROPEAN CENTRAL BANK
BANKING SUPERVISION

Guide on effective risk data aggregation and risk reporting

May 2024

1 Introduction

The ability of institutions to effectively manage and aggregate risk-related data is an essential precondition for sound decision-making and strong risk governance. This applies to any data used to steer and manage institutions, both strategically and operationally, as well as data used for risk, financial and supervisory reporting.

Various industry studies[1] have identified the economic benefits of more accurate data, including advancements in digitalisation, improved risk management and more effective strategic steering, which contributes to higher revenues and profitability. In the longer term, more accurate data can also help to lower operational and information technology (IT) costs through enhanced automation and the modernisation of IT architectures. In the context of risk management specifically, a major benefit of high data quality is an enhanced ability to avoid material losses due to, for example, an inability to accurately quantify group-wide exposures to specific groups of clients in a stress or crisis situation, a miscalculation of key risk management or regulatory indicators, or the inefficient monitoring of adherence to risk limits. From a prudential perspective, high data quality is critical for effective risk management processes, particularly for managing group-wide risk concentrations, whether credit, market or third-party related. It is also essential for compliance with supervisory regulations and assessments, which rely on timely, complete and accurate information being provided by supervised institutions. Unfortunately, losses caused by poor data quality are rarely captured in a systematic manner, often leaving the potential negative effects unquantified or underestimated as a result. Improving data quality requires a large investment and is a task made more difficult by the complexity of managing the execution risks of large-scale remediation projects.

The crucial nature of risk data aggregation was initially observed during the 2008 financial crisis[2] and, more recently, has been highlighted in the various data collection activities launched by ECB Banking Supervision during the global pandemic and other stress situations. Difficulties in terms of data accuracy, integrity, completeness, timeliness and adaptability are still widely encountered, suggesting that institutions are still focusing on the cost and implementation challenges of improving risk data aggregation and reporting, rather than the benefits of remediating long-standing deficiencies in this area.

[1] See, for example, "Living with BCBS 239", McKinsey & Company, May 2017 and "BCBS 239 Compliance: A catalyst for gaining competitive advantage", Deloitte, 2017.

[2] "Risk Management Lessons from the Global Banking Crisis of 2008", Senior Supervisors Group, October 2009.

Against this background, ECB Banking Supervision is intensifying its supervisory approach. Since its inception, ECB Banking Supervision has regarded governance and quality of risk data as a supervisory priority.[3] In 2016, the ECB launched a thematic review on effective risk data aggregation and risk reporting (RDARR).[4] The thematic review assessed credit institutions' overarching governance, data aggregation capabilities and reporting practices, based on a sample of 25 significant institutions. This assessment was guided by the Basel Committee on Banking Supervision's principles for effective risk data aggregation and risk reporting (Basel Committee on Banking Supervision (BCBS) 239 principles).[5] It was also complemented by extensive benchmarking and two additional analyses: a "data lineage" exercise for credit risk and a "fire drill" exercise for liquidity risk. Overall, the results of the thematic review and the findings from on-site inspections (OSIs) revealed shortcomings in the effectiveness of data governance frameworks (as this applies to RDARR)[6]. It was determined that none of the significant institutions in the sample of the thematic review, including those classified as global systemically important institutions, had fully followed the BCBS 239 principles. As such, serious weaknesses in terms of their RDARR practices were identified[7]. The identified issues were followed up during dedicated OSIs, as part of the Supervisory Review and Evaluation Process (SREP) and on-going supervision. However, the observed progress stalled on some of the key deficiencies, such as the effectiveness of governance arrangements, risk data architectures and supporting IT infrastructures. In 2019, the ECB therefore addressed a letter to all significant institutions[8] under direct supervision within the Single Supervisory Mechanism (SSM), urging them to make substantial and timely improvements and to implement the integrated reporting solutions considered to be best practice.

Despite this increased supervisory scrutiny, the ECB has concluded that the progress made by significant institutions to date has been generally insufficient. Despite its importance, RDARR has not been given an appropriate level of focus, has not been properly steered and many structural deficiencies relating to it have not yet been tackled. As a result, adequate RDARR capabilities are still the exception and full adherence to the BCBS 239 principles has yet to be achieved.[9]

[3] "ECB Banking Supervision: SSM priorities 2016", ECB, January 2016.

[4] See "ECB Banking Supervision: Report on the Thematic Review on effective risk data aggregation and risk reporting", ECB, May 2018.

[5] "Principles for effective risk data aggregation and risk reporting", Basel Committee on Banking Supervision, January 2013.

[6] This Guide always refers to the data governance framework as it applies to RDARR within the scope defined by the institution (see Chapter 3.2). At the institution's discretion, the framework can apply to a broader set of data that is beyond the scope of this Guide.

[7] Large-scale miscalculations of key risk ratios and limits were observed, caused by reconciliation errors, extensive manual adjustments, inconsistent or incomplete underlying data, and weak data quality controls. In many cases, production times of 40 or more working days were observed for monthly risk reports.

[8] See "Supervisory expectations on risk data aggregation capabilities and risk reporting practices: the letter of the Chair of the SSM Supervisory Board to all significant institutions", ECB, June 2019.

[9] RDARR was the worst-rated sub-category of internal governance in the 2023 SREP cycle and the ECB has observed an increasing number of outstanding supervisory measures in this area, most of them triggered by OSIs. Similarly, data quality management remains the least mature IT risk control domain within the annual SREP IT Risk Questionnaire. Deficiencies at several institutions were identified during more targeted OSIs. Likewise, recent crisis situations demonstrated the criticality of robust RDARR to enable the decision-making bodies to react in a timely manner during similar situations.

ECB Banking Supervision has identified deficiencies in RDARR as a key vulnerability in its planning of supervisory priorities[10] and has developed a comprehensive, targeted supervisory strategy for the coming years. This strategy aims to ensure that supervised institutions finally deliver substantial progress in remedying their identified structural shortcomings.

