Research article

Risk compliance and master data management in banking – A novel BCBS 239 compliance action-plan proposal

José Martins [a,b,*], Henrique S. Mamede [a,c], José Correia [a]

[a] *INESC TEC, Porto, Portugal*
[b] *AquaValor – Centro de Valorização e Transferência de Tecnologia da Água, Chaves, Portugal*
[c] *Universidade Aberta, Lisboa, Portugal*

ARTICLE INFO

ABSTRACT

For some years now, master data has become extremely relevant to business success and continuity in an increasingly competitive and global business environment. The banking sector is one example of how the implementation of well-structured and designed master data management policies and initiatives is crucial for reaching positive results. One of the areas in which banks need to ensure extremely fruitful master data management approaches and data governance procedures is when dealing with risk-related data, as it not only ensures accurate and well-supported management and decision-making, but also because banks are required to do so by imposed regulations, such as the BCBS 239. Drawing on a DSR methodology supported research project, where banking and IS-related expertise was continuously merged with existing theoretical knowledge on MDM and BCBS 239 related topics, and a permanent focus on the technical and functional complexity associated with implementing master data management and well-established data governance procedures that ensure regulatory compliance, we propose a novel, six-phase action plan that will allow banks to ensure compliance with BCBS 239 and, consequently, ensure efficient and effective risk data management and reporting.

1. Introduction

As information becomes an increasingly relevant and critical asset for organizations and societies, the global evolution towards an information-centered economy is becoming further noticeable (Amir et al., 2019). If this importance is significant for most companies, this is even more relevant for the financial sector, where the generation of business data is not only becoming increasingly complex but also the inherent data volume is reaching very significant numbers (Aithal, 2016).

The concept of master data refers to data that characterizes the business entities considered to be of greatest relevance to the organization and on which most organizations' operations reside. From a functional perspective, master data focuses on presenting accurate, solid, constant, and little-changing descriptions of real objects and occurrences. Still, despite being conceptually different from both transactional and inventory data, master data assumes the role of reference for the latter (Otto, 2012).

Thus, if one of the main challenges for organizations is to devise and implement mechanisms and practices that allow efficient management of their data (Parviainen et al., 2017), the other is to implement the same

approach for their master data, which is normally generated in a set of different business/functional areas or systems (Ofner et al., 2013). According to Spruit and Pietzka (2015), for organizations that operate in data-intensive scenarios, in extremely complex regulatory environments, and that have an urgent need to be continuously efficient and agile (like the financial sector), it is even critical to implement focused and structured master data management practices, as data tends to represent the main source of added value. Despite being well characterized in the existing literature, from our perspective, one of the most straightforward definitions of the concept of Master Data Management (MDM) is presented by White et al. (2006), according to whom "*MDM is a workflow-driven process in which business units and IT collaborate to harmonize, cleanse, publish and protect common information assets that must be shared across the enterprise. MDM ensures the consistency, accuracy, stewardship, and accountability for the core information of the enterprise*".

1.1. Methodological approach

As argued by Baskerville et al. (2018), when addressing a given research problem that falls within the Information Systems field of study, one should

---

* Corresponding author.

E-mail address: jose.l.martins@inesctec.pt (J. Martins).

always establish a validated research methodology that accurately supports all the activities that are to be conducted in order to reach a prospect solution. By merging this assumption with the issue inherent to our research project, i.e., the inexistence of a straightforward action plan that companies from the banking sector could simply acknowledge and implement, it is critical to identify a research methodology that would combine both (scientific and grey) literature and practical expertise and have already supported multiple information systems research projects. Thus, after actively analysing existing literature, we were able to identify DSR - Design Science Research methodology (Hevner and Chatterjee, 2010) as the most adequate for supporting our research activities, as we are pursuing an artifact by combining theoretical knowledge with know-how from both information systems and banking experts.

As perceived in Figure 1, our study methodology was composed of a two-stage iteration ("Design" and "Evaluate"), which was repeated until there was an acceptable level of confidence in the quality of the BCBS 239 compliance action plan. Hence, to undergo our research, we started by conducting a multi-vocal literature review that analysed both the scientific literature and the (typically known as) "grey literature" published by professionals (Garousi et al., 2017). As a result of this review, we were able to not only conceptualize the MDM and BCBS 239 related topics, but also to perceive the difficulty in identifying (and easily implementing a functional approach focused on implementing MDM in the banking sector. Hence, the following research question has been highlighted: "Is it possible to establish an action plan focused on delivering banking organizations the ability to be compliant with BCBS 239?".

Afterward, and after considering the consensus on banking organizations' necessity to define and implement data management strategies that allow them to extract from data the necessary knowledge so that they can remain efficient, competitive, and, above all, in compliance with existing standards and regulations, we were able to establish that the two main requirements of our research: 1) the proposal of an action plan for banks to implement "BCBS 239" (one of the most relevant banking regulations in force); and, b) the proposal of a master data maturity model that should be taken into account in implementing the action plan.

Hence, by merging the abovementioned requirements, needs, and overall theoretical knowledge on the MDM and BCBS 239 related topics, an initial design stage was implemented. This initial task originated the first version of our research main artifact (the BCBS 239 compliance action plan), which was presented to both the banking sector experts (from

multiple functional areas, and Risk managers, to Chief Data Officers, Executive Managers, and Board Members), and also Information Systems and Information Technologies experts (with and without any direct relation to the banking sector), in order to collect their feedback on the overall quality of the artifacts' initial version. This feedback was later incorporated into a novel version of the artifact that was once again presented to the group of experts that collaborated with our research. This two-stage iteration was repeated until the entire set of experts felt comfortable with the maturity and potential outcome of the proposed artifact. The final version of the proposed BCBS 239 compliance action plan is detailed further down.

The remainder of the paper is organized as follows. The second chapter presents a very focused analysis of the theoretical and practical framework surrounding the MDM concept. In the next chapter, we present an analysis of the relationships between data, master data governance, and compliance in the banking industry. Subsequently, we provide a detailed presentation of the proposed action plan for ensuring banks' compliance with BCBS 239, which is followed by a characterization of the proposed MDM maturity model for banking organizations. The paper ends with several conclusions and final considerations about the research carried out.

2. From compliance with BCBS 239 to master data management – a conceptual perspective

In this section, we present a detailed and focused analysis of the existing literature on the BCBS 239 standard and the master data management topics. Considering the practical context of banking and the inherent relation the sector has with the IT sector, the referred analysis details both the arguments of the scientific and the "grey" literature.

2.1. BCBS 239 principles and context

The "BCBS 239" concept refers to the "Principles for Effective Risk Data Aggregation and Risk Reporting" (BIS, 2013) made publicly available by the BCBS (Basel Committee on Banking Supervision) in early 2013. From a structural perspective, BCBS 239 is organized around a set of 14 Principles that draw attention to the diverse obligations and concerns that must be addressed when managing risk in banking institutions. These principles are grouped according to their technical/functional framework, as follows:
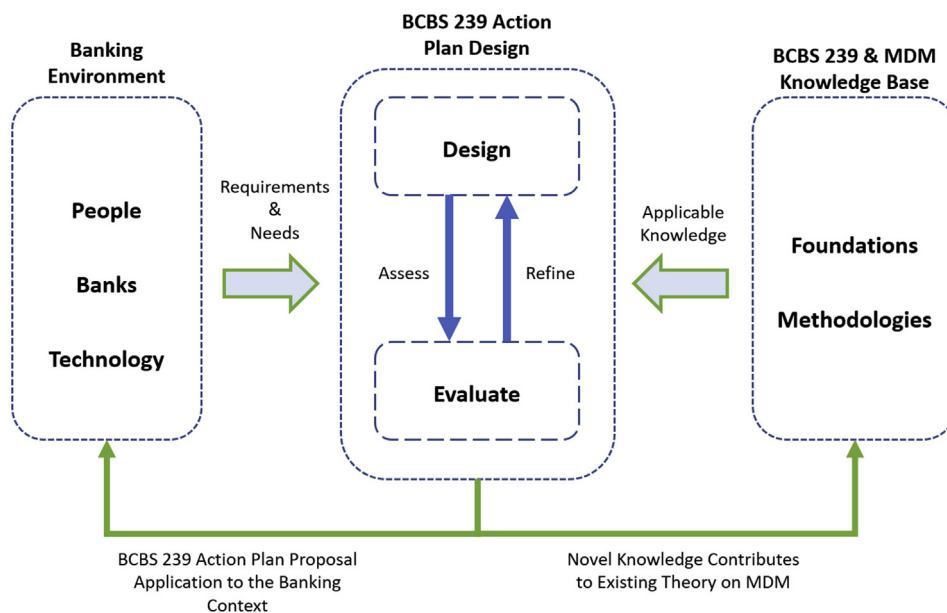

Figure 1. Research methodology used to support the study. (Adapted from (Brocke et al., 2020)).

