EUROPEAN CENTRAL BANK
BANKING SUPERVISION

Guide on effective risk data aggregation and risk reporting

July 2023 (draft for public consultation)

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 large losses due to, for example, an inability to quantify group-wide exposures to specific groups of clients in a 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, 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 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 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, timeliness and adaptability are still widely encountered, suggesting that institutions are still focusing on the cost and implementation challenges of improving risk data

[1] See, for example, "A marathon, not a sprint: Capturing value from BCBS 239 and beyond", McKinsey & Company, 2015 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.

aggregation and reporting, rather than the benefits of remediating long-standing deficiencies in this area.

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 (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 revealed shortcomings in the effective data risk aggregation frameworks. 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. The identified issues were followed up during dedicated on-site inspections and as part of the Supervisory Review and Evaluation Process (SREP). 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 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.[6]

ECB Banking Supervision has identified deficiencies in RDARR as a key vulnerability in its planning of supervisory priorities for the 2023-25 cycle, and has developed a comprehensive, targeted supervisory strategy for the upcoming years. This strategy

[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] RDARR was the worst-rated sub-category of internal governance in the 2022 SREP cycle and the ECB has observed an increasing number of outstanding supervisory measures in this area, most of them triggered by on-site inspections. 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 on-site inspections. 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.

aims to ensure that supervised institutions finally deliver substantial progress in remedying their identified structural shortcomings.

The purpose of the ECB Guide on risk data aggregation and risk reporting is to specify, underscore and reinforce supervisory expectations for RDARR. 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 includes a set of condensed prerequisites for effective RDARR that is intended to assist institutions in strengthening their capabilities, and also shares best 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.

These supervisory expectations have been verified by the ECB in conjunction with the national competent authorities, and explain in detail how ECB Banking Supervision applies the national laws transposing the Capital Requirements Directive (CRD)[7] on a case-by case basis and in line with the relevant European Banking Authority (EBA) guidelines (see Annex 1).

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 this guide addresses are not meant to be exhaustive or to limit any supervisory follow-up activity on risk data aggregation capabilities and risk reporting. 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 all RDARR-related recommendations addressed to them into account, such as recommendations on sound governance, risk management and data quality controls resulting from the SREP.

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

[7] 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).

consistent with effective risk management. The management bodies of institutions are assigned the responsibility of approving and periodically reviewing the strategies and policies for managing and monitoring risk. The members of management bodies are required to possess sufficient knowledge, skills and experience, both individually and collectively, to be able to perform their responsibilities and to 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 and ICT project and change management.[8] Furthermore, EBA guidelines specify that regular and transparent reporting mechanisms should be established at banks to provide 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/2017/12) require that the individual members of the management body of an institution 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[9] specifies the ECB's main expectations and policies for conducting suitability assessments of the members of an institution's management body.

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.

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, which are detailed below, are considered important prerequisites for robust governance and

[8] See Annex 1 for more details

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

effective processes to identify, monitor and report 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 paragraphs 19 to 27 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's responsibility, role and risk culture are all paramount in ensuring effective processes to identify, manage, monitor and report risks, as well as adequate internal control mechanisms. Insufficient knowledge, training and experience in RDARR topics and IT 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 and exercising full responsibility for risk data quality and governance as a part of the overall risk management framework.

2. Making RDARR a key priority for the institution and ensuring that adequate resources are dedicated to it. In addition, the management body should establish the institution's own view of what it means to be adherent to the BCBS 239 principles, as well as approve and implement the institution's RDARR frameworks. This includes setting (i) detailed requirements for data quality in terms of accuracy, completeness, timeliness and adaptability in normal and 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 be adherent to the BCBS 239 principles, while also considering any potential limitations that prevent full risk data aggregation in technical or legal terms. The management body should select at least one of its members to exercise this responsibility.

4. 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.

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

6. Regularly confirming that the internal risk, supervisory and financial reports are meaningful and well balanced in terms of qualitative and quantitative information and are able to contribute to sound decision-making. Furthermore, the management body should regularly monitor the defined data quality key performance indicators and corresponding action plans to solve significant deviations identified.