The purpose of this Guide is to describe the practices which, in the ECB's view, are necessary from the perspective of RDARR to ensure effective processes are in place to identify, manage, monitor and report the risks supervised institutions are or might be exposed to. This is also required by the currently applicable law (hereafter referred to as “minimum supervisory expectations”). The information in this Guide is based on evidence collected through the supervisory activities described above and, as such, prioritises discussion of project management and the role of the management body, as these were identified as root causes of the insufficient progress made on RDARR. This Guide focuses on the main deficiencies that have been identified by supervisors and is intended to assist institutions in strengthening their RDARR capabilities, while also sharing practices that have been identified in the industry. Thereby it summarises and re-states also previous communications on RDARR. Furthermore, the level of ambition that ECB Banking Supervision expects from institutions regarding their implementation programmes is re-stated, with a focus on tangible results. This Guide should also enable a more targeted focus of supervisory activities on the preconditions deemed essential for facilitating further progress in institutions’ governance and risk data aggregation capabilities.

The Guide comprises the minimum supervisory expectations compiled by the ECB in conjunction with the national competent authorities. It explains in detail how the ECB applies the relevant national laws, transposing the Capital Requirements Directive (CRD)[11] in line with relevant European Banking Authority (EBA) guidelines (see Annex 1). The ECB intends to follow up on these expectations in its supervisory activities on a case-by-case basis, in line with the principle of proportionality.

Progress in the areas discussed in this Guide is a precondition, but not necessarily sufficient, for achieving sound RDARR. This Guide does not impose new requirements and the issues it addresses are not meant to be exhaustive or to limit any supervisory follow-up activity on RDARR capabilities. The ECB expects institutions to consider this Guide in conjunction with the BCBS 239 principles. In addition to the applicable EU law, national law and the information provided in this Guide, institutions are recommended to take other relevant publications from international fora into account, such as those published by the Basel Committee on Banking Supervision. Furthermore, institutions should also take into account all recommendations and comply with all obligations addressed to them by the ECB in relation to RDARR and resulting from the SREP and other supervisory activities (in the areas, for example of internal governance, risk management and data quality

[10] See “ECB Banking Supervision: SSM supervisory priorities 2023-2025”, ECB, December 2022, and “ECB Banking Supervision: SSM supervisory priorities 2024-2026”, ECB, December 2023.

[11] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

controls). The ECB expects institutions to assess whether their data governance framework complies with the applicable legal framework, aligning with the contents of this Guide and taking any action that may be necessary.

2 References

The CRD defines a set of requirements applicable to RDARR that need to be transposed into national law (see Annex 1). It requires institutions to have robust governance arrangements for identifying, managing, monitoring and reporting the risks they are facing, as well as adequate internal control mechanisms that are consistent with effective risk management. The management body of an institution is responsible for approving and periodically reviewing the strategies and policies for managing and monitoring risk. Members of the management body are required to possess sufficient knowledge, skills and experience, both individually and collectively, to be able to meet their responsibilities and understand the institution's activities, including its main risks. An overview of national transpositions related to RDARR is provided in Annex 2.

The EBA provides further interpretations of legal provisions on the assessment of institutions' information and communication technology (ICT) for risk data aggregation capabilities, as well as specifications on the integrity of data, ICT projects and change management.[12] Furthermore, EBA Guidelines on internal governance specify that regular and transparent reporting mechanisms should be established at banks to provide the management bodies with timely, accurate, concise and meaningful risk reports.

The joint European Securities and Markets Authority (ESMA) and EBA Guidelines on the assessment of the suitability of members of the management body (EBA/GL/2021/06) require the individual members of the management body of an institution to have an up-to-date understanding of the institution's business, activities and its risks. The same is required for the management body as a collective. The ECB Guide to fit and proper assessments[13] specifies the ECB's main expectations and policies on conducting suitability assessments of the members of an institution's management body. Furthermore, the ECB Guide on climate-related and environmental risks[14] includes the expectation, among others, that the management body will consider climate-related and environmental risks when developing the institution's overall business strategy.

For institutions using internal models to determine regulatory capital requirements, there are binding requirements on the quality of the main data, particularly for default and historical loss information used both for model development and the quantification of risk parameters, as well for data documentation, reporting and the supporting IT infrastructure.

[12] See Annex 1 for more details.

[13] "Guide to fit and proper assessments", ECB, December 2021.

[14] "Guide on climate-related and environmental risks", ECB, November 2020.

The ECB uses the BCBS 239 principles as a benchmark of best practices when assessing institutions' RDARR capabilities. The ECB applies the principle of proportionality in its assessment, in line with national law implementing Article 74(2) CRD. The ECB's Report on the Thematic Review on effective risk data aggregation and risk reporting identifies a set of best practices and areas of concern related to the BCBS 239 principles.

3 Supervisory expectations

The ECB strongly recommends that significant institutions make substantial progress in improving their data aggregation capabilities and internal risk reporting practices and has identified seven key areas of concern. These seven areas, detailed in Sections 3.1 to 3.7 below, are considered important prerequisites for robust governance arrangements and effective processes for identifying, monitoring and reporting risks. They are intended to be addressed within a reasonably short time frame, if not properly addressed already.

3.1 Responsibilities of the management body

In accordance with Article 88(1) CRD and its respective national transpositions, as interpreted by Title II of the EBA Guidelines on internal governance (EBA/GL/2021/05), the management body must oversee the implementation of the institution's strategic objectives, risk strategy and internal governance. The management body comprises a supervisory function and a management function that may be performed by either a single body or two separate bodies. Which key elements of RDARR are under the responsibility of which function within the management body depends on the structure adopted by institutions, on the applicable governance structures foreseen in national company law and regulations, and on the internal governance arrangements of the institution.[15] This Guide does not advocate any particular governance structure and is intended to embrace all existing structures.