Government and Infrastructure (focus on banks)

- **Governance** – The entire set of bank's risk data aggregation resources and reporting practices ought to be governed and inline with the remainder of the guidelines and principles that the Basel Committee establishes.
- **Data architecture and IT infrastructure** – The banks' data architecture and overall IT infrastructure must ensure permanent and continuous support to the entire set of risk data aggregation resources and reporting practices, while still meeting the other established principles.

Risk Data Aggregation Capacity (focus on banks)

- **Accuracy and Integrity** – A bank must ensure the accurate and reliable generation of risk data and should do this by ensuring compliance with (normal and stress/crisis) reporting accuracy requirements. In order to decrease the probability of error occurrence, data should preferably be aggregated by automated mechanisms.
- **Completeness** – A bank must have the ability to collect and aggregate the entire set of material risk data that exists throughout the business group. Nevertheless, the existing data must be structured in a way that allows for its interpretation according to business line, legal entity, asset type, industry, region and other risk-relevant groupings, thus ensuring the clear identification and reporting of the risk exposures, concentrations and emerging risks.
- **Timeliness** – Besides assuming the continuous obligation to ensure compliance with the accuracy, integrity, completeness and adaptability principles, banks are also recommended to ensure the existence of processes that generate up-to-date and aggregated risk data in a timely manner. This timing will be dependent on the nature and volatility of the potential risk that is being measured, on the bank's global risk profile, and on the bank-specific frequency requirements for risk management reporting for both normal situations and stress/crisis occasions.
- **Adaptability** – A banking organization ought to have the ability to generate aggregate risk data that meets a broad range of on-demand ad hoc risk management reporting requests. This ability should be continuously available and should encompass both the requests that might arrive during stress/crisis situations, the requests that arise from changes in the internal needs, the requests focused on meeting supervisory queries.

Risk Reporting Practices (focus on banks)

- **Accuracy** – In order to be considered valid, risk management reports must accurately and precisely present the aggregated risk data in and accurate and precise manner and reflect the overall risk level in the same accurate and precise manner. Furthermore, reports must be reconciled and fully validated.
- **Comprehensiveness** - Risk management reporting must comprehend the entire scope of material risk areas within the bank. Additionally, the depth level and scope of the created reports should be coherent with the characteristics of the bank's operations and risk profile, and with the full set of requirements presented by the reports' recipients.
- **Clarity and usefulness** – All risk management reports are recommended to present information in a manner that is perceivable as clear and concise, hence reports must easily understandable and, in parallel, still be comprehensive enough to efficiently support decision-making processes. Furthermore, these reports should be developed in line with the recipient's information needs.
- **Frequency** – The frequency in which risk management reports are produced and distributed should be established by the board and senior management (or by the direct recipients). Hence, the referred frequency requirements should, transversely, reflect the risk information needs from those receiving the reports, the sole nature of the risk information that is being reported, the velocity at which the degree of risk can shift, and the overall importance of the report to the efficient and successful risk management and decision-making throughout the bank. To ensure further control, risk reports should be produced at a higher frequency during stress or crisis moments.
- **Distribution** – At the same time risk management reports should be distributed to the entire set of relevant parties, the inherent confidentiality must be always assured.

Review and Supervision (focus on banks)

- **Review** – The supervising entities should frequently review and fully evaluate a bank's compliance with the eleven effective risk data aggregation and risk reporting principles above.
- **Remedial actions and supervisory measures** - Supervisors should have access to efficient and effective toolsets and resources that allows them to demand successful and timely remedial action by a bank whenever they identify deficiencies in its risk data aggregation capabilities and risk reporting practices.
- **Home/host cooperation** - Supervisors are required to actively cooperate with other jurisdictions supervisors, in both the Principles supervision and review activities, and in demanding the execution of any necessary corrective action.

Therefore, and realizing the criticality of carrying out an efficient and effective management of data from Banking Institutions, functional and technical conditions must be guaranteed for the development and implementation of a framework that allows the management of data from these institutions (Figure 2) in order for them to ensure compliance with BCBS 239.

Although the Basel Committee on Banking Supervision has been forcing, nationally and internationally, the implementation of the BCBS239 standard, there are many banking institutions at European level that do not yet have adequate levels of compliance (Pilger and Maldonado, 2017). According to the referred Committee, despite the baking sector notorious efforts, not only none of the G-SIBs (Globally Systemically Important Banks) are fully compliant, as a significant part of these institutions are yet to build an adequate data architecture and a well-structured IT infrastructure (BIS, 2018; Elhassouni et al., 2020).

Thus, and according to the various international reports on the subject, among the various challenges facing banking sector organizations with regard to the implementation of BCBS 239, it is possible to highlight the following (Avantage Reply, 2016; BIS, 2018; ECB, 2018; Gillet and Lajkep, 2020; Harreis et al., 2017): a) lack of control in the front-office mainly due to the quality issues associated to manual data entries in a disparity of front-office systems; b) the existence of an inefficient data architecture and as a consequence the prevalence of multiple data repositories without a common data model and of various legacy systems who make it very difficult to establish relations/dependencies between data; c) the lack of a focused business perspective when implementing data collection mechanisms and when manually acquiring business-related data; d) the diminished interest of top management on the processes of transforming raw-data into valuable business information that, most of the times, forces these processes to be designed within the IT department; e) the existing decentralization of the data transformation processes that convert business data into information, that tend to happen in a separate and disaggregated manner instead of being done in a centralized way; f) the existence of ineffective data governance models that do not allow for a clear definition of data ownership and ownership policies; g) the small amount of funds and resources allocated to data transformation that tends to lead to the implementation of limited data management and transformation procedures; and h) the existing mindset that data transformation is just a compliance requirement instead of a full scope business need.

2.2. Best-practices for implementing BCBS 239

There is a significant consensus within existing literature that banks must ensure a continuous development of their skill set on what concerns risk data aggregation and risk reporting, mainly due to the recent events related to the global financial crisis that were the final proof that the banking system has little to none ability to reach accurate risk data in a systematic, efficient and effective manner (Valladares, 2018).

As argued by Gilbet and Lajkep (2020), as a response to the complexity associated with BCBS239, the majority of banks idealized and implemented extremely complex solutions focused on setting up the necessary procedures that would ensure long-term compliance with the regulation. However, these complex solutions demanded for a very solid knowledge and experience on managing projects that included multiple stakeholders that may (or may not) be located within the same physical location. Hence, the main issue that banks tend to face, lack of knowledge, experience, overall perception, and mindset on how to implement a solution that, at the same time, is complex from an IT perspective and must be totally aligned with the business goals and strategy.

With the above in mind, and after perceiving that most of the banking institutions under their scope were far from being compliant with BCBS 239, national regulators started to propose sets of best practices that when adopted would trigger the necessary changes that would lead to the much-wanted compliance. The central bank of the Portuguese Republic –

responsible for regulating the Portuguese bank and finance sector – was one of the abovementioned entities that proposed a set of best-practices for the banks operating in Portugal to incorporate in their operation (Banco de Portugal, 2019). These best-practices (Table 1) were organized according to BCBS 239 principles (BIS, 2013).

