EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Report on the Thematic Review on effective risk data aggregation and risk reporting

May 2018

Executive Summary

The ECB pays close attention to supervised entities' broad data quality, risk data aggregation and risk reporting capabilities, which are deemed essential preconditions for proper risk governance and sound risk-based decision-making and necessitate state-of-the-art IT infrastructure. Indeed, these represent key aspects of the ECB's periodic Supervisory Review and Evaluation Process (SREP) for significant institutions.

Sound and robust risk data aggregation capabilities and risk reporting practices have become even more important since the global financial crisis, which demonstrated that an institution's ability to manage risk-related data has a significant impact on its overall risk profile and the sustainability of its business model, especially when such entities face economic, financial, competitive and regulatory headwinds.

In 2016, the ECB launched, as one of its supervisory priorities, a "Thematic Review on effective risk data aggregation and risk reporting" (hereinafter "the Thematic Review"), seeking to carry out an in-depth assessment of credit institutions' overarching governance, data aggregation capabilities and reporting practices that are relevant for each institution as a whole, on the basis of a sample comprising 25 significant institutions. That assessment was guided by the Basel Committee on Banking Supervision's principles for effective risk data aggregation and risk reporting (hereinafter "the BCBS 239 principles").[1]

The outcome of the Thematic Review shows that the implementation status of the BCBS 239 principles within the sample of significant institutions is unsatisfactory, which is a source of concern.

Thus far, none of those significant institutions – some of which are classified as global systemically important banks – have fully implemented the BCBS 239 principles.[2] Weaknesses stem mainly from a lack of clarity regarding responsibility

1 See BCBS, "Principles for effective risk data aggregation and risk reporting", January 2013.

2 The deadline for global systemically important banks to meet these expectations should have been the beginning of 2016. Moreover, it is recommended that national supervisors also apply these principles to banks identified as domestic systemically important banks three years after designating them as such.

and accountability for data quality. It is often difficult to understand what the roles and responsibilities of business, control and IT functions are, and how those roles are allocated and exercised. Consequently, further efforts will be needed in this area in the coming years in order to enhance the effectiveness of risk data aggregation and risk reporting.

Against that background, this report seeks to convey the lessons learnt from the Thematic Review, describing the key areas of concern and providing examples of observed good practices, in order to encourage credit institutions to implement robust supervisory standards, in line with international best practices.

This report provides information about the methodology adopted by the Thematic Review and the findings observed, in order to raise awareness of the importance of strengthening governance arrangements around data aggregation and reporting capabilities, particularly as regards (i) increasing the involvement of relevant bodies/functions at different levels, (ii) the appropriate involvement of the various lines of defence and (iii) the formalisation of processes, roles and responsibilities.

If IT strategies relating to data and system architecture are comprehensive and sufficiently embedded in strategic decision-making processes, this will support the enhancement of such governance arrangements. Integrated operational processes for risk, adequate reporting, and the mitigation of risks stemming from pervasive manual processes (which in many cases are neither traced nor independently reviewed and approved) also represent good practices in this regard.

The general conclusions set out in this report are, of course, without prejudice to the ECB's assessment of the risk governance of individual credit institutions, which is conducted in the context of its ongoing supervisory work and takes account of the specificities of each entity in terms of the application of the relevant legal framework.

1 Introduction

One key lesson from the financial crisis was the need for more information on risk in order to make sound business decisions. IT, data architecture and related business processes were not sufficient to support the broad management of financial risks. Many credit institutions lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately at group level, across business lines and legal entities, as a result of inadequate risk information and weak risk data aggregation practices. As a result, those credit institutions' ability to take timely decisions was seriously impaired, with wide-ranging consequences for the credit institutions themselves and the financial sector as a whole.

In line with the European Banking Authority (EBA) guidelines on the SREP process,[3] as well as the BCBS 239 principles, the ECB focuses, in the context of the SREP process, on the assessment of three aspects that are key to ensuring sound risk management: (i) IT governance and risk infrastructure; (ii)data aggregation; and (iii)reporting.[4]

In late October 2015, the Supervisory Board of the ECB approved the launch of a Thematic Review, which was conducted in accordance with the supervisory examination programme adopted by the ECB's Supervisory Board and Governing Council on 6 January 2016[5] in line with Article 99 of the Capital Requirements Directive (CRD IV).[6]

Compliance with the BCBS's principles for effective risk data aggregation and risk reporting was also one of the supervisory priorities of the Single Supervisory Mechanism (SSM) for 2016 and 2017.[7]

The Thematic Review translated the BCBS 239 principles into an off-site supervisory tool by developing a set of checks that were used by all of the Joint Supervisory Teams (JSTs) conducting the assessment, thereby ensuring consistency across all of the 25 credit institutions that were subject to the review.

The assessment took stock of the risk data management frameworks adopted by those 25 significant institutions on the basis of: (i) institutions' descriptions of their risk data aggregation and risk reporting capabilities; (ii) institutions' evaluation of their own progress towards proper implementation of the BCBS principles; (iii) gap analysis conducted by those institutions for each principle; and (iv) action plans explaining how those gaps would be filled. This approach allowed JSTs to take account of specificities relating to operational complexity and group structure. Information on the budgets that were available in order to address gaps and weaknesses was also requested and considered.