7. Ensuring that members of the management body and internal control functions, including the heads of risk management, compliance and audit, have a sufficient understanding of data management, IT and financial and non-financial risks (including, inter alia, climate risk and IT and security risk), as well as the related data and reporting requirements. If required for their position or institution, the management body should ensure members have sufficient skills and experience in those same areas. This allows for 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.

8. 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.

9. Subject to role-specific considerations, undertaking regular training to ensure that individual members possess sufficient up-to-date knowledge and skills that allow them to understand and assess the business and main risks of the institution, including data management, information technology, 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 controls, the framework should be applicable to all material legal entities, risk categories, business lines and financial and supervisory reporting processes, and cover the entire lifecycle of the data, i.e. all processes from data origination, capture and aggregation to reporting.

The data governance framework of an institution should clearly define and document the scope of application and specify the reports, models, risk data and indicators that are included. The data and critical data elements should also be explicitly identified. Furthermore, clear, proportionate and measurable criteria for material legal entities to be included in the scope of application should be defined.

1. In terms of reports, the scope of the data governance framework should comprise the following:

   (a) Internal risk reports that provide information on risk appetite indicators (metrics and limits), as well as main overall risk reports, main risk reports per material risk type (financial and non-financial) according to the institution's risk identification process and any reports that are part of the management information system and are therefore used in decision-making and steering processes.

   (b) Financial reports that are published on at least a quarterly basis, as well as annual financial statements.

   (c) Supervisory reports that are submitted to financial supervisory or regulatory authorities. This includes, for instance, FINREP/COREP reporting templates, submissions to EBA/SSM stress test exercises and Pillar 3 disclosures.

2. In terms of models, the scope should include all key internal risk management models, including, but not limited to, Pillar 1 regulatory capital models (e.g. internal ratings-based approaches for credit risk), Pillar 2 risk and capital models and other key risk management models (e.g. IFRS9 collective provisions models, value-at-risk models). This includes their development and input data, and resulting risk metrics and indicators that are crucial to managing the risks faced by the institution.

3. In terms of risk data and indicators, the scope should at least include the institution's risk appetite indicators and the main risk metrics referred to in the internal risk reports described above.

3.3 Effective data governance framework

Clear roles and responsibilities in the area of data quality, as well as ownership of data quality for business, control and IT functions, are required to establish and maintain effective processes and controls. To ensure the effectiveness of group-wide data governance frameworks, significant institutions should set out clear requirements for data quality within the scope of application. The following list details the minimum elements required to achieve an effective data governance framework, both at the group level and the level of material legal entities.

1. Data owners (or data stewards) representing the first line of defence and being responsible for critical data elements throughout the complete aggregation process (front to end). This includes:

   - contributing to the definition of data controls and the classification of key risk data;

   - ensuring the accuracy, integrity, completeness and timeliness of data;

- ensuring monitoring and reporting of data quality through data quality processes;
- remediating 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 guidelines on 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 relevant change management processes, such as those triggered through mergers or acquisitions of material legal entities, the outsourcing of services 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 of the first line and ensures that an institution's RDARR processes are functioning as intended. This validation function should perform regular assessments of the institution's RDARR capabilities for all material entities and risk types, and cover all components of the RDARR processes (e.g. IT infrastructure, data lineage, data taxonomy), including the oversight of outsourced activities, IT change initiatives, mergers and acquisitions and new product launches. It should also be equipped with sufficient resources and relevant IT, data and reporting expertise. Appropriate organisational arrangements should be in place to ensure the effective independence of this validation function. Such arrangements can include the following.

   - The adequate segregation of duties. This can involve (i) the separation of the validation function into two different units that each report to different members of senior management, (ii) the separation of the function into two different units that both report to the same member of senior management, or (iii) separate staff within the same unit.[10] The decision as to which organisational arrangement to adopt should take the nature, size and scale of the institution into consideration, as well as the complexity of the risks inherent to its business model.
   - A clear and effective organisational structure and reporting lines, such that the function is not subordinated to the control units that it validates unless there are adequate mitigants in place.