2.3. Master data management overall importance and need

The uncertainty, volatility and instability of current markets are compelling organizations to maintain highly competitive mindsets, that are operationalized through the creation of differentiation mechanisms that not only allow for prominence but also exert pressure on competitors (Yu et al., 2018). This innovation-based, competitive and result-oriented posture is, as would be expected, increasingly related to firms' digital transformation and dependent on the internal reorganization of business processes, resources, and IT infrastructures (Weresa, 2019).

As argued by Townsend et al. (2018), one of the main assets of an organization is its data, since, in addition to guaranteeing the uniqueness of the organization, this data can improve the existing service/product portfolio, optimize customer relationship management and, ultimately, improve the performance and competitiveness of the organization. Even so, due to the multiplicity of available data collection sources, it is very common for an organization to be faced with very significant, heterogeneous and, often, inconsistent, duplicate and non-standardized data volumes, which require careful (life-cycle) management and maintenance so that they can be used in the decision-making process efficiently (Hashem et al., 2015).

If one acknowledges the existence of the abovementioned digital assets (aka "data") exist, then one must also recognize the need for a governance dimension, thus ensuring that can benefit from those assets, mainly by increasing their revenue, reducing their overall operational costs and, consequently, minimizing the inherent business-related risks (Abraham et al., 2019). To implement effective data governance, the value of the data has to be previously assessed and the inherent risk calculated, the implementation results must be continuously measured, and a constant reassessment process must be implemented (Al-Ruithe et al., 2019).

Therefore, it is widely recommended that data, considered critical for the organization's business, is managed in a structured manner and with a focus on ensuring the quality, integrity, and consistency of existing data. One of the ways to ensure effective and efficient management of existing data is the implementation of Master Data Management (MDM) (Gartner, 2018; Haneem et al., 2019). According to Vilminko-Heikkinen and Pekkola (2017), although there are some parallel views for the concept of Master Data Management, they all assume the same assumptions and
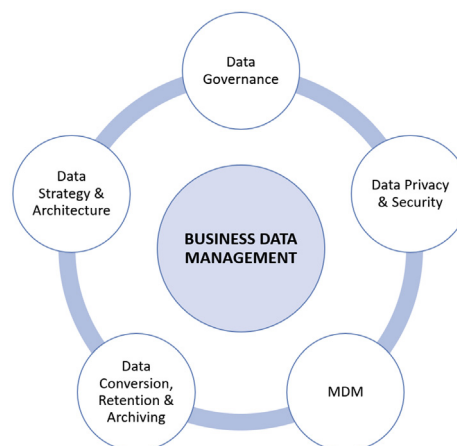

Figure 2. Business Data Management framework for BCBS239 compliance.

Table 1. BCBS 239 advocated best-practices organised according to a set of established principles. Based on (BIS, 2013).

Principle 1	Existing IT/IS management should strategically define a specific entity or functional unit that should be fully dedicated to managing existing resources and available data.
	It is also important to create a steering committee that focuses on data management issues and sits within an existing IT-related committee in which the board participates.
	In addition, it is important to define policies based on valid concepts and needs, composed of goals, responsibilities and procedures.
	In addition, the banking organization should combine the above policies with existing risk management policies and the overall strategic plan.
	To ensure full compliance with Principle 1, it is important that the bank implements the necessary internal audit activities and independent validation activities.
Principle 2	There should be a single and centralized database, built according to a formal concept dictionary that holds, in parallel, a formal definition of data and indication on its owner (business & IT). When creating this database, it is critical to merge it with a metadata repository holding an overall perspective on the data model.
	This principal also impels banking organizations to implement automatic control for permanent validation of data integrity throughout the entire data life-cycle.
Principle 3	Carry out the deployment of an action-plan, supported by a detailed documentation and including the accounting department, that allows for data reconciliation procedures focused on documenting and addressing the highlighted differences.
	Implement well documented controls and validation procedures all for the already existing manual data input processes and controls, and also for all final reports that are being generated.
	Finally, document in a formal manner the traceability of all used concepts, from its original source to the data point.
Principle 4	In order to transversely ensure compliance with BCBS 239, banking organizations must guarantee that all used data sources, concepts, processes and implemented systems are common to the entire organization, including branches and similar entities, and that have sufficient granularity for allowing a proper and accurate use.
Principle 5	In order to ensure the smaller possible bias impact, it is critical for banking organizations to implement solutions that allow for manipulation, analysis and interpretation automation. Nevertheless, there should also be an up-to-date mapping of all existing manual processes for both operational control and perspective evolution purposes, and also a clear definition of contingency and continuity plans.
	Finally, the referred organizations are also impelled to ensure a considerable level of independency towards data, systems or process that are either time-consuming or non-replicable.
Principle 6	Considering the need for banking organizations to be continuously prepared for dealing with potential changes and evolutions to existing processes and procedures, it is extremely important these organizations ensure they have access to human-resources that are both skilled and available to implement the referred actions and doing so with the appropriate solutions and supported by agile methodologies.
	Furthermore, banking organizations should also define regulatory anticipation procedures and implementation reports, that will allow for the managing bodies to perceive the business in a more accurate and detailed manner.
Principles 7 to 11	Considering the information needs and obligations of banking entities, it is of utmost importance that they ensure detailed formalization of the entire set of reports that will be generated (including frequency, recipients and expected content). It is also important to formalize and document existing report approval processes involving the bank's board of directors.
	Given the present regulative compliance necessities that banks face, there's a compelling got to implement consistency validation procedures that make sure that each internal and external coverage is correct and doesn't cause any legal risks.

vision. Thus, MDM can be perceived as a discipline, supported by digital technologies, in which the "business" and the "IT" work collaboratively to ensure uniformity, precision, management, semantic consistency and validity of the master data that is shared by the entire structure, processes and initiatives of the organization.

If these assets are not properly managed, problems will arise throughout the organization, mainly because people do make mistakes, mistakes that more commonly result in losses than security problems or computer systems intrusion. These losses will affect all aspects of IT and business and put the risk at an unsustainable point (Raguseo, 2018). Thus, and drawing on Haneem et al. (2019), by serving as a point of reference for business-critical data, MDM allows for the elimination of redundancies and inconsistencies in the data that tend to represent not only inefficiencies but mainly very considerable business and operational costs.

Hence, in this context, MDM refers to the processes, governance structures, systems and content created and implemented to ensure consistent and accurate source data for operational and analytical processes. This definition incorporates two concepts that are important to detail and that are: the concept of Master Data; the concept of Reference Data (Otto, 2012). The concept of Master Data refers to business information that can (and should) be shared internally in an organization. In practical terms, we are dealing with the entire set of data (structural information dataset) necessary so that the various business processes can be developed according to the established. Master Data – the main focus of MDM - typically includes business-critical domains, such as employees, customers, accounts, products and even accounting information. Reference Data - the other focus of MDM - refers to data that is used to categorize other data in the organization's repositories, or to serve as a basis for establishing relationships between existing data in an existing database and information outside the organization. Typically, Reference Data includes codes, states, product/service hierarchies and element lists (Gartner, 2018; White et al., 2006). From a broader perspective, MDM includes aspects such as (Informatica, 2020): a) Governance, policies, and procedures; b) Processes and workflows; and c) Standards and best-practices.

Thus, realizing the complexity associated with the Master Data Management of an organization and its, increasingly, dispersion across multiple systems and even repositories, it is understood as totally necessary to implement mechanisms for systematizing information flows so that they not only maintain compliance with the regulatory component, but also maintain alignment with business principles and vision. An MDM process is as more efficient as possible the existence of a central data repository, capable of providing the organization with a unique and validated view of information, eliminating inefficiencies, which can have a high associated cost and often caused by the existence the effect of "data silos" (Profisee, 2020b; Vilminko-Heikkinen and Pekkola, 2017).