The management body's responsibilities, role and the institution's risk culture are paramount in ensuring effective processes are in place for identifying, managing, monitoring and reporting risks, as well as adequate and robust internal control mechanisms. Lacking or insufficient knowledge, training and experience in RDARR topics and IT or lacking or insufficient awareness of the underlying risks means that improvements may be only partially or ineffectively implemented. To ensure appropriate risk data aggregation capabilities and internal risk reporting practices, the management body of each significant institution is responsible for the following.

1. Accepting accountability and exercising full responsibility for risk data quality and governance as a part of the overall risk management framework.

[15] The applicable law may consist of national regulations which may need to be interpreted in line with relevant Union law and EBA guidelines; see recitals 55-56 and Article 3(1), points 7-9 of CRD.

2. Making RDARR a key priority for the institution and ensuring that adequate and sufficient material, financial and human resources are dedicated to it. In addition, the management body should approve and implement the institution’s data governance framework. This includes setting (i) detailed requirements for data quality in terms of accuracy, integrity, completeness and timeliness in normal and in stress periods, and (ii) detailed key performance indicators for monitoring data quality.

3. Overseeing, prioritising and monitoring key deliverables within the agreed timelines of the remediation programmes (see Section 3.7) and the standard business processes, as well as regularly assessing RDARR capabilities in relation to the best practices described in the BCBS 239 principles. Additionally, the management body should establish the institution's view of what it means to adhere to the BCBS 239 principles, while also considering any potential limitations that might prevent full risk data aggregation in technical or legal terms.

4. Selecting one or two members of the management body in its management function to exercise responsibility for implementing the data governance framework.[16] This does not, however, in any way discharge the management body from its overall accountability and responsibility for the data governance framework of the institution. In cases where only one or two persons constitute the management function of the management body, also considering paragraph 25 of the background and rationale of EBA/GL/2021/05, one or two senior manager(s) with a direct reporting line and access to the management body should be appointed as having responsibility for ensuring implementation of the data governance framework in the institution.

5. Setting clear roles and responsibilities for RDARR within the business organisation (including relevant committees), as well as particular roles and responsibilities described in Section 3.3.

6. Ensuring the implementation of policies and processes for RDARR at the group level. The management bodies of the subsidiaries are responsible for implementing these group-wide policies and processes.

7. Regularly confirming that the internal risk reports are meaningful and well balanced in terms of qualitative and quantitative information and contribute to sound decision making.

8. Regularly monitoring the defined data quality key performance indicators and corresponding action plans to solve significant deviations identified. This

[16] It has been observed that the selection of one or two specific member(s) of the management body in its management function for RDARR facilitates the implementation of the framework and ensures that sufficient attention is devoted to data governance at the management body level. Appointing the CRO or the CRO together with the CFO – as responsible persons is seen as a pragmatic solution (if at the management body level). Where the management body delegates the executive function to a single person, selecting a senior manager as the head of the risk management function to exercise responsibility for implementing the data governance framework is seen as adequate.

includes responsibility for the implementation of robust data quality processes and controls.

9. Ensuring that members of the management body and heads of internal control functions, including the heads of risk management, compliance and internal audit, have a sufficient understanding of data management, IT and financial and non-financial risks (including, among others, climate risk and IT and security risks), as well as the related data and reporting requirements. If required for their position or institution, the management body should ensure its members have sufficient skills and experience in those same areas. This enables individual members to assess the effect of these matters on the institution's business and to address the challenges posed by the digitalisation of the banking sector and climate-related risks.

10. Ensuring that the knowledge, skills and experience of its members relating to data management, IT and financial and non-financial risks, as well as the related data and reporting requirements, are considered when assessing the collective suitability of its members. This should also be reviewed on an ongoing basis.

11. Subject to role-specific considerations, undertaking regular training to ensure that individual members of the management body possess sufficient and up-to-date knowledge and skills that allow them to understand and assess the business and main risks of the institution, including data management, IT, financial and non-financial risks, as well as the related data and reporting requirements, and their impact on the operations of the institution.

3.2 Sufficient scope of application

In line with the provisions of the national transposition of Articles 74 and 76 CRD, institutions should establish a data governance framework that allows the supervised institution to identify, manage, monitor and report risks. To ensure the completeness of processes and control mechanisms, the framework should be applicable to all material legal entities, risks and business lines as well as financial and supervisory reporting processes, and should cover the entire lifecycle of the data (i.e. all processes from data origination, capture and aggregation to reporting). In this regard, the ECB recommends that institutions fully integrate the data governance framework into the existing governance arrangements. Institutions should ensure that existing processes and control mechanisms are adequate and sufficient to manage data quality throughout the group (e.g. for financial and supervisory reporting processes).

The data governance framework of an institution should clearly define and document the scope of application and should specify the reports, models and risk indicators that are included, considering the nature, scale and complexity of the institution's operations and its risk profile.

Clear, proportionate and measurable criteria should be defined for material legal entities and included in the scope of application. Furthermore, this scope should include all material risks and risk concentrations from the institution's risk identification process.[17]

1. In terms of reports, the ECB recommends that the scope of the data governance framework should comprise, at a minimum, the following.

   (a) Internal risk reports used in decision-making and steering processes. This includes reports that provide information on risk appetite indicators (metrics and limits) as well as the main overall risk reports and main risk reports per material risk type (financial and non-financial).

   (b) Financial reports that are externally published as well as annual financial statements.

   (c) Supervisory reports that are submitted to financial supervisory or regulatory authorities. This includes FINREP/COREP reporting templates including the Short Term Exercise, submissions to EU-wide EBA stress tests and SREP stress tests[18] and Pillar 3 disclosures.

