DATA GOVERNANCE & MANAGEMENT PRACTICES

- OBSERVATIONS AND SUPERVISORY EXPECTATIONS FROM THEMATIC INSPECTIONS

INFORMATION PAPER

May 2024

Monetary Authority of Singapore

TABLE OF CONTENTS

1 Introduction

1.1 Financial services is a data-driven industry. Data is used extensively for decision-making in various areas such as fraud surveillance, anti-money laundering, liquidity management, underwriting and investment management. With the exponential growth of data availability and advancement in data analytics capabilities, more advanced approaches to leveraging data have been deployed with a view to increase operational efficiency and risk management effectiveness.

1.2 As financial institutions step up their use of data, the need for robust data governance must not be overlooked. Boards and senior management need to ensure that the data they rely on for decision-making is accurate, consistent and complete. They also need to put in place controls to mitigate the risk of privacy and confidentiality breaches, as well as the risk of data being misused.

1.3 This information paper focuses on data governance practices that address data quality risk. It includes a set of supervisory expectations to guide banks and finance companies in their efforts to strengthen their data management capabilities. The expectations are based on requirements set by the Basel Committee on Banking Supervision on "Principles for effective risk data aggregation and risk reporting" (BCBS 239[1]), as well as observations from thematic inspections on data governance and management of Domestic Systemically Important Banks (D-SIBs), conducted by the Monetary Authority of Singapore (MAS) in 2022/23. The inspections focused on:

(a) Board and senior management oversight on data management;

(b) Data management organisation and policy framework;

(c) Data quality and issues identification and escalation; and

(d) Independent validation.

1.4 MAS observed that the banks reviewed generally had established policies and controls to oversee data management, with some areas for improvements. MAS recognises that banks and other financial institutions are at different maturity levels in terms of data governance and management. Nonetheless, MAS expects banks and finance companies to put in place a data governance framework that sets out fundamental data controls pertaining to the management of data, including their risk data aggregation and

[1] The BCBS 239 principles apply to Global Systemically Important Banks and national supervisors are strongly encouraged by the Basel Committee to apply the principles to banks identified as D-SIBs, three years after their designation as D-SIBs. In Singapore, the D-SIBs which comprise the 3 local banks and 4 other foreign banks, are required to comply with the BCBS 239 principles.

risk reporting capabilities. While not the focus of this thematic, it should be noted that these controls need to be supported by a well-organised IT infrastructure and data architecture.

1.5 All banks and finance companies (collectively referred to in this paper as "banks") are expected to benchmark their data governance and management practices against this paper and implement the necessary measures as appropriate given their organisational structures, business models, scale of operations and risk profiles. Banks should also take into account relevant guidance from other agencies, industry bodies, international fora[2] as they consider the adequacy of their practices.

[2] Relevant publications include those issued locally, such as by the Info-communications Media Development Authority as well as the Basel Committee on Banking Supervision (BCBS). See for example "Progress in adopting the Principles for effective risk data aggregation and risk reporting" (Nov 2023) published by the BCBS at https://www.bis.org/bcbs/publ/d559.htm.

2 Observations from Thematic Inspections

2.1 Under each of the themes, we outline MAS' supervisory expectations, key observations from the inspection and the consequential areas for improvement with illustrations of good practices observed provided in boxes.

A Board and Senior Management (BSM) Oversight

2.2 *Supervisory expectations:* A robust data governance framework is an important enabler for effective risk management. BSM should exercise sufficient oversight over the processes needed to achieve effective risk data aggregation and reporting. To this end, the identification, assessment and management of data quality risks should be an important part of a bank's overall risk management framework[3].

2.3 All banks reviewed had established relevant management committees for the oversight of data risk, covering data management areas (e.g. data privacy and confidentiality) and various regulatory initiatives on data, including the implementation of BCBS 239 principles, where applicable. For certain banks that are more advanced in the use of data, there are also separate management forums on data and technology that focus on utilising data as a resource to drive business value, such as data monetisation[4] and big data programs.

Updating the Board on data management

2.4 *Supervisory expectations:* Banks should regularly update their Boards on pertinent data management areas, such as data quality and issues of systematic and material impact on financial and risk reporting, functioning of the data governance framework, as well as the progress of BCBS 239 implementation, where applicable. This update is important to enable the Board to have sufficiently holistic view over the bank's management of data risk, especially where the quality of data is below risk tolerance. It also allows the Board to oversee the implementation and maintenance of the approved data governance framework.