This raises the theme, which is one of the main objectives of an MDM process, which is to manage and make data available to the organization with a high level of quality, without duplicates, exact and current, to always obtain a unique view of the truth. Thus, it is essential to understand that the state of the data is what matters most and that, for this, there are several factors that have to be considered, namely (Geiger, 2007; Ghasemaghaei and Calic, 2019):

- **Completeness** - ensuring that data are all relevant elements to ensure that a system and process can function as intended;
- **Opportunity** - ensuring that data is delivered or is accessible in a timely manner when the opportunity arises to use it;
- **Compliance** - the data obey and comply with certain conditions and rules in accordance with the established standards, regulations and requirements;
- **Exclusivity** - ensuring that data is exclusive, that is, not duplicated;
- **Accuracy** - ensure that the data has been validated and approved by the standard precision assessment mechanisms;
- **Availability** - ensure that the data is available and in a state that allows its use;
- **Validity** - ensure that the data represent concrete and correct elements of the real world;
- **Consistency** - ensuring that the data is in a state of integrity that allows its use.

Hence, one can easily perceive that the implementation of an MDM process also includes Data Quality Governance (Risto et al., 2011). With this in mind, it is admissible that in order to provide for high quality data, that is considered necessary and adequate to meet the requirements of systems, processes and individuals, a set of specific control mechanisms must be implemented.

2.4. Data governance c master data management

In order for an organization to remain continuously competitive and efficient, it needs to ensure that its main asset - data - is properly structured, standardized and managed (Chiang et al., 2018). When conditions such as the immediate availability of data and the assurance that it is of the highest quality and relevance, it is possible to use this asset as the basis for business initiatives (Côrte-Real et al., 2017).

As argued by Leonelli (2019), good data governance ensures that existing data throughout an organization's entire infrastructure and operating systems, have the characteristics mentioned and can, ultimately, be used to generate value. According to Alhassan et al. (2018), in order to ensure its normal operation and be able to continuously innovate and grow, an organisation must adopt a data governance program that allows a straightforward insight on what existing data should be considered as valuable, where it is, how and by whom it is being used and where is it being integrated.

As detailed in existing literature, there is a variety of reasonings on the Data Governance - DG topic. This disparity is the result of two different perspectives on the topic, one that perceives data governance as an essential support to critical domains such as data quality, data security, and data lifecycle (Tallon et al., 2013), and the other perspective that perceives DG as a more restrained approach to corroborate the conceptual or empirical content of data (Rasouli et al., 2016).

Although it is clear that there is a concern on the part of organizations with data governance, the truth is that many of the already implemented data governance programs and initiatives were not effective and did not represent appropriate solutions (Ibrahim et al., 2018). This problem typically related to top management members who do not recognize the potential added value generation that a well-designed data governance strategy ensures (Ladley, 2019). Consequently, this tends to lead to the definition of internal policies and standards that are losing relevance, to the point that they become mere recommendations for IT teams, instead of being strict guidelines for the entire organization.

Nevertheless, and drawing on Abraham et al. (2019), as the annual global data volume sets at over 40 zettabytes, the number of different data sources (with different structures and formats) tend to increase and organizations are increasingly dependent on data to ensure a well-supported decision-making process, it is critical to implement well-structured data governance approaches focused on very good quality data (Profisee, 2020a).

Hence, if one perceives master data continuous development as one of the most important elements behind an organization information management strategy, as it ensures the needed consistency and uniqueness, it is critical that the organization implement a serious, well structured, data governance action-plan supported by all the established best-practices (Ibrahim et al., 2018; Liu et al., 2020; Paananen, 2020).

3. Data, master data governance and compliance in banking

Compliance is a concept that has its origin in the term "comply", that is, to be in accordance with any orientation, rule, command, or policy. Thus, banking compliance means complying with rules, laws, and guidelines, whether internal or external (Kaminski and Robu, 2016).

The main goal of bank compliance is to prevent, detect and resolve any deviation, less legal aspects and non-conformities in the Bank's operation (Edwards and Wolfe, 2004). Therefore, it constitutes a valuable support tool for the management of the institution, in general, and for managers and people responsible, in particular, for: a) Process

information; b) Security; c) Risk management; d) Ethical conduct and other controls; and e) Data reliability.

Due to the characteristics of the Banking Sector, which have been changing over the years, and the emergence of new processes, bank compliance has a strong influence as an advisory strategy. After all, when complying with policies, guidelines and legislation, the institution will have a more efficient decision-making process with regard to risk prevention strategies and determination of values or missions within the Bank (Broeders and Khanna, 2015).

According to Brown and Dinç (2011), the Banking Sector is a highly regulated sector of activity, which means, for each institution, the imperative need to respond adequately, accurately, correctly and in a timely manner to the multiple requests, both regular and untimely, requested by the regulatory authorities.

In order to respond to the various regulatory requirements, Banks need an integrated system environment that meets requirements such as access to cross-sectional data throughout the institution, the existence of a single truth of information on various elements such as customer details, customer identification programs, data auditing and traceability, customer data synchronization across multiple heterogeneous operating systems, continuous data governance, and also risk and compliance reporting (Li et al., 2012). This is event critical when considering that in order to comply with the various regulatory requirements, banks need to indulge in a master data management strategy that allows them to improve their data collection procedures, their data cleansing, comparison, consolidation and quality control tasks, and data distribution events (Prokhorov and Kolesnik, 2018).

Currently banks are required to improve their know-your-client abilities to improve their operation cost issues, to improve their risk management capacities, their capacity to fulfil regulators expectations on reporting frequency, accuracy and timeliness, and to improve their data quality procedures. According to Capgemini (2015), MDM will allow banks to address the complexity inherent to legacy systems, to improve their data consistency and accuracy, their ability to comply with regulators prospects, to improve data quality, centralization and interpretative bias, and will also allow to establish consolidated views on customers' information.

4. Action plan for implementing BCBS 239

With this section we intend to introduce a contextual perspective on the multiple implementation styles and approaches of the BCBS 239 standard that have been defined and, afterwards, present in a detailed manner our action plan proposal for implementing BCBS 239 in banking organizations.

4.1. MDM implementation styles and approaches

Realizing the MDM's focus on continuously increasing the quality of Master Data, to the point of ensuring a consistent use of this same data, over the years various styles of implementation of Master Data Management were presented (White et al., 2006). An MDM implementation style consists of two types of key systems: those responsible for generating disperse data from a business entity (typically already one or multiple existing IS), and the Master Data Management system itself (Galhardas et al., 2010; Piedrabuena et al., 2015). Amongst the full scope of implementation styles, the following are the most used:

- **Consolidation** - Efforts are made to add the master data to a common repository that tends to be used as a basis for reporting actions. In practical terms, this style of implementation tends to be of great use for the preparation of existing data in the sense that it is available to feed downstream systems (Dreibelbis, 2008). They present the limitation of being an implementation style that produces an output that only allows reading and not manipulation.

- **Registry** - Implements a global data registration system with formal links to the data of the various systems of the organization that, in real time, allows a reference to existing data. Being an implementation with a simpler and faster implementation effort, it allows the total view of the data to be built as new business needs arise. It produces outputs in reading mode and its management tends to be somewhat complex (Fan et al., 2014; Loshin, 2010).
- **Transactional Hub** - Implementation based on the creation of a single and centralized view of Master Data, which can be accessed through services available for this purpose. In this way, data consumption remains executable even if new applications and consumer systems are included or changes to existing ones. The implementation of MDM through a Transactional Hub can lead to a need to change existing systems at the date of its application (Dreibelbis, 2008).
- **Coexistence** – Implementation that combines both Consolidation and Transactional Hub styles, based on a single view of Master Data that is synchronized, in (semi) real time with existing consumer systems (Otto, 2012). Across the board, existing systems must remain watertight and unaltered so that there is no risk that synchronization tasks will result in errors. This implementation style generates editable outputs (Loshin, 2010).