2. In terms of models, the scope should include key internal risk management models including, but not limited to, 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 IFRS9 collective provisions models and value-at-risk models). This includes input data for model development as well as resulting model outputs (e.g. exposure at default, probability of default or loss-give-default estimates) that are crucial for managing the risks faced by the institution.

3. In terms of key risk indicators, the scope should include at least the institution's risk appetite indicators as well as other key risk indicators referred to in the internal risk, financial and supervisory reports and models described above. The set of key risk indicators depends on the risk profile of the institution and should be defined by the institution itself. In this regard, the critical data elements underlying the key risk indicators should also be explicitly identified.[19]

3.3 Effective data governance framework

A clear allocation of roles and responsibilities in the area of data quality, as well as ownership of data quality for business, internal control and IT functions, is required to establish and maintain effective governance processes and control mechanisms

[17] See the ECB Guide to the internal capital adequacy assessment process (ICAAP), ECB, November 2018. See also the ECB Guide on climate-related and environmental risks and the BCBS Principles for the effective management and supervision of climate-related financial risks.

[18] Taking place every 2 years. See the ECB's banking supervision website for more information on EU-wide EBA stress tests and SREP stress tests.

[19] In this context, critical data elements are those data elements that are used to calculate the key risk indicators and have a direct or significant impact on the value of the indicator or technical routine of the calculation and the reporting.

within the overall internal control framework.[20] To ensure the effectiveness of a group-wide data governance framework, significant institutions should set out clear requirements for data quality within the scope of application. The frameworks should be formalised in internal policies covering the underlying processes, including the roles and responsibilities of the different functions involved as well as any related decision-making process, and subject to approval at an appropriate level and regular review.

The following list details the minimum elements which in the ECB's view institutions should have in place to achieve an effective data governance framework, both at the group level and at the level of material legal entities.

1. Data owners responsible for key risk indicators and critical data elements throughout the complete aggregation process (front to end). Delegation of this responsibility is generally considered to be adequate and includes:
   - contributing, in alignment with data users (or consumers), to the definition of data quality controls and the classification of key risk indicators and underlying critical data elements;
   - ensuring the accuracy, integrity, completeness and timeliness of data;
   - ensuring the monitoring and reporting of data quality through data quality processes;
   - ensuring the remediation of insufficient data quality;
   - managing metadata relating to the data lineage and data dictionary (see Section 3.4).
2. A central data governance function that is responsible for (i) issuing policies and processes for data quality management, (ii) overseeing proper implementation of the data governance framework across the organisation, (iii) ensuring the evaluation and monitoring of data quality, and (iv) participating in change management processes with a material impact on RDARR, such as those triggered through mergers or acquisitions of material legal entities, the outsourcing of functions to third parties, the launch of new products, the launch of new tools, upgrades of existing tools and other IT change initiatives.
3. A validation function within the second line of defence that is independent from the units involved in data governance, RDARR processes and ensures that the institution's RDARR processes are functioning as intended. In cases where the validation function is part of the same function that is responsible for data governance or RDARR (e.g. the risk management function), adequate segregation of duties and other mitigating measures should be implemented in order to avoid or mitigate conflicts of interest.[21] This validation function should perform regular assessments of the institution's RDARR capabilities for all

[20] The general requirements for an internal control framework and the respective responsibilities of the internal control functions remain (Title V, EBA Guideline on internal governance (EBA/GL/2021/05)).

[21] See paragraph 107 of EBA/GL/2021/05.

material entities and risk types and should cover all components of the RDARR processes (e.g. IT infrastructure, data lineage and data taxonomy), including the oversight of outsourced functions, IT change initiatives, mergers and acquisitions and new product launches. It should also be equipped with adequate and sufficient human resources and the relevant IT, data and reporting expertise. Appropriate organisational arrangements should be in place to ensure the effective independence of this validation function. The decision as to which specific organisational arrangements to adopt should take the nature, size and scale of the institution into consideration, as well as the complexity of the risks inherent in its business model.

4. An internal audit function that serves as the third line of defence and periodically provides independent reviews of the validation function, data governance framework, RDARR capabilities and processes and the quality of data used for the quantification of risks. These independent reviews may be complemented by supervisory reviews or, whenever deemed necessary by the institution, by an external independent review.

3.4 Integrated data architecture

To ensure the quality of the data used for risk, supervisory and financial reporting, an integrated data architecture[22] should be implemented and documented at the group level. This should include data taxonomies – specifically a dictionary of the main business definitions and a metadata repository – that cover material legal entities, business lines, material risks and related reports, key risk indicators and their critical data elements, as well as models that are within the scope of application. There could be specific data taxonomies per risk type or legal entity, as long as these are consistent and cover the scope of application (see Section 3.2). The management of data taxonomies should entail:

1. uniform data definitions and glossaries with clear ownership of data;

2. validation rules allowing specific values or a range of values;

3. complete and up-to-date data lineages[23] on data attribute level[24] (starting from data capture and including extraction, transformation and loading) for the risk

[22] Data architecture enables the institution to integrate all relevant data sources in line with defined data taxonomies.

[23] Data lineage is information about the movement and transformation of data from front (capture) to end and enables a bank to (i) understand if data quality controls are sufficient and well placed in the data flow, (ii) identify interconnections between data definitions and taxonomies, (iii) ensure that when data fields are loaded or transformed across or within systems they are still in line with the reporting requirements and definitions, (iv) support the identification of data points needed for specific ad hoc reporting needs, (v) in case of data quality incidents be able to track back the source of the issue in a timely manner and to (vi) allow traceability for (external) validation.

[24] A data element contains information as an independent field while a data attribute, in general, is a single value description (i.e. its metadata, such as a business description of the content, type, format, etc.) for a data element (or data point or data object). As an example, data attributes are often stored as a column in a table and are used in the technical mapping to calculate key risk indicators, whereas data elements impact the specific indicator values.

indicators, and their critical data elements, identified as being within the scope of application (see point 3 of Section 3.2).