2.5 The thematic noted that updates to the Board varied in terms of coverage and often did not include issues relating to data management and data quality, in particular those that can impact on publicly disclosed and key financial and risk metrics for decision-

[3] Refer to para 27 of BCBS 239.

[4] The term "data monetisation" refers to the use of data and/or data analytics to enhance the bank's bottom line such as in terms of improved revenue via more targeted marketing, cost reduction strategies and efficiency gains.

making purposes. While some banks regularly track the implementation status of BCBS 239, others only do so on an ad hoc basis, if at all.

Reporting of data governance metrics

2.6 *Supervisory expectations:* Senior management should be provided with relevant, accurate and complete information in a timely manner. There should also be an analysis of data risk that spotlights systemic and material issues on data quality. This information is needed to enable robust management oversight of material data quality issues, drive rectification and implement sustainable measures.

2.7 Some banks have included data risk within their established risk appetite statement, which then drives the reporting of data risk and remediation of data issues. Relevant metrics should be incorporated into the management reports on data management (see Box A.1 for an example). MAS noted some gaps in management reporting on data management, such as:

(a) Results of data quality checks were reported at the overall bank-wide level with no further breakdown by business unit (BU)/support unit (SU). Reporting only the overall data quality score[5] may mask possible low scores in certain BU/SUs that warrant further attention and targeted actions.

(b) Lack of analysis performed on the data quality trends, including whether the bank's overall data quality had improved or deteriorated over time, common root causes and risk implications.

(c) No regular tracking of data management issues, such as expired end-user computing tools and material data quality issues.

Box A.1 Examples of metrics for reporting to Board/Senior Management

An enterprise-level view of metrics designed to assess the effectiveness of data management and programs at one bank included:

a) data risk indicators
b) data quality, e.g. trend of data quality risk score
c) outstanding material data issues over period of review
d) policy compliance and deviation
e) data culture, e.g. on training and talent development

[5] Data quality score refers to the measure of the quality of data along the different data quality dimensions, e.g. % of null data fields within a data set for measuring data quality dimension on completeness.

The relevant data governance metrics were aligned with the bank's risk appetite statement, which specifically listed data risk appetite tolerance level on certain data risk, such as data privacy breaches, misuse of data, unavailability of data etc.

B Data Management Organisation[6]

2.8 All banks reviewed had a central data management office (DMO) or equivalent function set up (either locally or at the regional/Group level) that is responsible for data governance framework and policies, and data management processes. These processes included the maintenance of metadata, lineage documentation and data quality controls, as well as supporting the respective data management activities of the business and support functions. For banks that operate on a federated organisation model, there were also dedicated DMO resources for material business lines and support functions, such as finance and risk management.

2.9 *Supervisory expectations:* Banks should put in place sufficient measures and ensure clarity of roles within the data management operating model to oversee proper implementation of their data management framework and standards across the organisation, as well as to ensure effective monitoring of data quality. Regardless of whether the DMO is organised centrally or established across business and support functions, banks should provide the DMO with a clear mandate to perform the measurement and monitoring of data quality, including tracking and following up on data quality issues and exceptions/deviations from data management standards. In addition, there needs to be clarity of roles between the DMO at group level and local functions to implement data controls. For Singapore-headquartered banks, this clarity should likewise extend to their overseas operations.

2.10 The thematic inspections observed gaps in the enforcement of data management standards by DMOs, such as a lack of formalised roles and responsibilities for different data stakeholders, inadequate follow-up of long outstanding exceptions and conduct of data quality checks. In some banks, initiatives were taken to strengthen the control mandate of DMO so as to exercise stronger enforcement in the following areas:

(a) Rectification of exceptions in metadata;

[6] Data management organisation refers to the operating model that banks put in place to articulate roles and responsibilities of individual data stakeholders, mandate of key functions, and decision-making and control processes.

(b) Implementation of relevant data controls as agreed between different data stakeholders; and

(c) Establishment of appropriate data quality thresholds and control assessment.