To this end, that analysis followed a risk-based approach, assessing the data aggregation and reporting capabilities that were in place for individual

3 In particular, para. 106 of the EBA's Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) reads: "In line with the EBA Guidelines on internal governance, competent authorities should assess whether the institution has effective and reliable information and communication systems and whether these systems fully support risk data aggregation capabilities at normal times as well as during times of stress. In particular, competent authorities should assess whether the institution is at least able to: a. generate accurate and reliable risk data; b. capture and aggregate all material risk data across the institution; c. generate aggregate and up-to-date risk data in a timely manner; and d. generate aggregate risk data to meet a broad range of on-demand requests from the management body or competent authorities." (p. 53).

4 See SSM SREP Methodology Booklet (2016 edition).

5 Also on the basis of Article 4(1)(e) of Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63; hereinafter "the SSM Regulation"), under which the ECB ensures compliance with EU law (including national law transposing directives) which imposes requirements on credit institutions to have in place robust governance, including risk management processes.

6 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).

7 See ECB Banking Supervision: SSM supervisory priorities 2017.

processes/activities/business lines/subsidiaries in relation to market risk, credit risk, liquidity risk, counterparty credit risk, operational risk and interest rate risk in the banking book on the basis of their materiality. The aim was, in particular, to allow for a more targeted assessment commensurate with each credit institution's risk profile, as well as highlighting issues stemming from institutions' business models and geographical footprints.

Moreover, that assessment was complemented by two additional analyses: a "data lineage" exercise and a "fire drill" exercise for credit risk and liquidity risk respectively.

The data lineage analysis, which was applied to two selected data points, was aimed at assessing credit institutions' ability to manage the data life cycle, from the original data source through the process and application chain, taking account of the controls applied. This helped to clarify the risk data management process, contributing to the identification of the root causes of data quality issues across operating units (business lines, legal entities, functional areas, etc.).

The aim of the fire drill exercise was to assess credit institutions' ability to aggregate and report a number of selected data points in an accurate, comprehensive and timely manner under time pressure. Each credit institution's independent internal audit department (or internal validation unit) was asked to carry out an independent validation report on the "agreed upon procedures"[8] required by operating guidelines with the aim of assessing the quality of the data reported by the relevant credit institution.

That credit institution-specific analysis was followed by extensive benchmarking – both quantitative and qualitative – from which good practices and a set of main gaps were derived.

The main outcomes of the Thematic Review have fed into the assessment of data aggregation and reporting capabilities as part of the SREP process and have already been communicated to individual credit institutions in the context of individual supervisory dialogues.

At the end of the Thematic Review, JSTs informed credit institutions of the main findings via follow-up letters, which will be followed up on the basis of credit institutions' action plans.

This report, which identifies the main gaps and good practices for each BCBS principle, comprises three main sections. The first section covers the first two overarching principles, which are concerned with governance (Principle 1) and data architecture and IT infrastructure (Principle 2); the second section covers principles relating to risk data aggregation capabilities; and the third covers principles relating to risk reporting practices. The last part of the document sets out overall conclusions, as well as detailing the next steps planned by the ECB in order to further strengthen its approach to risk data aggregation capabilities and risk reporting practices.

8 As per International Standard on Related Services (ISRS) 4400.

2 Governance and IT infrastructure

In line with the BCBS, the ECB stresses that the principles relating to governance and data architecture and IT infrastructure are foundational and constitute overarching standards.

The involvement of a credit institution's board (for guidance, oversight and the approval of policies) and its executive and senior management (for implementation and monitoring)[9] in risk data aggregation and the risk reporting framework is, together with sound risk data architecture and appropriate IT infrastructure, a key precondition for ensuring compliance with other principles.

Clear roles, incentive schemes and responsibilities are of key importance in the area of risk data management. It is crucial in this regard that integrated IT platforms are put in place, covering all material risk types and all material subsidiaries and building on unique ("golden") sources of information. It is also important that data architecture supports audit trails and the implementation of controls.

BCBS Principle 1: Governance

"A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other principles and guidance established by the Basel Committee."[10]

In this respect, the Thematic Review assessed the existence and structure of (i) data governance frameworks (including the question of whether credit institutions had a BCBS 239 steering committee), (ii) risk-related IT strategies, and (iii) internal audit and/or formal independent validation frameworks, as well as (iv) the involvement of all governing bodies in ensuring and monitoring the implementation of risk data aggregation and risk reporting.

The following key areas of concern were identified:

i. As regards data governance frameworks, weaknesses stem mainly from a lack of clear roles and responsibilities in the area of data quality, as well as a lack of ownership of data quality for business, control and IT functions. In addition, clear data governance structures are not embedded in institutions' organisational charts.

ii. Not all material legal entities are included in BCBS 239 implementation projects.

[9] References to a credit institution's board should be understood as referring to the management body in its supervisory function (see Article 3(8) of CRD IV), and references to executive and senior management should be understood as referring to the management body in its executive function (see Article 3(9) of CRD IV).

[10] Such as the BCBS's Principles for enhancing corporate governance (October 2010) and Enhancements to the Basel II framework (July 2009).

iii. Large-scale IT projects or strategies designed to implement the BCBS principles are defined incompletely. Project schedules are not sufficiently clear with regard to the finalisation of necessary improvements. The scope of the project is not always clearly defined, resulting in a non-existent or inadequate roadmap for its implementation.

iv. Internal validation units assessing bank's data aggregation capabilities and reporting practices are not always independent and adequately staffed, with insufficient involvement of and distinction between the various lines of defence.

v. Ultimately, there is a lack of strategic attention at executive and senior management level, resulting in insufficient support for and visibility of risk data aggregation projects, leading to unclear budgetary processes, ineffective leadership and/or weak project management practices.