Implementation choices should be fit for purpose, well documented and focused on providing the necessary information for steering the institution and managing its risks.

3.5 Group-wide data quality management and standards

Group-wide policies and processes should be established within the overall risk management framework or the data governance framework to ensure that data quality controls are effective and complete and material data quality issues are remediated, as well as to make any limitations transparent and account for data quality risks within the scope of application. Such group-wide policies and processes should ultimately include the following.

1. The implementation of data quality controls (covering, at least, the dimensions of accuracy and integrity, completeness and timeliness) from front office systems (and other capture systems) to the reporting layer for the key risk indicators and critical data elements identified as being in the scope of application, automated where appropriate. In addition, periodical reconciliation with institutions' sources and reports (in the areas of accounting and finance and with external sources used) and related model development data.

2. The definition and measurement of data quality indicators covering, at least, the dimensions of accuracy and integrity, completeness and timeliness (including tolerance levels and robust correction processes) with documented operational processes in case of breaches. Data quality indicators should allow for the systematic monitoring and recording of the quality of the related data covering the entire lifecycle of the data.[25] They should also be periodically communicated to the institution's management body alongside an impact analysis of the given data quality on risk measurement effectiveness and the risk profile of the institution (see Section 3.1).

3. An up-to-date and complete overview ("register") of data quality issues and limitations, including (i) an assessment of the severity of these issues, (ii) a root cause analysis, (iii) a quantitative impact analysis of material/severe data errors on the risk and business areas affected, (iv) clearly defined processes and responsibilities for remediating and escalating data quality issues, depending on the materiality of the issues, (v) deadlines for remediation, and (vi) a date for effective remediation (including appropriate evidence).

[25] As an example, the ECB identified good practices related to the assessment of the quality of data used from third-party providers in its "Good practices for climate-related and environmental risk management".

4. The full integration of end-user computing or end-user developed applications, including an overview of such applications, into data quality management policies and processes.

5. Arrangements for any manual workarounds within the scope of application to be documented and subjected to adequate control mechanisms (e.g. the "four-eyes principle", rigorous documentation and audit trailing of changes, data overrides and sign-offs) until the data preparation and reporting steps that are determined to have a material impact on data quality are embedded in an audit-trailed IT-controlled environment.

6. Adequate consideration of data quality risks in the internal capital adequacy assessment process (ICAAP) and the internal liquidity adequacy assessment process, as existing data quality issues might lead to an underestimation of risks and should be addressed in the risk quantification by an additional margin of conservatism.

3.6 Timeliness of internal risk reporting

Accurate, complete and timely data are fundamental to effective risk management and identification. To manage risks effectively, the right information needs to be presented to the right people at the right time. There are two factors that determine the timeliness of risk reporting: the frequency of risk reporting and the time needed to produce the reports.

The frequency of internal risk reporting should be consistent with the dynamics of potential changes to the risk figures: greater dynamism requires higher reporting frequencies. For example, the ECB Guide to the ICAAP clarifies[26] that "the frequency of reporting of the ICAAP outcomes (such as how material risks, key indicators, etc. are evolving) to the management body is expected to be at least quarterly but, depending on the size, complexity, business model and risk types of the institution, reporting might need to be more frequent to ensure timely management action". Additionally, different types of risk figures are subject to different degrees of dynamism, with economic risk measures generally being more volatile than normative risk measures and, thus, generally requiring higher reporting frequencies.

The time needed to produce a risk report has a similar impact on the effectiveness of risk management: the longer it takes an institution 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.

The ECB expects an institution to ensure that the combination of reporting frequency and production time is calibrated in such a manner as to allow for timely reactions to changes in its risk situation, thereby complying with its set of internal risk appetite indicators (metrics and limits). For internal risk reports in normal situations, it is generally understood that institutions will not be able to react to changes in a timely

[26] In paragraph 29.

manner if a monthly or quarterly risk report needs more than 20 working days to produce. The production time is dependent on the materiality and volatility of the key risk indicators to be reported.

In addition to sound reporting capabilities in normal situations, institutions should implement effective RDARR capabilities for stress or crisis situations to adequately manage unexpected stress events, such as the recent COVID-19 pandemic, as well as to ensure proper adaptation to new or altered reporting and disclosure requirements. In times of emerging stress, risk data aggregation capabilities should be adaptable enough to meet ad hoc data requests with sufficient granularity (e.g. customer data for managing credit risk concentrations) both at entity and at group level. The ECB expects timely risk reporting to remain unhampered by such issues as a fragmented IT infrastructure or a large amount of manual aggregation processes, even in stress situations.

3.7 Effective implementation programmes

Institutions that do not yet follow the best practices that are described in the BCBS 239 principles should put implementation measures in place accordingly. An implementation programme should cover any gaps and address any weaknesses identified through internal or external reviews, including OSIs and off-site reviews by ECB Banking Supervision. The programmes should be supported by adequate project management governance, including measures and metrics to control project execution risks, and adequate material, financial and human resources. 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. Implementation activities should consider their potential effect on (i) internal models, (ii) interactions and interdependencies of risk data aggregation with the integration of financial reporting frameworks, and (iii) overall business and ICT strategies. The implementation programmes should be ambitious yet feasible. Periodical reporting on the progress of the programmes, including analysis of impediments, delays and other factors, should be in place.

As specified in point 3 of Section 3.1, the management body is responsible for the timeline and milestones of the implementation. Good project management practices provide that one or two member(s) of the management body in the management function to be appointed with responsibility for the execution of the programme, and reporting to the management body in its supervisory function. The management body requests and receives regular information on the progress made and assesses and reacts to any delays in the implementation.

4 Supervisory approach

This Guide is a key building block of the 2023-25 work programme. With it, the ECB details its minimum supervisory expectations for a set of priority topics that have been identified as necessary preconditions for effective RDARR.