2.11 For foreign D-SIBs operating in Singapore, critical data and reports are typically generated from global systems, which are subject to group policy framework and processes. In such circumstances, the DMO at group level is responsible for coordinating data management policy implementation and control processes across entities operating in different jurisdictions. The thematic inspections noted the following practices that helped to ensure effective implementation of group-wide data quality standards:

(a) Establishment of a data management charter that detailed the specific roles and responsibilities between Group DMO and the local first line business/support functions.

(b) As part of its independent validation activities for local reporting, data tracing was conducted to verify end-to-end implementation of data controls across the different hops and systems, including global systems that local operations relied on.

(c) Group DMO or system owners of global systems provided regular attestations to reporting units in various jurisdictions that relied on key data from such systems for downstream critical reporting at local level, such as risk and financial reporting. The attestations were periodically validated to ensure that they were made by the appropriate authority, supported by proper checks/reviews conducted and in line with validation outcomes.

C Data Quality Management and Controls

2.12 Banks should have an established data quality management framework and processes to provide assurance that data is of acceptable quality and fit-for-purpose, throughout the entire data lifecycle. As banks explore the use of artificial intelligence and machine learning (AIML), having a foundation of good quality data becomes even more critical.

2.13 MAS observed that the banks reviewed generally had clearly defined frameworks and processes to ensure data quality for key data and reporting. However, gaps were noted in the following areas:

(a) Data quality controls;

(b) Data quality scorecard to monitor and measure data quality and take corrective actions; and

(c) Data quality controls for end-user computing tools.

Data quality controls

2.14 *Supervisory expectations:* Banks should put in place mechanisms to ensure effective implementation of controls along the data flow, to ensure quality of data for reporting and other applications.

2.15 The banks reviewed had established data quality frameworks that encompassed data quality dimensions[7], types of preventive controls such as data entry rules, validation checks on transfer/loading of data between systems, and detective controls on data output via reconciliation/variance analysis conducted on key reports.

2.16 To ensure proper implementation of data quality controls, one bank maintained detailed documentation that covered controls in key reporting process and system controls, with an associated process to validate the controls. Another bank relied on a data service level agreement between data producer and data consumer to confirm the existence of data controls prior to use of data. A number of banks also leveraged on the Risk Control Self-Assessment (RCSA)[8] process to ensure execution of data quality controls. However, MAS noted a few instances where the RCSA did not include data quality controls in all stages of data flow, such as checks on data at originating source.

Box C.1 Programs to strengthen data risk and control awareness

A few banks had data governance training modules, and one bank included members of the Board in the training. Another bank had a program to embed data governance best practices in day-to-day operations, e.g. implemented data protection by design in system development process.

A few banks had also set out clear metrics depicting specific responsibilities for different data roles, along the areas of “know your data”, “monitor/assure your data”,

[7] Data quality dimensions are specific aspects or characteristics used to assess the quality of data. These dimensions help organisations ensure that their data is fit for purpose, reliable and valuable for decision-making. Common data quality dimensions include accuracy, completeness, consistency, timeliness, validity, uniqueness, integrity and accessibility.

[8] This refers to a bank's internal risk and control self-assessment which focuses mainly on operational risk.

and "assess your data related risk" etc. This raised the awareness across different data stakeholders on their responsibilities for data quality controls.

Data quality scorecard

2.17 *Supervisory expectations:* Banks should establish data quality indicators or scorecards with appropriate thresholds to enable systematic measurement and monitoring of quality of data across relevant data quality dimensions.

2.18 Most banks have programs for measuring data quality via scorecards at different levels, such as entity, BU/SU, system, application, or critical data element (CDE) level. The data quality scorecards measure quality across various data quality dimensions, such as accuracy, validity, completeness, integrity, consistency and timeliness. For each relevant dimension and use case, banks would set specific data quality rules and thresholds at the CDE level, which are usually executed via an automated system/platform to derive the final scores on data quality. There would be a further process to analyse the scores, identify data elements below the data quality threshold, and remediate the associated data issues. Some banks were in the process of enhancing their data quality program, such as through evaluation of differentiated and dynamic thresholds according to data types/use cases, and exploration of the use of data analytics in detecting data quality issues.

2.19 MAS noted the following areas for improvement:

(a) Some banks set a common threshold level for all data sets, which may not reflect their unique characteristics. For instance, in a specific use case involving customer information, data field on "customer full name" could be more critical relative to that of "date of birth". Data owners could set a higher data quality threshold for the first data field and a lower threshold for the second data field.