An organization's data can be considered as operational data and non-operational data. While operational data refers to data (collected in real time) that supports the organization's daily processes and activities, non-operational data represents an asset that is stored in repositories (typically data warehouses) and that are used in decision-making actions. Functionally, Master Data Management implementations can be categorized according to the procedural approach that is inherent to it. There are two possible approaches that can be used in this categorization action (Woo, 2019):

- **Analytical Approach** - Analysing published case studies and public knowledge on the subject, the analytical approach is the one that has served as the basis for most MDM implementations. The focus of Analytical MDM is to ensure that only one perspective of Master Data is propagated throughout the application infrastructure up to the data warehouse, and this is where business intelligence and analytics activities should fetch the data for its execution. Thus, it is possible to acknowledge that the implementation of an Analytical MDM approach serves the purpose of assisting the company in its decision-making process. Although the implementation of Analytical MDM tends to be something of low effort and relatively simple, the quality of the resulting data is not the best in terms of promoting operational and administrative efficiency (Vilminko-Heikkinen and Pekkola, 2017).
- **Operational Approach** - The objective of the Operational MDM is to ensure that there is a single view of Master Data in the main operating systems used by the business teams. It is on these systems that Master Data is originally created and it is also here that it risks being considered a concern. This situation occurs due to the fact that the implementation of the operational MDM creates an interconnection between the various existing business applications, consequently having to take into account issues as relevant as privacy, security and regulatory compliance (Xyloyiannis, 2017).

From a full scope perspective, and drawing on the existing knowledge on MDM (Woo, 2019; Xyloyiannis, 2017), when considering an analytical approach to MDM there are two implementation styles to choose from, namely the consolidation style and the registry style. If, on the other hand, we are considering an operational approach, the transactional hub and the coexistence implementation styles are the way to go.

4.2. The complexity associated with BCBS 239 compliance

Even though it has been available since 2013, BCBS 239 remains shrouded in confusion, mainly due to the potential for bias associated with the individual interpretation of its principles. This interpretation difficulty, coupled with the complexity inherent to its implementation has led to significant extensions (up to 24 months in excess) to the execution of projects and initiatives carried out by the banking institutions in order to ensure compliance (Lukas and Hubert, 2015).

BCBS 239, although complex to implement, is based on principles that focus on ensuring the economic and organizational viability of banking institutions and improving their risk management capacity. Thus, it is assumed that a banking institution that achieves compliance with BCBS 239 is better prepared to anticipate new market opportunities and, at the same time, to prevent future situations of financial market instability. Thus, from an operational point of view, the development of initiatives aimed at adapting banking institutions to the principles of BCBS 239 must be cooperative, collaborative, and multidisciplinary, involving business teams, IT specialists, those responsible for the leadership and governance of existing data, and the managers and administrators of the institutions themselves. In short, it is not possible to assume that regulatory compliance will be achieved only with the implementation of ad-hoc technological solutions (however complex they may be), but with a collective effort and an alignment of the strategic views of all members banking institutions (Lux, 2014).

Hence, it is indirectly determined to extend the scope of the Master Data Management and Data Governance processes to the entire structure of entities in the Banking Sector and not just to data related to Risk Management. This will certainly contribute to an increase in the complexity already existing in the Sector.

4.3. MDM implementation plan proposal

According to Orgeldinger (2018) and Dill (2019), the implementation of BCBS 239 requires a multidisciplinary approach and a series of organizational skills that must be worked together. In their research, the authors not only highlight the need to develop the ability to establish a structured and focused methodological approach, and the ability to ensure a well-defined internal organization, but also refer these aspects as being those with the most significant impact to the implementation process. Furthermore, the same authors establish that the technological capabilities of the organization and the existence of a properly formed and strategically aligned leadership, will also influence the process of implementing all the measures necessary to comply with BCBS 239.

Although it is not possible to establish an action plan generic enough to ensure full compliance with BCBS 239 to the entire set of banks, based on the previous experience of other entities, by combining the existing scientific and grey literatures, it is possible to outline a sequence of steps that, when effectively completed, provide the institution with the ability to operate in accordance with the regulations.

Hence, drawing on existing knowledge and supported by the research methodology described in the early sections of the paper, a novel action-plan for compliance with BCBS 239 has been iteratively developed and assessed by multiple experts and stakeholders from the Portuguese banking and finance sector. This artifact, composed by six sequential stages that should be continuously executed in order to ensure unceasing compliance, can be perceived in Figure 3.

One of the main obstacles to the process of adaptation to BCBS 239 is the conceptual and functional perception that compliance with regulations only arises with the creation of a centralized data repository, which allows a unified storage of all data related to the Financial and Risk components. This operation, although idyllic, is extremely difficult and painful to be carried out successfully in a timely manner and with existing resources. Thus, it is becoming consensual that the

implementation of an organizational adaptation process based on very focused and sequential iterations is the most reasonable approach (KPMG, 2016).

As currently established, banking institutions are forced to provide a set - almost multidisciplinary - of risk reports. However, in an open way we can recognize that this type of reports comes with one of two purposes: 1) Reports created for risk managers, which allow a detailed view of the business, and which present the most relevant information for the business; and 2) Reports created to satisfy the requests of the institution's supervisory entities or stakeholders, and which tend to be focused on presenting only information that is in accordance with the regulations in force and requirements of the requesting entities.

Therefore, we can assume that an iteration represents the execution of a series of functional, operational and technical processes that allow reaching a specific report or set of reports (Figure 2). In this way, it is expected that after multiple iterations, it will be possible for the Banking Institution to have carried out the operational, functional and technological changes/evolutions necessary to ensure compliance with BCBS 239.

4.3.1. Business requirements definition

From an operational point of view, business requirements represent the needs that users generate when carrying out their tasks. These requirements are by no means limited to a specific data repository, as they tend to be specified at a higher level in which they understand in parallel the information needs and the results that are intended with that same information.

In operational terms, when defining the business requirements inherent in an iteration, the following points must be considered: 1) Mandatory reports and operations in accordance with the supervision and regulations in force; 2) Reports, calculations and operations carried out internally, in an ad-hoc manner, to respond to specific requests from management/administration; 3) Existing internal reports (Ex: Profit & Loss report); 4) Open points from previous audits that can (and should) be resolved; 5) Extra features and/or specificities that must be incorporated into existing reports or processes; 6) Potential actions to correct and/or normalize data stored in the systems; and 7) Definition of the capacity for storing historical data that can be used when producing specific information/results.

4.3.2. Data Dictionary specification

In this specific scope, the concept of Data Dictionary refers to the set of files that store all the data introduced in the various interface systems and collected in an automated way, and which are necessary to respond to business requirements. Therefore, it is necessary that when defining data dictionaries, the following questions should be considered: 1) Guarantee that data is stored with formal nomenclatures; 2) Framework of the data in terms of business and content; 3) Stipulation of the range of allowable values for each type of data/attribute; 4) Stipulation of admissible formats for each type of data/attribute; 5) Establishment of the relative importance of each type of data/attribute for the final result and for the business itself; 6) Assigning ownership of the data; and 7) Control criteria and mechanisms that should focus on the type of data/attribute.

During the process of analysis, specification, and modelling a solution, the data dictionaries are considered as the basis for the creation of the Data Model (central part of the entire solution), since they allow a clear perception about the data and, consequently, an easy detection of redundancies.

4.3.3. Information availability and Data Quality Control

The Information Availability and Data Quality Control process generically represents the process of transforming raw data - collected from various sources and stored in multiple repositories - into something more complete, contextual, temporal and useful, or that is, structured information. To ensure that the information provided is the most relevant, useful and accurate, it is necessary to guarantee the registration of the existing flow since the collection of a specific data and its refined representation in Information.

From an operational point of view, this record of the relationships between the Information that is consumed by the Banking Institution and the various data collected is even more critical due to the existence of multiple processes of transformation, refinement and even enrichment of that same data in order to be possible to aggregate them and really ensure that these are value added generators.

Thus, it is very relevant to create formal mappings that define the relationships between the various data (attributes) collected by the existing applications and systems and the Information that is generated based on that same data and that typically appears in the various output elements (information visualization systems, reporting, etc.).

In addition to being necessary to trace the origin of the information available, the quality of the data used for its construction is also essential.