The more targeted focus of supervisory activities on the areas that are critical to delivering progress is coupled with a more intrusive use of supervisory powers to tackle severe, long-lasting deficiencies. The work programme includes (i) additional targeted engagement with a clear focus on selected priority areas, in particular on the responsibility of management bodies for governance and execution oversight, (ii) horizontal benchmarking of findings from off-site and on-site activities against expectations expressed in the Guide, and (iii) an enhanced focus on the data quality of institutions' supervisory reporting.[27]

ECB Banking Supervision is committed to using all of its supervisory tools and powers if supervisory measures and time frames are not met (e.g. in the context of the SREP, related regular supervisory activities, OSIs and internal model investigations).

Accordingly, ECB Banking Supervision is intensifying its intrusiveness in the context of the annual SREP assessments, as well as in more targeted engagements. Related findings and measures are being closely followed up.[28] Supervisory intensity is being upscaled in cases where past supervisory actions have not led to the desired changes in a timely manner or where deficiencies continue to be evidenced (e.g. in the biennial EBA/SSM stress tests). The ECB is further strengthening the use of quantitative and qualitative measures to address gaps in institutions' internal control and governance frameworks, in particular for RDARR. Effective supervisory tools that are being used include clear qualitative requirements with time-bound milestones for remediation. If such requirements and timeframes are not met by institutions, or material shortcomings breaching the applicable framework are evidenced (such as inaccurate information reported on key risk indicators), the matter is escalated further and can potentially result, for example, in the imposition of enforcement measures, sanctions and capital add-ons. Furthermore, as the management body is accountable for the implementation of effective and prudent governance arrangements, deficiencies in these areas may also lead to a reassessment of the suitability of the responsible members[29] and, in severe cases, the removal of such members.

[27] This applies to the data quality of FINREP/COREP templates in particular. For this, the ECB uses data quality indicators that represent the minimum quality standards expected from the banks in terms of accuracy, timeliness and completeness. In addition, the ECB publishes additional data quality checks twice per year, which are aimed at enhancing the quality of supervisory reporting data in accordance with Article 4(1) of Decision ECB/2014/29 of 2 July 2014 as amended by Decision ECB/2017/23 of 3 August 2017. See the ECB's banking supervision website for more information on additional supervisory data quality checks. Furthermore, institutions are expected to always ensure consistency between their supervisory reporting and Pillar 3 disclosures. They can count on the support of the EBA, which has prepared and maintained a tool that specifies the mapping of the templates and tables for disclosures with those on Implementing Technical Standards reporting. The mapping tool is accessible to the public on the EBA's website.

[28] See "Aggregated results of SREP 2023", ECB, December 2023.

[29] See Section 5.2 of the "Guide to fit and proper assessments", ECB, December 2021.

In addition, RDARR capabilities are being considered as an important aspect in many regular supervisory activities. The ECB takes these capabilities into account when assessing consolidation transactions, for instance in the context of the consolidation plan.[30] Furthermore, in the context of fit and proper assessments, the ECB, together with the national competent authorities, assesses the knowledge, experience and skills of members of the management body and – where an assessment is provided under national law – key function holders, taking institution-specific and role-specific circumstances into consideration. In the particular context of the ongoing digitalisation of the banking sector and the associated security threats, the suitability assessments take into consideration the risks that institutions may be exposed to, including data management, IT and security risks and climate-related and environmental risks[31], as well as related data and reporting requirements, subject to a case-by-case analysis.

Within the context of supervisory reporting, ECB Banking Supervision has consolidated and complemented the measurement of data quality by introducing its Management Report on Data Governance and Data Quality. When completing this report, institutions are asked to respond to a set of open questions, with at least one member of the management body signing the answers to further foster management body accountability.

Furthermore, the ECB continues to assess data governance and quality management through OSIs and internal model investigations, including, but not limited to, dedicated inspections on RDARR.[32]

With this Guide, the ECB intends to reinforce and clarify its minimum supervisory expectations on a set of priority topics that are preconditions for effective RDARR. This is to support institutions in improving their data governance framework and governance arrangements and ensuring effective processes are in place to identify, manage, monitor and report risks through adherence to the BCBS 239 principles and by setting priorities for implementation projects. The ultimate objective of this is to ensure that institutions have effective steering and risk management based on reliable information.

[30] See Section 2.2 of the "Guide on the supervisory approach to consolidation in the banking sector", ECB, January 2021.

[31] "ECB Guide on climate-related and environmental risks", ECB, November 2020, provides and explains a series of standards on reporting related to climate risk." Walking the talk - Banks gearing up to manage risks from climate change and environmental degradation - Results of the 2022 thematic review on climate-related and environmental risks", ECB, November 2022, gives an overview of the implementation of these supervisory expectations and points out that the collection of granular data and efforts to overcome data gaps are still in their early stages. "Good practices for climate-related and environmental risk management", ECB November 2022, includes a number of examples of good practices in data governance and internal risk reporting. In addition, in 2022 the ECB performed a climate risk stress test ("2022 climate risk stress test", ECB, July 2022, and "ECB report on good practices for climate stress testing", ECB, December 2022).

[32] See Section 1.2.3.3 of the "ECB Annual Report on supervisory activities 2023", ECB, March 2024.

Annex 1: Regulatory references

Since stating the main principles for a strong governance framework, risk data architecture and IT infrastructure, and describing the main dimensions of institutions' risk data aggregation capabilities and internal risk reporting practices in the BCBS 239 principles, the BCBS has followed up with several progress reports.[33] These reports issued recommendations to institutions with regard to continuing their implementation efforts, as well as recommendations to supervisors monitoring their progress.