(b) Under the federated operating model, banks allowed BU/SUs to set thresholds that deviated from the baseline, but there was no materiality trigger for the thresholds to be subject to further review.

(c) The understanding of data quality at the entity level was impeded where different BU/SUs used different data profiling and quality scorecards. These differences made the aggregation of data quality results more challenging and hence a consolidated view across multiple dimensions was often not produced.

Box C.2 Ensuring quality in metadata

Banks have different approaches to maintain and update metadata, which is needed for data quality assessment and downstream controls to ensure quality of data for deployment. For instance, some banks spelt out the specific metadata that different data stakeholders needed to own and maintain. Another bank supplemented this with formalised data service level agreements to document and approve the updating of metadata.

Another bank ensured proper input of metadata upfront during data ingestion stage from source to data lake/enterprise data warehouse via automated validation checks on data quality dimensions, such as completeness and consistency. If the metadata was not updated or maintained properly, the platform would not allow the dataset to be deployed for further development or analytical work. This approach and underlying data architecture allowed the bank to quickly formulate a new automated process to plug identified gaps and ensure proper maintenance of metadata.

End-user computing (EUC) tools

2.20 *Supervisory expectations:* Data quality management framework should include standards and controls to ensure quality of data and output generated from EUCs, with sufficient assurance testing and management reporting[9]. While EUCs could be used to support data preparation and reporting, these tools require additional data quality controls to mitigate potential errors in the output produced, since enterprise technology infrastructure support and controls would typically not be fully applied to EUCs. Banks should have a process to risk-rate EUCs based on the business operations they support and the potential risks they are exposed to, such as data loss. For higher risk EUCs, banks should establish a plan to either decommission, transition them as a business service application, or retain them as EUCs with adequate controls applied.

2.21 All the banks reviewed used EUCs to some extent for data processing and reporting, given constraints in automation and system support. These banks sought to keep the use of EUCs to a minimum, and subjected them to a dedicated control framework that included risk assessment, periodic review and assurance testing of controls. A few banks also deployed a dedicated information platform to inventorise and manage EUCs, with automated triggers on periodic review and attestation of controls.

[9] Basel paper on "Progress in adopting the Principles for effective risk data aggregation and risk reporting" (April 2020) emphasised the need to have adequate testing to mitigate reliance on manual-intensive processes or EUCs for risk reporting.

2.22 MAS noted the following areas for improvement:

(a) In assessing the risks of EUCs, the criteria adopted by some banks were not sufficiently comprehensive. One bank adopted a set of generic risk assessment criteria adapted from internal audit[10] that was not specific to EUCs, with no justifications provided to support the assigned ratings. Banks should use EUC-specific factors in assessing EUC risks (e.g. confidentiality of information stored and processed by EUC, availability of application support, backup and recovery process, as well as technology obsolescence). Such risk assessments should be subjected to adequate review and challenge by the second line of defence (2LoD).

(b) Some banks relied on the RCSA program, as a risk-based approach, to manage the use of EUC and its associated risks. In addition, some banks required the EUC owners to perform periodic reviews of the EUC inventory, including the inherent and current risk ratings, with sign-off by the relevant BU/SU stakeholders. To enhance the effectiveness of the attestation process, banks should set out clearly the specific checks and controls to be reviewed prior to the sign-off.

(c) Some banks continued to use high risk EUCs beyond the approved date of decommissioning or retirement, without a remediation plan drawn up.

(d) While some banks reported on EUCs at the local Operational risk forum and/or Technology risk forum, others did not have regular reporting on EUCs at a country-level forum. Where there is a BCBS 239 steering forum in place, key issues relating to EUCs that are used in BCBS 239 reports should also be reported at the steering forum.

Box C.3 Reporting on EUCs

Some banks performed comprehensive EUC risk reporting and analytics with a focus on high risk EUCs. Regular reporting at country-level forums covered policy updates and burndown analytics for EUCs. Some features in the regular reports included:

a) Overall EUC landscape showing the trends and variances in both the high risk and low risk EUCs;
b) High risk EUC retirement/decommission trends by BU/SU;
c) Aging of high risk EUCs over time both at country-level and by BU/SUs, including how long each of the EUCs had been rated high risk; and

[10] These are risk assessment criteria for audit assessment and planning, and generally covered financial, operational, regulatory and reputational impact.

d) Decommission plans for high risk EUCs.