Against this background, the ECB observed the following best practices, which can help to strengthen governance arrangements in the area of risk data aggregation and risk reporting:

- Effective data governance frameworks set out both internal and external requirements in the area of data quality, covering all of the relevant data production cycles for data used in the overall management of credit institutions – from data origination, generation and system entry to final reporting[11]. They also determined the necessary structures, organisational units and committees, pointing to the relevant roles and responsibilities within those units. They also contained guidelines on communication, reporting and decision-making processes for group entities.

- Those data governance frameworks included the following:

    - As part of the second line of defence, a data governance office responsible for: (i) issuing policy and guidelines; (ii) overseeing proper implementation of the data quality framework throughout the organisation; (iii) classifying key risk data; (iv) evaluating and monitoring data quality through data quality processes; and (v) participating in relevant change management processes such as the merging or acquisition of legal entities or the launch of new products.

    - As part of the first line of defence, a network of local data owners responsible for each material legal entity and business line who participate in the definition of data control procedures and are responsible for ensuring the confidentiality, accuracy, integrity and timeliness of data. There was also centralised identification of data owners/process-owning managers reporting directly to the CEO and operating in addition to the controls guaranteed by line structures. Their mandate included the

[11] This approach is in line with that adopted by the BCBS, which regards credit institutions' application of the BCBS 239 principles to regulatory and financial reporting as an example of effective governance (see BCBS, "Progress in adopting the Principles for effective risk data aggregation and risk reporting", March 2017, Appendix 2, section 1.1, p.15).

adoption of policies, the monitoring of implementation of the data quality framework, the classification of key risk data, the development of data quality controls, and the monitoring and reporting of data quality processes, with a clear division of responsibilities between data owners and IT staff. Data quality reporting processes were implemented across the whole of the banking group, with specific training plans and incentive policies put in place. Proper change management processes ensured that data quality requirements were met, both as regards risk and for other managerial purposes.

- Steering committees were responsible for monitoring implementation of the BCBS principles at group level, helping to ensure full compliance and group-wide consistency and awareness at every level of the organisation.

- Well-structured and coherent IT strategies sought to improve risk data aggregation and risk reporting capabilities and demonstrated that institutions were able to remedy any shortcomings without delay. Underlying IT systems and processes were also incorporated in credit institutions' business continuity plans. Internal audit and/or formal independent validation frameworks were put in place, as were subsequent regular assessments of data aggregation and risk reporting for all risk categories, including potential oversight of outsourced activities. Periodic reviews and monitoring were carried out for projects.

- Institutions' boards were responsible for guidance, oversight and the approval of policies; executive and senior management were focused on and closely involved in the implementation and monitoring of the risk data aggregation and risk reporting framework; IT departments were heavily involved in the implementation of the BCBS principles; and risk personnel were given the tools, powers and resources to execute projects in accordance with the implementation roadmap. In order to ensure consistency between all of these bodies, some credit institutions had business areas, departments, policies and procedures spanning the entire organisation with regard to risk data compilation, aggregation and reporting, covering all material entities and risk types.

- Data quality repositories[12] were established at group level, helping to provide a consolidated overview.

- Some credit institutions had a specific annual operational budget dedicated to the implementation of the BCBS 239 principles in order to check that budgetary requirements were properly addressed, with detailed plans aimed at achieving complete compliance being submitted to executive and senior management and the board for approval.

- Credit institutions' boards and executive and senior management were aware of the limitations of the reports submitted to them in terms of coverage, legal and

[12] These data quality repositories contained policies, guidelines, operational procedures and organisational charts relating to data governance, both at holding level and at subsidiary level.

technical constraints in the data aggregation process, and/or shortcomings in the reporting process.

BCBS Principle 2: Data architecture and IT infrastructure

"A bank should design, build and maintain data architecture and IT infrastructure which fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times but also during times of stress or crisis, while still meeting the other Principles."

As in the case of Principle 1, adequate IT infrastructure is a fundamental prerequisite for effective risk data aggregation capabilities and risk reporting practices.

In this respect, the Thematic Review assessed the existence and structure of (i) data architecture frameworks, (ii) data taxonomy, (iii) dependence on manual processes and the level of automation within the data compilation process, (iv) consistency and data quality checks, (v) escalation processes, (vi) business continuity and (vii) drill-down capabilities.

The Thematic Review identified the following areas of concern in this respect:

i. As regards data governance architecture frameworks, there was a lack of integrated solutions in the data aggregation and report compilation processes.

ii. In many cases, institutions did not have a homogeneous and integrated data taxonomy covering all material legal entities and risk types.

iii. Manual processes were not fully identified, properly documented and independently reviewed, and the level of automation remained unsatisfactory even for key and complex tasks.

iv. Many consistency checks were incomplete and carried out manually.

v. In many cases, there was no clear escalation process in place to rectify errors detected by consistency checks.

vi. IT systems and business processes were not always properly included in business continuity arrangements.

vii. Some credit institutions had limited drill-drown capabilities, with IT risk platforms unable to manage information for individual customers at transaction level.