One of the most interesting ways to guarantee data quality is the creation of Data Quality Dashboards (DQDs), based on a pre-established set of Data Quality Indicators (DQIs) duly aligned with the business and which must take into account the various characteristics of the Information: i) Opportunity; ii) Trust; iii) Accuracy; iv) Completeness; v) Relevance; vi) Accessibility; vii) Actuality; viii) Granularity; and ix) Consistency.

It will also be necessary to have a set of indicators very specific to the use of data in the Banking Sector, namely: 1) The purpose; 2) The scope of application; 3) The content; 4) The frequency of collection and use; 5) The format; and 6) The descriptive narrative.

Finally, and as a mean to guarantee a last layer of validation of the quality of the data and, consequently, of the information produced, quality criteria must be established in terms of the reports generated, which must be verified through specific tasks.

4.3.4. Data optimization assessment

In order to ensure that the data available for the creation of business Knowledge and Information, the IT and business teams should jointly assess the potential for optimization of said data and the processing, standardization, transformation and recovery. For this operation to be more efficient, the content of each of the processing workflows - optimized for each department or specific business need - must be formally registered, using schemes and descriptors.

Considering the always continuous evolution processes of existing IT solutions in the market and their increasing capacity to operate in multiplatform environments, it is important that analyses are repeatedly carried out on the potential use of new solutions that may allow to optimize processes transforming existing data or even identifying
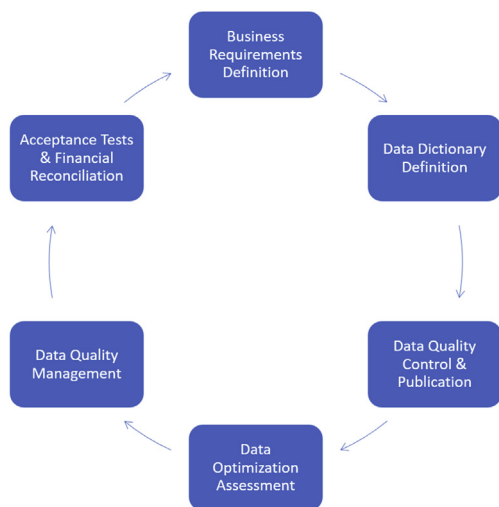

Figure 3. Proposed action-plan Interactive workflow for BCBS 239 Compliance.

potential new data processing workflows. Many of the most current solutions tend to be based on machine learning and artificial intelligence concepts and techniques, which have a very relevant capacity in terms of the analysis and validation of existing data.

4.3.5. Data profiling c data quality issues management

Data Profiling, or data profiling, is a data analysis process that aims to discover and characterize specifics of data sets (data sets). The creation of profiles allows the emergence of a view of the structure, content, rules, and relationships of the data, always based on the formal establishment of the standard characteristics of the data: types of data, maximum sizes of each attribute, cardinality of the attributes, granularity, intervals of values, existing standards (format and content), implicit rules, and relationships between columns and between files (as well as the cardinality of those relationships).

From a formal point of view, the creation of data profiles should also include the analysis of the content of the data by considering the percentage distribution of the existing values.

Distribution analysis involves counting all records associated with each value and dividing them by the total number of records in order to understand what percentage of the data is associated with a determining value and how the percentages compare. Understanding the percentages is useful, especially for sets of high cardinality values and for data sets with a large number of records.

The results of creating data profiles can be compared with the existing formal documentation regarding the expectations set for the data or they can serve as a basis for building global knowledge about the existing data.

The creation of data profiles and other ways of evaluating their quality, will allow the identification of unexpected conditions in the stored data.

These data quality issues tend to create adverse conditions (and in specific situations that even make it unfeasible) to the use of that data by a data consumer.

Managing data quality problems is a process of reducing or eliminating the impact of adverse conditions that prevent the effective use of data. In formal terms, this management includes the tasks of identification, definition, quantification, priority setting, tracking, reporting and the problem-solving task itself.

Priority setting and resolution depend on the existing data governance strategy. Here, more than ever, solving a problem means finding a solution and implementing that solution.

4.3.6. Acceptance tests c reconciliation

The activities related to the acceptance tests by the users must be carried out during the implementation phase, in the sense that it is possible to proceed not only with the identification of potential additional problems/needs, but also with the possibility of making the necessary corrective efforts.

In order to ensure that the desired outputs are achieved, the efforts of IT teams and business teams in the various testing activities must be combined. Thus, in parallel, multidisciplinary validation efforts can be developed and which, much more quickly, will be able to achieve appropriate solutions.

The tests carried out must be based on a set of pre-established metrics and must ensure that the results achieved are in line with these metrics (although there may, and should, be an acceptable margin of error).

The last step for the validation of the outputs and data (treated, standardized and valued, etc.) that serve as a basis, data analysts must, in collaboration with the businesspeople who establish the criteria, build a Reconciliation Report. This report should be produced regularly in order to ensure, on a routine basis, that the data in the repositories and which serve as the basis for the developed outputs are in line with the existing accounting data (typically considered the "only source of truth").

4.4. Proposed action plan conceptual validation and discussion

Even thou multiple individual initiatives have been performed to ensure banks become compliant with Basel's Committee BCBS 239 guidelines, to the best of our knowledge there isn't one approach that is consensually considered as a baseline guidance for easily reaching compliance. Hence, considering this global mindset, we thrived the development of a novel and valuable approach that could be widely applied by the banking sector when pursuing BCBS 239 compliance.

In order to ensure perfect alignment with Gregor and Hevner (2013) DSR-based methodology, the development, tunning and assessment of the posed artifact (in this case, an "action plan"), has been made together with the IS experts and some of the Portuguese banking sector prominent stakeholders. This group of experts was gathered in multiple online work sessions, where their concerns, doubts and expectations on both BCBS 239 and the proposed artifact, were given voice. This feedback was then analysed and taken in consideration when tunning the novel beta-versions of the action plan. In order to reach a level of consensual agreement, multiple iterations were made. The stoppage moment happened only when both the experts and the research team mutually considered the proposed action plan as a stable and a valuable contribute for reaching BCBS 239 compliance.

After reaching a comfortable maturity level, the proposed BCBS 239 compliance action plan, composed of six cyclic phases that go from the business requirements definition to the performance and documentation of acceptance tests and overall financial reconciliation, it was then presented to multiple high-management and c-level executives from Portuguese banks that analysed it and reached a set of interesting considerations and some concerns.

If, on one hand they completely agree that the majority of past initiatives that aimed to reach BCBS 239 compliance failed due to a misalignment between the established requirements and the actual business (current and future) needs, and so an initial phase totally devoted to accurately and cooperatively identify and details the business requirements inherent to the become BCBS 239 compliant, on the other hand they highlight that this activity must be done with extreme care, as it involves multiple departments and multiple directive structures that might not be exactly focused on the same goals at that precise moment.

Another keen aspect that has been highlighted as important is the fact that the proposed action plan contemplates a detailed contextualization of the Information Quality concept and the straightforward identification of the multiple perspectives from which data should be perceived in the banking sector. This feature represents a focused answer to one of the most prominent issues when managing information or data in a big organization: the existence of multiple individual definitions for the same concepts.

Considering the wide scope of the data generated and managed by banks, the abovementioned banking experts and executives stated that the inclusion of an activity strictly aimed at establishing data profiles will certainly help banks to further detail the multiple structures, rules, and relations between data and, by inherence, allow for a more efficient validation, management and use of that same data. However, and despite perceive this as a positive point, the referred experts also highlighted that the identification and characterization of each data profile might be a complex activity that, in order to be successful, must be considered of high priority and, consequently, be the focus of a considerable set of capable and experience human resources.

When addressing the "Acceptance Tests & Financial Reconciliation", the abovementioned experts stated a brief consideration on the level of expertise that was inherent to the activities typically enrolled in this phase, and that this should be taken in consideration to the point of, in some cases, banks would need to create teams specially committed to their execution.