Some banks' 2LoD performed annual assurance reviews on EUCs. The assurance reviews covered EUCs across BU/SUs and incorporated sample testing of EUC control effectiveness as well as compliance with policy standards and MAS' Technology Risk Management Guidelines. Thematic weaknesses were highlighted at the risk forum and high risk issues tracked until closure at both the risk forum and relevant BU/SU forums.

D Data Issues Identification and Escalation

Escalation of data issues

2.23 *Supervisory expectations:* Banks should measure and monitor the quality of their data. There should be appropriate escalation criteria and action plans to rectify poor data quality and underlying gaps. Management should receive adequate information on material data quality issues, trend analysis, and progress of remediation measures. For overseas-headquartered banks, local management in Singapore should provide this oversight for the data used in the Singapore operations.

2.24 The thematic inspections noted various weaknesses in the policies and processes on data issues identification and escalation:

(a) Severity rating was not assigned to data issues, and no escalation criteria was established for management reporting and/or prioritisation of remediation.

(b) Guidance on assignment of severity rating of data issues was not formalised into a policy requirement, which could lead to insufficient attention on prioritising data issues for remediation.

(c) Aging of data issues and trends were not reported at data management forum.

(d) Root cause analysis on data issues was not conducted on a timely basis for remediation.

Data lineage

2.25 *Supervisory expectations:* Data lineage documentation impacts the capability to track the flow of data from the point of data entry in originating systems, through various intermediate systems and hops such as core banking system, risk and finance engines, to

the end-point of data consumption by users for applications and reports. Data lineage serves many purposes, one of which is the detection and investigation of root causes of data quality issues across BU/SUs. In this regard, banks should have robust and complete data lineage for CDEs, as part of their capabilities to identify and rectify data issues and defects.

2.26 MAS' thematic inspections revealed that the standard of data lineage across the banks reviewed was uneven. There were only a handful of banks that had the capability to capture the full end-to-end data lineage for CDEs, with sufficient granularity (including transformation logic and data control rules) and coverage (including EUCs and manual processes). Some banks only maintained data flow diagrams and incomplete data lineage (e.g. omitted certain hops) or data lineages that are put together from various sources manually.

Box D.1 Tracking and analysing data on data concerns

Some banks are starting to implement better system support for prioritising and remediating data issues at scale. This will allow them to address the high volume of issues and associated complexities that require multiple inputs from various data stakeholders. Common features of such system workflow tool include:

a) Centralisation of data issues within a single repository, with ability to capture material issues at local, regional and group levels.
b) Provision of visualisation/reporting on volumes, aging, categories, and trending to enhance the remediation of data issues.
c) System logging of data issues by respective data owners and consumers, with notification to trigger root cause analysis, risk rating and remediation measures.

In another bank, other than identifying the underlying gap that led to a data quality issue (e.g. mismatched account balances due to incorrect application of accounting treatments), it is a policy requirement for data owners to also log the underlying gap in a separate operational risk system for further investigation, if the gap is deemed to be severe and could have systematic risk implications. Both data quality issue and underlying gap will be rated in terms of severity, tracked and reported on their remediation status.

E Observations relating to BCBS 239

2.27 The BCBS 239 principles apply to Global Systemically Important Banks (G-SIBs) and national supervisors are strongly encouraged by the Basel Committee to apply the principles to banks identified as D-SIBs, three years after their designation as D-SIBs. In Singapore, the D-SIBs which comprise the 3 local banks and 4 foreign banks, are required to comply with the BCBS 239 principles.

2.28 While compliance with BCBS 239 principles was not the only scope of the thematic, this section elaborates on further inspection observations relating to BCBS 239 that are relevant for D-SIBs and branches/subsidiaries of G-SIBs that are operating in Singapore.

Expanding the scope of application

2.29 *Supervisory expectations:* The principles and supervisory expectations contained in BCBS 239 apply to a bank's risk management data, and the scope of application should minimally include the main risk reports for all material risks, i.e. in-scope reports[11]. As the application of the relevant principles and standards within BCBS 239 will strengthen the data management of critical functions and data domains, banks should seek to expand the range of in-scope reports beyond those expected under BCBS 239.