CRD defines a set of requirements applicable to RDARR that need to be transposed into national law. Article 74 CRD requires institutions to have "[…] robust governance arrangements, which include a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective processes to identify, manage, monitor and report the risks they are or might be exposed to, adequate internal control mechanisms, including sound administration and accounting procedures, and remuneration policies and practices that are consistent with and promote sound and effective risk management." According to Article 76 CRD, "Member States shall ensure that the management body approves and periodically reviews the strategies and policies for taking up, managing, monitoring and mitigating the risks the institution is or might be exposed to" and, according to Article 88(1)(b) CRD, "[…] the management body must ensure the integrity of the accounting and financial reporting systems, including financial and operational controls and compliance with the law and relevant standards". Finally, for the members of the management body to be able to perform their tasks and responsibilities, they also have to comply with Article 91 CRD, which provides that "[…] members of the management body shall possess sufficient knowledge, skills and experience to perform their duties […] and the management body shall possess adequate collective knowledge, skills and experience to be able to understand the institution's activities, including the main risks. The overall composition of the management body shall reflect an adequately broad range of experience".[34] An overview of relevant national transpositions is provided in Annex 2.

In its Guidelines for common procedures and methodologies for the SREP and supervisory stress testing (EBA/GL/2022/03), the EBA provides that "[…] competent authorities should assess whether the institutions´ information and communication technologies are effective and reliable and whether these systems fully support risk data aggregation capabilities at normal times, as well as during times of stress".

The EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) define ICT and security risk as the "risk of loss due to breach of confidentiality, failure of integrity of systems and data, inappropriateness or unavailability of systems and data or inability to change IT within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes

[33] Most recently in "Progress in adopting the Principles for effective risk data aggregation and risk reporting", Basel Committee on Banking Supervision, November 2023.

[34] When taking fit and proper decisions, the ECB applies the substantive fit and proper requirements laid down in the binding national law which implements Article 91 CRD (a minimum harmonisation provision).

security risks resulting from inadequate or failed internal processes or external events including cyber-attacks or inadequate physical security." These guidelines include specifications on the integrity of data as well as ICT project and change management.

Furthermore, the EBA Guidelines on internal governance (EBA/GL/2021/05) state that "regular and transparent reporting mechanisms should be established so that the management body, its risk committee, where established, and all relevant units in an institution are provided with reports in a timely, accurate, concise, understandable and meaningful manner and can share relevant information about the identification, measurement or assessment, monitoring and management of risks".

The joint ESMA and EBA Guidelines on the assessment of suitability of members of the management body (EBA/GL/2021/06) require that members of the management body have an up-to-date understanding of the business of the institution and its risks and, collectively, that the management body is able to understand the institution's activities and main risks. To this end, when assessing the knowledge, skills and experience of a member of the management body, supervisors should give consideration to experience relating to, among other areas, risk management, the assessment of the effectiveness of an institution's arrangements, the interpretation of an institution's financial information and the identification of key issues based on this information. In the specific framework of collective suitability, the joint ESMA and EBA Guidelines require that the management body collectively possess the skills to effectively manage and oversee the institution, including, among other aspects, the business of the institution, the main risks related to it and IT and security.

The ECB's Report on the Thematic Review on effective risk data aggregation and risk reporting identifies a set of best practices and areas of concerns related to the BCBS 239 principles.

For institutions using internal models to determine regulatory capital requirements, there are binding requirements on the quality of the main data, in particular regarding default and historical loss information used for model development and the quantification of risk parameters, as well as for data documentation and reporting and supporting IT infrastructure. The ECB Guide to internal models[35] includes a granular overview of requirements from the Capital Requirements Regulation (CRR), Commission Delegated Regulations, and other supervisory work in this area, namely EBA draft regulatory technical standards, guidelines and BCBS principles for the key areas of use for internal models. In particular, the ECB Guide to internal models includes a section dedicated to data maintenance for the IRB approach, in accordance with Articles 144(d), 174(d) and 176 CRR. With regard to internal validation requirements for the IRB approach, in 2023 the EBA finalised the supervisory handbook for the validation of IRB systems that covers the governance and main responsibilities of the internal validation function as well as specific content

[35] See "ECB guide to internal models", ECB, February 2024.

on the assessment of the modelling environment, focusing on data quality and IT implementation.

The ECB Guide to fit and proper assessments[36] specifies the ECB's understanding of the applicable legal framework and, thereby, its main expectations and policies when conducting suitability assessments of members of management bodies, key function holders and branch managers, within the scope of the applicable national law. These include the assessment of theoretical knowledge and practical experience from both an individual and a collective suitability perspective, taking institution-specific and role-specific circumstances into account.

The ECB Guide on climate-related and environmental risks[37] provides and explains a series of expectations on reporting related to climate-related and environmental risks, taking into account the EBA Guidelines on internal governance (EBA/GL/2021/05). In this regard, the ECB expects institutions, among other things, to systematically collect and aggregate the data needed to provide their management bodies with risk reports assessing the impact of climate-related and environmental risks on their business model, strategy and risk profile in a timely manner.

From a macroprudential perspective, the European Systemic Risk Board (ESRB) has repeatedly highlighted the importance of receiving high-quality data in order to monitor and address financial stability risks. In the context of the reporting required by the European Market Infrastructure Regulation, the ESRB has highlighted the difficulties that persistent data quality issues pose for the adequate monitoring of financial stability risks. It has made concrete proposals to improve supervisory reporting and has called for increased supervisory attention to be paid to data quality.[38]

Annex 2: National transpositions of relevant CRD IV provisions

- Belgium: Circular on the Bank's expectations as regards quality of reported prudential and financial data (Circular NBB_2017_27) of the Nationale Bank van België/Banque Nationale de Belgique, which requires institutions to establish robust governance and control frameworks on the quality of the prudential and financial data

- Bulgaria: Articles 11(1-2), 10(4,6), 73(1), 73b(1-3) and 74(3) of the Law on credit Institutions (Закон за кредитните институции); Article 2 of the Bulgarian National Bank's Ordinance No 7; Articles 4-7 and 13-14 of Ordinance No 10

- Germany: The third sentence of Section 25a(1) of the German Banking Act (*Kreditwesengesetz*), the German Federal Financial Supervisory Authority's understanding of which is specified in module AT 4.3.4 of the Minimum

[36] "Guide to fit and proper assessments", ECB, December 2021.