4. An internal audit function that serves as the third line of defence and periodically provides independent reviews of the data governance frameworks, RDARR capabilities and processes and the quality of data used for the

[10] The ECB considers the third option to potentially be more suitable for small legal entities that are not classified as global systemically important institutions or as other systemically important institutions.

quantification of risks. This may be complemented, 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 should be implemented and documented at the group level. This should include data taxonomies – specifically a dictionary of the main business concepts and a metadata repository – that cover material legal entities, business lines, material risks and related risk indicators, reports, and models that are within the scope of application. There could be specific data taxonomies per risk types or legal entities, as long as they are consistent and cover the scope of application (see Section 3.2). The management of data taxonomies is recommended to 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 (including data capture) for all risk indicators and metrics within the scope of application.

Implementation choices should be proportionate, well documented and focused on providing the necessary information for steering the institution and managing its risks (see also point three of the list in Section 3.1).

3.5 Group-wide data quality management and standards

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

1. The implementation of data quality checks from front office systems to the reporting layer, automated where appropriate, as well as periodical reconciliation with other sources and reports (i.e. in the areas of accounting, finance, and with external trusted sources like credit bureaus, land or housing registries, national authorities’ lists etc.) applied to all material risk indicators and related model development data. Additionally, the implementation of regular procedures to assess and ensure the accuracy of critical data for risk management at the source of data, front office and the risk reporting systems using such information.
2. The definition and measurement of data quality indicators (including tolerance levels) with documented operational procedures in case of breaches. Data

quality indicators should allow for the systematic monitoring and recording of the quality of the related data. 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.

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 quantitative impact analysis of material/severe data errors on the risk and business areas affected, and (iii) clearly defined responsibilities for remediating and escalating data quality issues depending on the materiality of the issues.

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

5. Arrangements for any manual workarounds within the scope of application to be documented and subjected to adequate controls (e.g. “four-eyes principle”, rigorous documentation and audit trailing of change management, data override and sign offs) until the data preparation and reporting steps that are determined to have 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 (ILAAP), as existing data quality issues might lead to an underestimation of risks and are expected to 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 is expected to be consistent with the dynamics of potential changes in the risk figures; higher dynamism requires higher reporting frequencies. For example, the ECB guide to the ICAAP clarifies 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”.[11] Additionally, different types of risk figures are subject to

[11] See paragraph 29 of the ECB Guide to the internal capital adequacy assessment process (ICAAP), ECB, November 2018.

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 report has a similar impact on the effectiveness of risk management: the longer it takes an institution to produce risk reports, the longer the period in which the risk situation remains unclear and the higher the likelihood of delayed reactions.

An institution is expected 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 regular reporting, it is generally understood that institutions will not be able to react to changes in a timely manner if a monthly or quarterly risk report needs more than 20 working days to be produced.

In addition to sound regular reporting capabilities, institutions should implement effective ad hoc RDARR capabilities 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 the managing of 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 programs

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 on-site inspections by ECB Banking Supervision. The programmes should be supported by adequate project management governance, including measures to control project execution risks, and adequate financial and human resources. The implementation plans should clearly define targets, milestones, roles, responsibilities and, if applicable, intermediate measures to mitigate weaknesses that require 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 integration 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 programs, including analysis of impediments, delays and other factors, should be in place.

As specified in point three of the list in Section 3.1, the management body decides on the accountability, timeline and milestones of the implementation. Good project management practices provide that at least one member of the management body should have responsibility for the execution of the programme. 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 on 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 are coupled with a more intrusive use of supervisory powers to tackle severe, long-lasting deficiencies. The work program 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[12] and the institution-specific supervisory "fire drill" exercises that test ad hoc reporting capabilities.

ECB Banking Supervision is committed to using all of its supervisory tools and powers if supervisory measures and timeframes are not met (e.g. in context of the SREP, related regular supervisory activities, on-site inspections 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.[13] 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 controls and governance, in particular for RDARR. Effective supervisory tools that are being used include clear, qualitative measures with time-bound milestones for remediation. If such measures and timeframes are not met with serious and sufficient rigour on the part of an institution's management body, or severe shortcomings breaching the applicable framework are evidenced (such as inaccurate

[12] 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, punctuality and completeness. In addition, the ECB publishes additional data quality checks two times 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 ITS reporting. The mapping tool is accessible to the public on the EBA website.

[13] See Section 5.2.4. of "Aggregated results of SREP 2022", ECB, February 2023.

information reported on key risk indicators), the matter is escalated, which potentially includes enforcement and capital add-ons.