Overall, the ECB noted that silo-based IT architecture for different reporting purposes had led to a lack of integrated solutions and hampered compilation processes, increasing inefficiencies during reconciliation procedures. Supervisory assessments – both on and off-site – clearly confirmed the potential for this to lead to: (a) duplication and redundancies in terms of IT infrastructure and organisational arrangements; (b) a need for complex, time-consuming and expensive reconciliation processes; and (c) an increase in the probability of errors in life cycle data management processes.

Against this background, the ECB observed the following best practices, which can help to strengthen data architecture and IT infrastructure:

- Credit institutions established and used common data sources for the production of risk, accounting and regulatory reporting, as well as homogeneous and integrated data taxonomies covering all material legal entities and risk types and integrated IT risk platforms based on transaction-level granularity. In a few cases, this was implemented by establishing an overarching data governance framework responsible for all kinds of reporting (as well as other operational processes) to reduce the burden of time-consuming reconciliation phases. Credit institutions also demonstrated the availability of audit trails and showed that the implementation of controls was supported by data architecture. Some data compilation processes were fully automated, and where this was not feasible, documentation on manual processes was complete and easily accessible. Manual interventions – including supporting end-user computing (EUC) tools – were traced and ranked by complexity and relevance. Modifications made to relevant information were subject to independent validation and/or approval. To this end, IT systems facilitated the implementation of consistency checks, with EUC tools designed to support the application of access controls, the segregation of duties, and the separation of testing and production.

- Credit institutions carried out automated consistency checks, from front office systems to the reporting layer, as well as reconciliation with other sources (i.e. accounting, finance, etc.). These checks had a dual objective, assessing the effectiveness of (a) controls implemented along the data life cycle, starting with the front office application of each legal entity in the group, and (b) reconciliation processes between risk data and other credit institution data (i.e. accounting). Data quality indicators (including tolerance levels), detailed procedures, work instructions (key operating procedures) and a documented operational procedure in case of breaches will all help this process, with the quality of the related data being constantly monitored using a dashboard. The EBA's validation rules represent effective minimum guidance for credit institutions when checking the accuracy of reporting data prior to submission to the competent authority. Furthermore, some credit institutions cross-checked internal and external reporting files on a regular basis, covering all existing data quality checks, with data quality being closely monitored.

- There was a constant search for data quality improvements, with data quality improvement processes involving all material business areas across credit institutions.

- All types of control were documented (especially for partially automated and manual processes), as were the functions responsible for such controls, including staff incentives at all levels of the banking group (headquarters, branches, subsidiaries, etc.). Responsibility for making sure that controls were properly documented was explicitly assigned to a specific person or function. That individual was able to identify the stage of the process at which the controls were carried out and explain what the results of those controls were,

how errors were identified, reported and corrected, how those figures were reconciled with other sources, and whether the data were unambiguously defined in a data dictionary.

- Clear escalation processes were in place at holding level, as well as at the level of each material legal entity, in order to rectify errors identified by consistency checks. Risk management was strengthened after serious operational incidents. Contingency plans were designed in line with the outcomes of business impact analysis. Recovery measures made sure that there was an adequate flow of risk information to the board, executive and senior management, control functions and the relevant business unit itself. Both at the level of the material legal entity and at holding level, efforts were made to provide information with the highest level of granularity (e.g. transaction data). This allowed credit institutions to respond quickly and with limited adaptation costs to future risk management requirements, as well as allowing them to deal with any ad hoc needs during crisis situations or periods of financial stress. Furthermore, the same set of information acted as the main – or, better still, the sole – data source for accounting and regulatory reporting, which simplified risk/finance/supervision reconciliation processes. This also allowed reconciliation to be achieved by design.

Overall, the ECB observed that IT infrastructure for risk data aggregation and risk reporting sought to provide transaction-level granularity and facilitate periodic reconciliation between risk data and other credit institution data. In this respect, the use of Legal Entity Identifier codes to help aggregate exposures to counterparties would also represent a good practice.

3 Risk data aggregation capabilities

It is important that data quality standards, certification policies, and escalation processes and procedures are comprehensive, consistent and embedded in well-designed controls in order to properly manage risks and ensure that all material risks, legal entities and business lines are taken into consideration.

It is also important that procedures for aggregating data are flexible enough to allow for higher reporting frequencies in stress/crisis situations which entail exceptional requirements.

Fully automated processes requiring no manual intervention will strengthen credit institutions' ability to produce aggregated data on an ad hoc basis for internal risk management purposes and in response to external requests.

BCBS Principle 3: Accuracy and integrity

"A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors."

In this respect, the Thematic Review assessed the existence and structure of (i) data quality policies and control procedures for both internal and external data, (ii) key quality indicators (KQIs) for both internal and external data, (iii) rules used to transform granular data into meaningful aggregates, (iv) reconciliation between risk data and "golden" sources, and (v) audit trails from the origin of the data (i.e. from the "golden" source) to risk reports.