5. Conclusions

The enforcement of risk management guidelines and regulations that ensure that the financial markets would not endure, once again, in a social and economic worldwide hecatomb, must be applauded and, if possible, transversely impregnated throughout banks organogram. Despite its merits, the existing normative is not only extremely technical, but also very difficult for banks to implement and, thus, ensuring compliance. Adding to these issues, there is a recognized (practical and theoretical) knowledge gap that impairs both the banks' operations departments and the decision-making and administration boards.

By acknowledging data as, possibly, the most relevant asset to their business success and continuity, the banking sector must be empowered to not only make better use of their (master)data, but to ensure that it is maintained and managed in accordance with all best practices already established.

5.1. Impacts on research and practice

The study consolidates existing theory on Basel Committee 239 regulation, namely by merging literature focusing, on one hand, the principles that compose the standard and, on the other hand, the suggested individual best-practices for implementing it. Hence, for researchers performing their efforts on studying the risk management topic, and particularly for those evaluating the decisive role of banking compliance assurance as a mean to safeguard that the banking sector remains stable and operational, our research serves the purpose of delivering, in a simple and straightforward manner, not only an overview on the abovementioned topics, but also a set of existing streams of research that are currently being addressed.

In parallel, we also deliver an intensive theoretical analysis to the Master Data Management concept framework, its overall importance, already proven implementation styles and approaches, and also discuss on the alignment that must exist between MDM and Data Governance. For researchers, this work might serve as the basis for establishing novel hypothesis on both the practical implementation of MDM initiatives supported by structured Data Governance approaches, and on the adoption, by the banking sector, of these two concepts as one combined approach.

Most of the existing literature on risk management associated with the banking sector tends to focus on the existing standards, regulations, and monitoring policies, and on the IT-related technical aspects behind the implementation of IST that allow for a solid management of existing data. On a novelty note, with this research we present a solid argument on how data is currently the main asset of the banking sector, and that structured master data management initiatives are mandatory for achieving compliance with existing norms and regulations. If existing master data is well structured and has a well-defined storage, ownership, integration, and use, then it will be of extreme usefulness to both business continuity, and quality and compliance assurance necessities.

By drawing our efforts on solid scientific and grey literature, thus ensuring a vertical incorporation of both theoretical and practical knowledge on our research methodology and activities, a novel approach for ensuring banks compliance with existing risk management guidelines and regulations has been outlined. This approach is composed by a six-phase (continuous) workflow, that was drawn to be implemented in a straightforward manner, goes from an initial business requirements analysis to a set of linear data optimization assessment and data quality management tasks, and to a set of acceptance tests and financial reconciliation activities. Hence a considerably important practical contribute.

Considering the iterative manner in which the proposed artifact was developed and tunned, and the feedback that resulted from its discussion with both some of the most prominent Portuguese bank's c-level executives and directive bodies, when fully absorbing the proposed action plan, banks are more capable of ensuring the necessary adaptation and (evolutionary) changes that will lead them to be fully compliant with regulations such as the BCBS 239.

Furthermore, our research also contributes for the development of regulatory bodies awareness on the already proven difficulties and constraints on not only implementing the published standards and regulations, but also on the very interpretation of its content and of its contextual perspectives. Hence, this might serve as a mediator input for future standards, guidelines and regulations for the banking sector.

5.2. Limitations and future research

To the best of our knowledge, the presented arguments are a novel contribute to both theory and practice. Nevertheless, we recognized that further research should be performed in order to ensure an on-sight application, tunning and validation of the proposed BCBS 239 compliance action-plan, and consequently a correct management and manipulation of both master data and risk related data. This future research should be performed through the collaboration with multiple banks of different dimensions and with activities in various countries within the European Union scope. Hence, after careful consideration of our study contributes and perspective limitations, we have prospected two future research lines: 1) Despite the proposed artifact methodologically supported genesis, it was yet to ensure its practical value as no practical validation of its guidelines has taken place. Hence, as future research we to believe that the practical validation (and potential improvement) of the proposed action plan by implementing case studies in multiple banks should bring interesting insights not only to its present condition but also to its potential evolution; and 2) considering the compliance with BCBS 239 is closely dependent on the adoption of efficient and effective data management and manipulation behaviours by banking staff, it would be of great interest to further study what triggers and influences their attitudes and behaviour towards data.

Declarations

Author contribution statement

José Martins; Henrique Mamede & José Correia: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Wrote the paper.

Data availability statement

The data that has been used is confidential.

Declaration of interests statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

Abraham, R., Schneider, J., vom Brocke, J., 2019. Data governance: a conceptual framework, structured review, and research agenda. Int. J. Inf. Manag. 49, 424–438.

Aithal, P.S., 2016. Ideal banking concept and characteristics. Int. Res. J. Manag. IT Soc. Sci. 3 (11), 46–55.

Al-Ruithe, M., Benkhelifa, E., Hameed, K., 2019. A systematic literature review of data governance and cloud data governance. Personal Ubiquitous Comput. 23 (5), 839–859.

Alhassan, I., Sammon, D., Daly, M., 2018. Data governance activities: a comparison between scientific and practice-oriented literature. J. Enterprise Inf. Manag. 31 (2), 300–316.

Amir, D., Pierre, B., Jan, K., 2019. Enticing the IT crowd: employer branding in the information economy. J. Bus. Ind. Market. 34 (7), 1403–1409.

Avantage Reply, 2016. BCBS239 - Practical Implementation Issues.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A., Rossi, M., 2018. Design science research contributions: finding a balance between artifact and theory. J. Assoc. Inf. Syst. Online 19 (5), 3.

Banco de Portugal, 2019. Análise temática sobre qualidade de dados (BCBS 239): conclusões preliminares. Banco de Portugal - Unidade de Inovação e Tecnologia. https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/workshop_2019_7_bcbs_239_algumas_conclusoes_deep_dive_risco_tic_-_qualidade_de_dados.pdf.

BIS, 2013. Principles for Effective Risk Data Aggregation and Risk Reporting. https://www.bis.org/publ/bcbs239.pdf.

BIS, 2018. Progress in Adopting the "Principles for Effective Risk Data Aggregation and Risk Reporting. https://www.bis.org/bcbs/publ/d443.pdf.

Brocke, J. vom, Hevner, A., Maedche, A., 2020. Introduction to Design Science Research, pp. 1–13.

Broeders, H., Khanna, S., 2015. Strategic Choices for banks in the Digital Age, vol. 7. McKinsey & Company.

Brown, C.O., Dinç, I.S., 2011. Too many to fail? Evidence of regulatory forbearance when the banking sector is weak. Rev. Financ. Stud. 24 (4), 1378–1405.

Capgemini, 2015. Master Data Management for Banking. https://www.capgemini.com/wp-content/uploads/2017/07/mdm_for_banking_2015_v2_print.pdf.

Chiang, R.H.L., Grover, V., Liang, T.-P., Zhang, D., 2018. Special issue: strategic value of big data and business analytics. J. Manag. Inf. Syst. 35 (2), 383–387.

Côrte-Real, N., Oliveira, T., Ruivo, P., 2017. Assessing business value of big data analytics in European firms. J. Bus. Res. 70, 379–390.

Dill, A., 2019. Bank Regulation, Risk Management, and Compliance: Theory, Practice, and Key Problem Areas. Taylor & Francis.

Dreibelbis, A., 2008. Enterprise Master Data Management: an SOA Approach to Managing Core Information. Pearson Education India.

ECB, 2018. Report on the Thematic Review on Effective Risk Data Aggregation and Risk Reporting.

Edwards, J., Wolfe, S., 2004. The compliance function in banks. J. Financ. Regul. Compl.

Elhassouni, J., El qadi, A., El alami, Y. E. madani, El haziti, M., 2020. The implementation of credit risk scorecard using ontology design patterns and BCBS 239. Cybern. Inf. Technol. 20 (2), 93–104.

Fan, W., Ma, S., Tang, N., Yu, W., 2014. Interaction between record matching and data repairing. J. Data Infor. Qual. (JDIQ) 4 (4), 1–38.