2.30 Banks have generally identified a set of in-scope reports that would be reviewed and approved at a management forum (e.g. a BCBS 239 steering committee). The types of reports identified vary across banks, with some banks applying BCBS 239 beyond risk management reports to include those relating to critical functions such as anti-money laundering, tax management, financial segment reporting and key regulatory reports. For these banks, the data quality standards and guidelines complying with BCBS 239 are mandatory for CDEs in these other areas such as screening and risk assessment for financial crimes, financial reporting under certain accounting standards, and trade surveillance to detect market abuse.

Effective independence of independent validation (IV) function

2.31 *Supervisory expectations:* BCBS 239 principles state that an IV function is an important component of a strong governance framework. Banks should put in place appropriate organisational arrangements and mitigants to ensure the effective independence of the IV function, including situations where the function is within the 2LoD that house other risk reporting functions. A strong and independent IV function will

[11] In-scope reports refer to risk reports for all material risks as defined by the bank, and which will contain the bank's risk management data. This includes data that is critical to enabling the bank to manage the risks it faces (e.g. customer ID, customer name, industry code).

be able to better ensure effective implementation of data management standards, and that risk data aggregation and reporting processes are robust.

2.32 MAS noted that most banks established the IV function within the 2LoD, either within risk management or compliance function. Where the validation function reports to an executive who is also in charge of risk reporting, it will give rise to possible conflict of interests, as the function will be validating the reporting processes owned by its immediate supervisor. MAS noted that in one instance, the key personnel responsible for IV was within the risk management function, but was reporting to a senior management staff in charge of risk reporting. The IV activities conducted did not provide adequate verification and challenge on data controls. The bank subsequently established relevant measures to mitigate the conflict.

Approach and execution of IV

2.33 MAS noted that most of the banks reviewed had established or are starting to formalise the IV function. In terms of validation methodologies, MAS observed three distinct approaches:

(a) Having a dedicated IV team to evaluate the design of data and reporting standards, as well as conduct sampling checks to test effectiveness of controls and policy implementation.

(b) Leveraging on the existing RCSA framework and process, where 2LoD control personnel independently perform verification of controls and challenge on the sample testing performed by 1LoD functions.

(c) Placing reliance on sample review evidence and artefacts provided by 1LoD to conclude on the extent of compliance with BCBS 239.

2.34 *Supervisory expectations:* A bank's risk data aggregation capabilities and risk reporting practices should be subject to an appropriately high standard of validation. For in-scope reports for material risks, banks should adopt a validation approach that involves an evaluation of control design and detailed testing of control effectiveness by an independent function. For other types of reports, banks should apply a standard of validation that is commensurate with the criticality of the report and information within for decision-making.

2.35 The thematic inspections noted the following weaknesses across the three validation approaches:

(a) Some banks did not obtain formal approval on the annual IV plan, or state clearly the timeline in the IV plan to complete validation of all in-scope reports.

(b) Some IV teams relied on the existing business-as-usual (BAU) controls and testing processes, such as the RCSA testing performed by the BU/SUs as well as various system control testing, to derive comfort on adequacy of the controls. However, these teams did not confirm if the gaps identified via the various BAU control testing processes were remediated. While IV may rely on certain BAU control testing processes, the IV team should still verify that the testing procedures performed are aligned with established standards and policies, and that exceptions identified via BAU control testing are remediated.

(c) At some banks, fire drills to test the capability to generate ad hoc reports had been suspended since the Covid-19 pandemic, and have not been resumed. Regular drills should be part of a bank's process to ensure that they have the capability to provide ad hoc reports during a crisis period in a timely manner.

3 Conclusion

3.1 Banks recognise that data has become a strategic asset and that the ability to manage and analyse risk data accurately and agilely is essential for sound decision making. MAS expects banks and finance companies to have robust processes in data governance and management, including monitoring of data quality and remediation of data issues.

3.2 The banks reviewed have taken, or are taking, remedial actions to improve frameworks, processes and execution of data governance and management. Banks that are not part of the thematic inspections should benchmark their practices against this paper and take steps to address gaps, if any, in a risk-appropriate manner.

Monetary Authority of Singapore