The Thematic Review identified the following areas of concern in this respect:

i. Data quality policies were not always complete and formally approved by the relevant governance bodies, with control procedures not implemented on a regular basis.

ii. KQIs did not cover all relevant metrics or were incomplete in various respects (KQIs not well defined for some risk categories and trigger levels, frequency of monitoring not clearly specified, tolerance thresholds not consistent or vaguely defined, etc.). In some cases, tolerance thresholds were set arbitrarily, and control outcomes below those thresholds had the potential to impede sound decision-making. In other cases, there were no breach/escalation processes in place in case of KQI breaches.

iii. In some cases, changes to data (changes to definitions, manual adjustment of data, etc.) were neither well documented nor traceable. Consolidating entities sometimes had a limited overview of the implementation status and the effectiveness of data quality mechanisms in place in major entities.

iv. Some institutions did not have reconciliation procedures, or those procedures were applied in an ad hoc manner (not always including major business lines, risk categories, entities, portfolios, etc.).

v. Audit trails were not available for all risk areas, with the result that some data functionalities were neither described nor traceable for internal audit departments (e.g. in order to perform ex post analysis of manual modifications made to risk data).

Against this background, the ECB observed the following best practices, which can help to strengthen the accuracy and integrity of data:

- Group-wide data quality standards and policies were reviewed on a regular basis, increasing their effectiveness. Control procedures – which were properly executed and periodically assessed – were applied consistently, for both internal and external data. Those standards covered all material risk categories and were approved by all major entities in accordance with the relevant policy implementation processes – i.e. with a complete certification process in respect of major entities, business lines, portfolios and products. All of those standards had to be formally approved by all relevant governance bodies. Delays in the certification process were followed up and reported centrally to ensure a timely follow-up. The certification process was based on data quality metrics with well-calibrated tolerance levels. Those tolerance levels were set in such a way that

control outcomes below those thresholds did not compromise the interpretability of the metrics and allowed for sound decision-making.

- Roles and responsibilities in respect of the certification process were clearly defined and were a formal part of the relevant individuals' job descriptions.
- KQIs were in place for both internal and external data, with escalation processes in case KQIs were breached.
- Data quality certification processes were in place for "golden" sources – the authoritative sources of risk data for each type of risk – and re-run when major changes were made (system overhauls, migrations, etc.). The rules of those processes were consistent with the relevant group-wide data taxonomy. The identification of critical data points across the group was subject to in-depth production auditing and mapping (source, control process, remediation plan, etc.). To make the process work, credit institutions recertified those critical data points on an ongoing continuous basis.
- When changes were made to data, the rationale for those changes was clearly logged, together with details of the people responsible (i.e. who requested the changes, who made them and who approved them).
- Reconciliation was carefully conceptualised. Critical data elements were identified and linked to key metrics, with reconciliation procedures sufficiently formalised in operational guidelines. The results of reconciliation exercises were regularly analysed by business areas and internal audit departments alike, with discrepancies followed up and analysed to assess their root causes. Remediation actions were then initiated, with proper escalation processes in place to rectify errors detected by consistency checks. In order to fully implement these good practices, proper reconciliation procedures were put in place, encompassing all major business lines, risk categories, product types and entities, with few exceptions, and relevant remediation plans were established where necessary.

BCBS Principle 4: Completeness

"A bank should be able capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings, as relevant for the risk in question, that permit identifying and reporting risk exposures, concentrations and emerging risks."

In this respect, the Thematic Review assessed the existence and structure of (i) credit institutions' capacity to cover all material risk types across legal entities and/or business lines and (ii) the application of materiality thresholds.

The Thematic Review identified the following areas of concern in this respect:

i. Credit institutions' ability to capture and aggregate data and implementation risks relating to change projects was regarded as a concern, with institutions demonstrating insufficient ability to capture and aggregate all material risk types across legal entities and/or business lines. Weaknesses were often observed in relation to this principle when credit institutions implemented major change projects, especially when those projects over-ran significantly. This gave rise to increases in implementation risk, partly as a result of processes still being dependent on manual aggregation to some extent.

ii. Some of the criteria used for excluding specific legal entities and/or assets from particular risk categories were unclear. In the case of some credit institutions, foreign legal entities' data had yet to be included in a dedicated central repository, or improvements to measurement processes and underlying thresholds had not yet been fully reviewed.

Against this background, the ECB observed the following best practices, which can help to strengthen the completeness of data:

- Institutions included and analysed business units, subsidiaries and off-balance-sheet entities (e.g. special-purpose vehicles) in their annual group risk inventories, for instance by working on introducing a group-wide unique customer key that facilitates the identification of counterparty credit risk exposure to single counterparties across the credit institution in order to be able to identify the counterparty credit risk exposure to a single counterparty at smaller subsidiaries.
- Risk-relevant branches and subsidiaries were included in internal reporting, with the annual risk inventory process determining all relevant branches and subsidiaries within the group. Off-balance-sheet exposures were also included, allowing the institution to fully aggregate all exposures to counterparties on the basis of current data granularity. All exceptions were documented and approved by the board.

BCBS Principle 5: Timeliness

"A bank should be able to generate aggregate and up-to-date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptablility. The precise timing will depend upon the nature and potential volatitlity of the risk being measured as well as its criticality to the overall risk profile of the bank. The precise timing will also depend on the bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, set based on the characteristics and overall risk profile of the bank."

In this respect, the Thematic Review assessed credit institutions' ability to (i) aggregate information in a timely manner in accordance with requirements stipulated by business areas, management, control functions, the board and supervisors, and (ii) aggregate risk data more frequently for risk reporting during periods of stress or

crisis (i.e. indicators of credit risk exposure to large borrowers, counterparty credit risk, trading exposures, liquidity risk, time-critical operation risk, etc.).