[37] "Guide on climate-related and environmental risks", ECB, November 2020.

[38] "ESRB's view regarding data quality issues and risks for financial stability", ESRB, 2022; "EMIR 3.0 / EMIR review", ESRB, 2023.

Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* – MaRisk)

- Estonia: Articles 82, 55, 48 of the Credit Institutions Act *(Krediidiasutuste seadus*)

- Ireland: Regulations 61, 64, 79 of Statutory Instrument 158/2014 and the Central Bank of Ireland's Corporate Governance Requirements for Credit Institutions

- Greece: Article 66 (1-2) on robust governance arrangements, effective processes for identifying, managing, monitoring and reporting the risks, internal control mechanisms, remuneration policies and practices of Law 4261/2014 on Access to the activity of credit institutions and prudential supervision of credit institutions (transposition of Directive 2013/36/EU), repeal of Law 3601/2007, and other provisions (*Πρόσβαση στη δραστηριότητα των πιστωτικών ιδρυμάτων και προληπτική εποπτεία πιστωτικών ιδρυμάτων (ενσωμάτωση της Οδηγίας 2013/36/ΕΕ), κατάργηση του ν. 3601/2007 και άλλες διατάξεις*)

- Spain: Section 6, item 52 on data aggregation and risk reporting of Circular 2/2016 of the Banco de España

- France: Article 104 of Arrêté du 3 novembre 2014 relatif au contrôle interne des entreprises du secteur de la banque, des services de paiement et des services d'investissement soumises au contrôle de l'Autorité de contrôle prudentiel et de résolution

- Croatia: Hrvatska narodna banka’s Decision on governance arrangements (*Odluka o sustavu upravljanja*); Articles 103 and 104 of the Credit Institutions Act (*Zakon o kreditnim institucijama*)

- Italy: First part, Title IV, Chapter 4, Section V of the Banca d’Italia’s Circular No 285/2013 on Prudential Requirements and Standards (*Disposizioni di vigilanza per le banche*); Article 53 and Article 53 bis of Legislative Decree 385/1993 on the Consolidated Law on Banking (*Testo Unico Bancario*)

- Cyprus: The Central Bank of Cyprus’ Directive on Internal Governance of Credit Institutions (*Η περί Εσωτερικής Διακυβέρνησης των Πιστωτικών Ιδρυμάτων Οδηγία*)

- Latvia: Financial and Capital Market Commission Regulation No. 277: Regulation on Establishment of the Internal Control System (*Iekšējās kontroles sistēmas izveides normatīvie noteikumi*)

- Lithuania: Resolutions of the board of Lietuvos bankas No 03-176 and 149

- Luxembourg: Paragraph 132, chapter II of Circular CSSF 12/552 of the Luxembourg Financial Sector Supervisory Commission (“Commission de Surveillance du Secteur Financier” – “CSSF”) on central administration, internal governance and risk management; paragraph 30 of Circular CSSF 11/506 of the Luxembourg Financial Sector Supervisory Commission on principles of a sound stress testing programme

- Malta: Articles 14 and 17b of the Banking Act (Chapter 371 of the Laws of Malta), Malta Financial Services Authority's Banking Rule BR/24 on Internal Governance of Credit Institutions Authorised Under the Banking Act
- Netherlands: Article 3:17 of The Financial Supervision Act (*Wet op het financieel toezicht*); Articles 17, 20, 23, 23a of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft*)
- Austria: Article 39 of the Austrian Banking Act (*Bankwesengesetz*) and Article 3(4) and Article 3(5) of the Austrian Financial Market Authority's Regulation on Credit Institute Risk Management (*Kreditinstitute-Risikomanagementverordnung*)
- Portugal: Articles 115-A and 115-K of the Legal Framework of Credit Institutions and Financial Companies; Notice of Banco de Portugal No 3/2020 (on internal governance and internal control); Circular-Letter of Banco de Portugal No 2020/05 (*Expetativas de supervisão relativas a capacidades de agregação e práticas de reporte de dados de riscos*)
- Slovenia: Chapter 6 of the Slovenian Banking Act (*Zakon o bančništvu*)
- Slovakia: Section 23, 24 and 27 of Act No 483/2001 on Banks and on amendments and supplements to certain laws (Zákon o bankách a o zmene a doplnení niektorých zákonov); Articles 2, 4, 5, 6, 7, 11(2)(b), 12(2)(e) and 13(1)(c) of the Decree of Národná banka Slovenska 4/2015 on additional types of risk, on details of the risk management function of banks and branches of foreign banks and on the definition of a sudden and unexpected change in market interest rates (*Opatrenie o ďalších druhoch rizík, o podrobnostiach o systéme riadenia rizík banky a pobočky zahraničnej banky a ktorým sa ustanovuje čo sa rozumie náhlou a neočakávanou zmenou úrokových mier na trhu*)
- Finland: Chapter 7, Section 1, Chapter 9, Sections 2 and 3 and Chapter 11, Section 6a of the Act on Credit Institutions (*Laki luottolaitostoiminnasta Kreditinstitutslag*); Chapter 6.1, paragraph 3 and Chapter 8 of the FIN-FSA Finnish Financial Supervisory Authority's Regulations and Guidelines 8/2014 on Management of operational risk in supervised entities of the financial sector (*Operatiivisen riskin hallinta rahoitussektorin valvottavissa*) of the Finnish Financial Supervisory Authority

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.bankingsupervision.europa.eu

For specific terminology please refer to the SSM glossary (available in English only).

PDF ISBN 978-92-899-6667-2, doi:10.2866/081671 QB-05-24-202-EN-N