In addition, RDARR capabilities are being considered as an important aspect in many regular supervisory activities. The ECB takes risk data aggregation and reporting capabilities into account when assessing consolidation transactions, for instance in context of the consolidation plan.[14] Furthermore, in the context of fit and proper assessments, the ECB, together with the NCAs, 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 those related to data management, IT and security risks and climate risk, 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 a 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 on-site investigations and internal model investigations, including, but not limited to, dedicated inspections on RDARR.[15]

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 governance arrangements and ensuring effective processes 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 that are based on reliable information.

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.[16] These

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

[15] See Section 1.3.2 of the "ECB Annual Report on supervisory activities 2022", ECB, March 2023.

[16] Most recently, in "Progress in adopting the Principles for effective risk data aggregation and risk reporting", Basel Committee on Banking Supervision, April 2020.

reports observed that none of the global systemically important institutions that were initially in scope had fully complied with the principles. As such, the reports issued recommendations to institutions for 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, paragraph 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”.[17] An overview of relevant national transpositions is provided in Annex 2.

In its Guidelines for common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing (EBA/GL/2022/03), the EBA provides that “competent authorities should assess whether the institution’s 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 information technology within a reasonable time and with reasonable costs when the environment or business requirements change (i.e. agility). This includes 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.

[17] 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).

Furthermore, 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/2017/12) 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 information technology 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 both for model development and the quantification of risk parameters, as well for data documentation and reporting and supporting IT infrastructure. The ECB guide to internal models[18] includes a granular overview of requirements from the CRR, Commission Delegated Regulations, and other supervisory work in this area, namely EBA draft regulatory technical standards, guidelines and Basel principles for the key areas of use for internal models. In particular, the ECB guide to internal models includes a section dedicated to the data maintenance for the internal ratings-based (IRB) approach, in accordance with Articles 144(d), 174(d) and 176 CRR.[19] With regard to internal validation requirements for the internal ratings-based approach, in 2022 the EBA held a consultation on the supervisory handbook for the validation of internal ratings-based systems that covers the governance and main responsibilities of the internal validation function as well as specific content on the assessment of the modelling environment, focusing on data quality and IT implementation.

[18] See "ECB guide to internal models", ECB, October 2019.

[19] In its current version, the ECB guide to internal models refers to the Final Draft Regulatory Technical Standards on the specification of the assessment methodology for competent authorities regarding compliance of an institution with the requirements to use the IRB Approach in accordance with Articles 144(2), 173(3) and 180(3)(b) of Regulation (EU) No 575/2013 (EBA/RTS/2016/03), which has now been published as Commission Delegated Regulation (EU) 2022/439 following amendments.

The ECB Guide to fit and proper assessments[20] 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.

From a macroprudential perspective, the European Systemic Risk Board (ESRB) has repeatedly highlighted the importance of receiving high-quality data to monitor and address financial stability risks. In the context of the reporting required by the European Market Infrastructure Regulation, the ESRB highlighted the difficulties that persistent data quality issues pose for the adequate monitoring of financial stability risks, made concrete proposals to improve supervisory reporting and called for increased supervisory attention to be paid to data quality.[21]

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 includes information on the quality of the prudential and financial data for supervisors

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

- Estonia: Articles 82, 82, 82-1 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 Code for Credit Institutions

- Greece: Article 66 (1-2) on robust governance arrangements, effective processes to identify, manage, monitor and report the risks, internal control mechanisms, remuneration policies and practices of the 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,

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

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

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 banch*); 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 the Bank of Lithuania No. 03-176 and 149
- Luxembourg: Paragraph 132, chapter II of Circular 12/552 of the Luxembourg Financial Sector Supervisory Commission on central administration, internal governance and risk management; paragraph 30 of Circular CSSF 11/506 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 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 (*Regime Geral das Instituições de Crédito e*

Sociedades Financeiras – RGICSF) of 31 December 1992, approved by Decree-Law 298/92; Notice of the Banco de Portugal No. 3/2020 (*Regulamenta os sistemas de governo e controlo interno e define os padrões mínimos em que deve assenter a cultura organizacional das entidades sujeitas à supervisão*); Circular the 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); Article 2, 4, 5, 6, 7, 11(2)(b), 12(2)(e), 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*); ; and 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).