The Thematic Review identified the following areas of concern in this respect:

Owing to the considerable complexity of IT systems and the fragmented information and communication technology landscape at many of the credit institutions in the sample, reporting processes were frequently delayed and often labour-intensive. Processes were overly reliant on manual or semi-manual processing and multiple data sources, increasing the risk of further delays.

As a consequence, some institutions were not fully able to generate aggregated and up-to-date risk data in a timely manner and comply with the principles relating to accuracy, integrity, completeness and adaptability at the same time.

In a few cases, critical timeliness issues were observed for risk types such as credit risk and interest rate risk in the banking book, whereby the timeliness reported for these risk reports (expressed as the number of days after the reference period) was around 60 days in normal situations and around 30 days even in stress test situations.

The fire drill exercise revealed a number of other issues. Not all institutions were able to submit the data requested at group level within a short period of time. Moreover, in the area of liquidity, not all subsidiaries were capable of producing figures by the requested deadline for the predefined reference dates/time frames. In a number of cases, credit institutions were also unable to demonstrate their ability to aggregate data more frequently during periods of stress, in the absence of specific procedures for that purpose.

When credit institutions are requested to provide ad hoc data/information to the regulator, timeliness and correctness are persistent problems. It is important that credit institutions define specific frequency requirements, both for stress/crisis situations and for the aggregation of up-to-date data in normal situations.

Some credit institutions' current systems do not support the accelerated production of key risk metrics and risk reports in times of stress/crisis. It is important, therefore, that those institutions adopt dedicated protocols – one for each risk metric or risk report – in order to establish production processes in case of stress/crisis.

Against this background, the ECB observed the following best practices, which can help to improve the timeliness with which aggregated and up-to-date risk data are generated:

- Some more advanced credit institutions have identified a specific set of metrics to be generated during periods of stress, with those metrics being reviewed and approved by the internal audit function. Those metrics, which are normally required on a monthly basis, are generated on a weekly or daily basis during such periods.

BCBS Principle 6: Adaptability

"A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad-hoc risk management reporting requests, including requests during stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries."

In this respect, the Thematic Review assessed credit institutions' ability to (i) produce aggregated data to meet users' needs and (ii) drill down as required (including on the basis of ad hoc requests).

The Thematic Review identified the following areas of concern in this respect:

Credit institutions demonstrated a limited ability to deploy local risk data obtained from subsidiaries, branches and business lines.

Decentralised databases resulted in a limited ability to deploy local risk data obtained from subsidiaries. The granular data that need to be used for aggregation were not sufficiently accurate and/or complete to allow flexible reporting in the requested time frame.

Moreover, there was an overreliance on unstructured data sources, including huge amounts of data stored on printed paper sheets, in scanned and/or digitised documents and in other unstructured electronic documents (PDFs, Word files, Excel notes, etc.).

Against this background, the ECB observed the following best practices, which can help to strengthen the adaptability of risk data:

- Data customisation capabilities allowed for amendments to aggregation criteria, and it was easy to adapt data aggregation policies, procedures and processes in line with changes to the internal and external environment.
- Changes to the organisation of the business and external factors influencing credit institutions' risk profile were taken into account, as were changes to the regulatory framework.
- Data aggregation processes were flexible, so as to (i) allow the delivery of risk data with differing levels of granularity, (ii) enable risk data to be aggregated for assessment and quick decision-making, (iii) enable data to be customised in line with users' needs (e.g. using a risk dashboard) and (iv) drill down as needed

4 Risk reporting practices

Strong data customisation capabilities will allow changes to aggregation criteria and facilitate the delivery of risk data with differing levels of granularity, such that data aggregation policies, procedures and processes can easily be adapted in line with changes to the internal and external environment.

To this end, it is important that risk reports also include forward-looking information on adverse scenarios. Moreover, a group-wide internal data dictionary also represents a good practice in this regard.

It is therefore important that the frequency of risk reporting is sufficient to allow timely decision-making, with reports being sent to all recipients by means of a secure automated distribution channel.

Having an effective feedback process is also of key importance.

BCBS Principle 7: Accuracy

"Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated."

In this respect, the Thematic Review assessed whether (i) credit institutions have automated and manual checks in place, including an inventory of the validation rules applied to information included in risk reports, and (ii) credit institutions have established accurate and precise requirements for both regular and stress/crisis reporting through policies governing the degree of approximation and designating critical position and exposure information.

The Thematic Review identified the following areas of concern in this respect:

Plausibility and consistency checks were insufficient. On the whole, there was no proof of the accuracy or traceability of data, with insufficient validation checks and controls.

The absence of the necessary audit trails was also problematic, since key data concerns regarding lineage and selection could not always easily be traced back to the root cause owing to manual processes. By the same token, the quality and consistency of metric-level commentaries was also a matter of concern, owing to a lack of automated compilation processes and dedicated policies/requirements.

Moreover, in some cases, there was an absence of proper reporting on key data concerns in high-level risk reports for senior management (with concerns being expressed in the form of footnotes and commentary).

Many reconciliation errors were noted in the area of regulatory capital, owing to extensive manual intervention in order to transfer data between systems and verify, correct, complete and convert information. In addition, extensive use was made of Excel and other end-user programming, which makes this process rather complex and error-prone. This casts doubts on the appropriateness of data for risk management and steering purposes, the existence of effective controls and the quality of the reconciliation of risk and finance data.

Rejected data were not well managed. Risk reports suffered from inconsistencies and lacked metrics on data quality and harmonised procedures for the management of rejected data.