Galhardas, H., Torres, L., Damásio, J., 2010. Master Data Management: A Proof of Concept. ICIQ.

Garousi, V., Felderer, M., Hacaloğlu, T., 2017. Software test maturity assessment and test process improvement: a multivocal literature review. Inf. Software Technol. 85, 16–42.

Gartner, 2018. Master data management (MDM). In: Gartner Glossary. https://www.gartner.com/en/information-technology/glossary/master-data-management-mdm.

Geiger, J., 2007. Ensuring Quality Data; There are several dimensions of quality that need to be evaluated for each data element. These include accuracy, completeness, uniqueness, structure, timeliness and value distribution. Inf. Manag. 17 (1), 43.

Ghasemaghaei, M., Calic, G., 2019. Can big data improve firm decision quality? The role of data quality and data diagnosticity. Decis. Support Syst. 120, 38–49.

Gilbet, T., Lajkep, K., 2020. Implementing BCBS 239, what does it take? https://www.finalyse.com/blog/implementing-bcbs239.

Gillet, T., Lajkep, K., 2020. Implementing BCBS239, what does it take?.

Gregor, S., Hevner, A.R., 2013. Positioning and presenting design science research for maximum impact. MIS Q. 337–355.

Haneem, F., Kama, N., Taskin, N., Pauleen, D., Bakar, N.A.A., 2019. Determinants of master data management adoption by local government organizations: an empirical study. Int. J. Inf. Manag. 45, 25–43.

Harreis, H., Ho, T., Machado, J., Merrath, P., Rowshankish, K., Tavakoli, A., 2017. Living with BCBS 239. https://www.mckinsey.com/business-functions/risk/our-insights/living-with-bcbs-239.

Hashem, I.A.T., Yaqoob, I., Anuar, N.B., Mokhtar, S., Gani, A., Khan, S.U., 2015. The rise of "big data" on cloud computing: review and open research issues. Inf. Syst. 47, 98–115.

Hevner, A., Chatterjee, S., 2010. Design science research in information systems. In: Design Research in Information Systems. Springer, pp. 9–22.

Ibrahim, A., David, S., Mary, D., 2018. Data governance activities: a comparison between scientific and practice-oriented literature. J. Enterprise Inf. Manag. 31 (2), 300–316.

Informatica, 2020. Master Data Management - what it Is and Why it Matters. https://www.informatica.com/resources/articles/what-is-master-data-management.html.

Kaminski, P., Robu, K., 2016. A Best-Practice Model for Bank Compliance. https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-for-bank-compliance.

KPMG, 2016. BCBS 239: Bracing for Change and Capturing the Opportunity. https://assets.kpmg/content/dam/kpmg/pdf/2016/03/BCBS-239-Bracing-for-change-and-capturing-the-opportunity.pdf.

Ladley, J., 2019. Data Governance: How to Design, Deploy, and Sustain an Effective Data Governance Program. Academic Press.

Leonelli, S., 2019. Data governance is key to interpretation: reconceptualizing data in data science. Harv. Data Sci. Rev. 1 (1).

Li, J., Feng, J., Sun, X., Li, M., 2012. Risk integration mechanisms and approaches in banking industry. Int. J. Inf. Technol. Decis. Making 11 (6), 1183–1213.

Liu, Y., Liu, H., Yang, F., Chen, X., 2020. Application of master data classification model in enterprises. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol. 1, pp. 1989–1993.

Loshin, D., 2010. Master Data Management. Morgan Kaufmann.

Lukas, P., Hubert, P., 2015. Solutions for risk data compliance under BCBS 239. J. Invest. Compl. 16 (1), 66–77.

Lux, C., 2014. BCBS 239 – its time to get back to banking basics. Glob. Bank. Finance Rev. https://www.globalbankingandfinance.com/bcbs-239-its-time-to-get-back-to-banking-basics/.

Ofner, M.H., Straub, K., Otto, B., Oesterle, H., 2013. Management of the master data lifecycle: a framework for analysis. J. Enterprise Inf. Manag.

Orgeldinger, J., 2018. The implementation of Basel committee BCBS 239: short analysis of the new rules for data management. J. Cent. Bank Theor. Pract. 7 (3), 57–72.

Otto, B., 2012. How to design the master data architecture: findings from a case study at Bosch. Int. J. Inf. Manag. 32 (4), 337–346.

Paananen, J., 2020. A New Data Governance Model for the Bank of Finland. Metropolia University of Applied Sciences. https://www.theseus.fi/bitstream/handle/10024/349729/Paananen_Jukka-Pekka.pdf.

Parviainen, P., Tihinen, M., Kääriäinen, J., Teppola, S., 2017. Tackling the digitalization challenge: how to benefit from digitalization in practice. Int. J. Infor. Syst. Project Manag. 5 (1), 63–77.

Piedrabuena, F., González, L., Ruggia, R., 2015. Enforcing data protection regulations within e-government master data management systems. ICEIS (3), 316–321.

Pilger, A., Maldonado, J., 2017. BCBS 239 a Long Road to Compliance. https://www.finalyse.com/blog/bcbs.

Profisee, 2020a. Data Governance – what, Why, How, Who & 15 Best Practices. Profisee - Trust Your Data. https://profisee.com/data-governance-what-why-how-who/.

Profisee, 2020b. Master Data Management - what, Why, How & Who. Profisee - Trust Your Data. https://profisee.com/master-data-management-what-why-how-who/.

Prokhorov, I., Kolesnik, N., 2018. Development of a master data consolidation system model (on the example of the banking sector). Procedia Comput. Sci. 145, 412–417.

Raguseo, E., 2018. Big data technologies: an empirical investigation on their adoption, benefits and risks for companies. Int. J. Inf. Manag. 38 (1), 187–195.

Rasouli, M.R., Trienekens, J.J.M., Kusters, R.J., Grefen, P.W.P.J., 2016. Information Governance Requirements in Dynamic Business Networking. Industrial Management & Data Systems.

Risto, S., Olli, J., Hanna, K., Harri, H., 2011. Managing one master data – challenges and preconditions. Ind. Manag. Data Syst. 111 (1), 146–162.

Spruit, M., Pietzka, K., 2015. MD3M: the master data management maturity model. Comput. Hum. Behav. 51 (part B), 1068–1076.

Tallon, P.P., Ramirez, R.V., Short, J.E., 2013. The information artifact in IT governance: toward a theory of information governance. J. Manag. Inf. Syst. 30 (3), 141–178.

Townsend, M., Le Quoc, T., Kapoor, G., Hu, H., Zhou, W., Piramuthu, S., 2018. Real-Time business data acquisition: how frequent is frequent enough? Inf. Manag. 55 (4), 422–429.

Valladares, M., 2018. Why the Basel Committee's William Coen Is Impacting Global Banking Reform. https://www.forbes.com/sites/mayrarodriguezvalladares/2018/09/03/basel-committees-william-coen-is-instrumental-to-global-banking-reform/?sh=3c17f71c2531.

Vilminko-Heikkinen, R., Pekkola, S., 2017. Master data management and its organizational implementation. J. Enterprise Inf. Manag.

Weresa, M.A., 2019. Technological competitiveness of the EU member states in the era of the fourth industrial revolution. Econ. Bus. Rev. 5 (3), 50–71.

White, A., Newman, D., Logan, D., Radcliffe, J., 2006. Mastering Master Data Management. Gartner Group, Stamford.

Woo, K., 2019. Operational or Analytical MDM – Which Is Right for You? https://qmetrix.com.au/operational-or-analytical-master-data-management/.

Xyloyiannis, C., 2017. Supplier Master Data Management – Analytical or Operational MDM? https://www.hicx.com/supplier-master-data-management-2/.

Yu, X., Tao, Y., Tao, X., Xia, F., Li, Y., 2018. Managing uncertainty in emerging economies: the interaction effects between causation and effectuation on firm performance. Technol. Forecast. Soc. Change 135, 121–131.