On the whole, credit institutions lacked dedicated policies establishing requirements or expectations as regards the accuracy and precision of approximations used for regular and crisis reporting. Some credit institutions had no policies governing the degree of approximation and designating critical position and exposure information.

Some credit institutions are not able to gather accurate and complete information in order to activate proper and timely corrective actions. This, in turn, adversely affects the overall quality of the reporting. This is due to gaps in control and monitoring processes and happens when first-level controls are not automated, control functions have not established common platforms and the process of feeding group customer databases needs to be improved.

Generally, the level of effectiveness of control processes carried out centrally at entity level is poor.

Against this background, the ECB observed the following best practices, which can help to strengthen the accuracy of data:

- Credit institutions established a proper, clear set of documentation on data quality requirements and a comprehensive list of data accuracy checks covering all material business lines, including plausibility checks and mathematical checks.
- Credit institutions' decision-making bodies provided detailed indications of (i) their data accuracy requirements for risk reporting and (ii) their expectations regarding approximations for regular and stress/crisis reporting.
- A combination of well-implemented data quality dashboards, ongoing maintenance of credit institutions' data quality frameworks and permanent monitoring of institutions' BCBS 239 implementation programmes provided effective support in this regard.
- A few credit institutions had harmonised procedures for the management of rejected data. Those credit institutions' internal audit functions regularly validated their risk data aggregation and risk reporting processes within an integrated data quality framework which involved both first and second lines of defence.
- The ability to trace data lineage and key data concerns back to the original supporting key risk metrics allowed credit institutions' executive and senior management to be given clear and manageable high-level risk reports.
- Reconciliation with other types of data is key, and credit institutions had effective procedures governing the reconciliation of accounting and risk data where figures on risk-weighted assets were calculated on the basis of accounting data. Credit institutions demonstrated that IT reconciliation tools

were available to the main entities in the group and that risk data could be delivered for the Internal Capital Adequacy Assessment Process, allowing for easy reconciliation between regulatory capital and economic capital figures.

BCBS Principle 8: Comprehensiveness

"Risk management reports should cover all material risk areas within the organisation.The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients."

In this respect, the Thematic Review looked at whether risk management reports (i) included exposure and position information for all significant risk areas and all significant components of those risk areas, (ii) identified emerging concentrations of risk and provided information in the context of limits and risk appetite/tolerance, (iii) allowed the monitoring of emerging trends through forward-looking forecasts and stress tests, (iv) contained forecasts or scenarios for key market variables and set out the impact on the credit institution so as to inform the board and executive and senior management regarding the likely future trajectory of the credit institution's capital and risk profile.

The Thematic Review identified the following areas of concern in this respect:

Not all material risk areas are covered by risk reporting, with the forward-looking aspect providing cause for concern in every single risk area. In this regard, credit institutions have difficulties incorporating forward-looking aspects of risk reporting (including stress testing and scenario analysis), which leads to issues with the monitoring of emerging trends if those aspects are not properly integrated into the credit institution's internal reporting. It is also important that emerging risks are properly defined. These risks are sometimes assessed and reported on an ad hoc basis, rather than on the basis of a regular, well-documented procedure. Sometimes, not all relevant risk parameters are highlighted. Credit institutions also have difficulties including forward-looking aspects in their risk appetite metrics/limits (e.g. when it comes to integrating the results of stress testing and scenario analysis into metrics/limits). It is important that credit institutions integrate these aspects into all relevant processes (i.e. capital planning, recovery plans and stress testing).

Credit institutions also have difficulty breaking risk data down into different risk categories and sub-categories (e.g. general credit risk and counterparty credit risk).

Sometimes, only a limited set of key risk metrics is in place, and this does not cover all aspects of a risk category or all levels of application and does not provide sufficient detail.

Against this background, the ECB observed the following best practices, which can help to strengthen the comprehensiveness of data:

- Relevant risk areas were covered by sufficiently detailed risk reporting, with risk reporting procedures ensuring full coverage (both geographically and in terms of the type of risk) and reporting policies establishing a minimum level of coverage at holding and legal entity/geographical level by type of risk.
- Risk reporting policies also specifically stipulated that reports should identify emerging risks, as well as concentrations and any other potential deviations from established limits, benchmarks, etc.
- Risk reports included an economic forecast for the next two years for the main geographical areas, including relevant macroeconomic metrics and interest rate curves for the main countries. These covered both baseline and adverse scenarios.

BCBS Principle 9: Clarity and usefulness

"Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand, yet comprehensive enough to facilitate informed decision-making. Reports should include meaningful information tailored to the needs of the recipients."

In this respect, the Thematic Review looked at whether risk reports were meaningful, tailored to the needs of recipients (particularly the board and executive and senior management), and clear, concise and easy to understand, and whether they included qualitative interpretation.

The Thematic Review identified the following areas of concern in this respect:

Overall, there was a lack of formalised risk reporting policies.

Weaknesses related mainly to the quality of the feedback provided by boards and executive and senior management, whereby governing bodies generally lacked a formal way of expressing their views regarding the clarity and usefulness of risk reporting and were unaware of the limitations of the reports they received.

Comments included in reports were considered too concise to provide a good understanding of the situation, and gaps were frequently observed in specific areas. Some of the information provided was considered insufficient owing to long production times and insufficient frequency.

Moreover, difficulties explaining calculations and assumptions led to errors and misinterpretations, while the absence of group-wide definitions for some items created discrepancies in reporting across groups.

Credit institutions also lacked the ability to tailor information to different audiences, with some reports considered too technical, too complex or too detailed to be fully operational.

The use of satisfaction surveys in order to meet these expectations represents a good practice. This involves a validation group evaluating the need to adapt risk

reporting in order to address highlighted weaknesses, as well as the preparation of ad hoc presentations to executive and senior management in conjunction with the risk reports delivered. It is important that risk reports contain a useful summary of the risks taken by the entity, as well as qualitative considerations.

Against this background, the ECB observed the following best practices, which can help to strengthen the clarity and usefulness of data:

- Credit institutions had in place group-wide internal data dictionaries, glossaries and explanatory notes covering the metrics used in reports, together with detailed internal regulations stipulating the format of the documentation to be sent to governing bodies.
- Detailed initial reporting requirements were established by governing bodies.

BCBS Principle 10: Frequency

"The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed, at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis."

In this respect, the Thematic Review looked at whether all relevant and critical risk position/exposure reports were available with greater frequency and better timeliness in times of stress/crisis, allowing management to react better to evolving risks.

The Thematic Review identified the following key areas of concern in this respect:

Generally, frequency requirements and standards were insufficient. For many credit institutions, this resulted in a lack of specific policies governing the frequency of report production for all material risks in times of stress, leading to difficulties when trying to increase frequency in stress situations.

In some instances, the frequency of risk reporting was not sufficient for some risk types. In a few cases, critical frequency issues were identified for risk types such as credit risk and interest rate risk in the banking book, whereby the lowest frequency reported was around 90 days, even during stress test situations.

Against this background, the ECB observed the following best practices, which can help credit institutions to produce and distribute risk management reports more frequently:

- Appropriate frequency requirements were put in place for all material risks, both in normal times and in times of stress, with frequency increasing in stress situations for all risk types.

- Credit institutions endeavoured to be able to take most decisions within 24 hours in times of stress, with impact assessments being carried out within the same time frame wherever possible.

BCBS Principle 11: Distribution

"Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained."

In this respect, the Thematic Review looked at whether credit institutions had procedures in place that would allow the rapid collection and analysis of risk data and the timely dissemination of reports, balanced with the need to ensure confidentiality where appropriate (i.e. with reports delivered to the correct recipients using secure channels).

The Thematic Review identified the following areas of concern in this respect:

Intended recipients and confidentiality levels were sometimes not documented. The implementation of clear confidentiality and distribution policies was still a work in progress in some cases. Similarly, the automation of the distribution process needed to be improved in some instances.

Against this background, the ECB observed the following best practices, which can help to enhance the distribution of risk management reports:

- Recipients of all reports were formally defined, ensuring that distribution was automated and secure.
- Credit institutions had a detailed policy on a need-to-know basis for each individual report. The certification and distribution process was fully automated, with a clear list of recipients drawn up centrally by a secretariat to ensure timely transmission and confidentiality. Board members could, for example, have exclusive access to reports via an IT platform managed by the board's secretary – protected, for instance, by a two-level access key requiring not only a personal password, but also a six-digit one-time code generated by a device issued to them.

5 Supervisory conclusions and the way forward

The development of adequate risk data aggregation and risk reporting capabilities in order to ensure sound risk management is the responsibility of credit institutions themselves.

The assessment conducted by the ECB shows that credit institutions' implementation of the BCBS 239 principles remains unsatisfactory and that the overall level of progress is a source of concern for all of the credit institutions in the sample.

Full implementation of the BCBS principles will probably not be achieved any time soon, as several credit institutions' implementation schedules are set to run until the end of 2019 or beyond.

Ensuring full implementation of these principles is an ongoing process, and further efforts will be needed. Thus, it is important that credit institutions deal with changes to their business models and risk profiles in a proper manner, as well as periodically assessing the adequacy of their risk data aggregation and risk reporting capabilities.

This Thematic Review has allowed the ECB to identify follow-up supervisory actions, as well as issues to be addressed in the context of forthcoming on-site inspections, aspects to focus on as part of the SREP process and issues to be included in the subsequent supervisory examination programme required by Article 99 of CRD IV.

Although the banking industry is already working towards integrated solutions (a single organisational set-up for group-wide data governance, a single authoritative source for risk, managerial and regulatory purposes, reconciliation by design, etc.), it is important that all of the institutions in this sample continue remedying the weaknesses that have been identified on the basis of the deadlines agreed with the JSTs. JSTs will monitor and follow up on these issues.[13]

Overall, while this report reflects the lessons that have been learnt from the 25 institutions that were assessed in this Thematic Review, many of these lessons will also apply to other significant institutions. With this in mind, the ECB will continue to encourage all significant institutions to implement data aggregation and reporting principles, taking into account their size, business models and complexity (in line with the principle of proportionality).

In this regard, the BCBS encourages competent authorities to assess whether institutions identified as domestic systemically important banks properly implement these principles within three years of being designated as such, recommending that credit institutions start the implementation process early, given that global systemically important banks generally take around five to six years to achieve full compliance with these principles.

The ECB will continue working to promote good practices in this regard, as well as playing an active role in the implementation of international standards at EU and global level.

[13] In the context of its monitoring of improvements to institutions' risk data aggregation and risk reporting capabilities, the ECB takes the opportunity to keep the BCBS's Risk Data Network regularly informed and updated.

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