LEPUS

BCBS 239: Strategies and Capabilities

Sponsored by:

informatica

Put potential to work.™

BCBS 239: Strategies and Capabilities

The implications of regulatory reforms on global financial markets have never been greater. In response to the global financial crisis, the Basel Committee issued several principles for devising a sound risk management system with references to data aggregation. Efforts to improve the ability of banks to aggregate risk data is primarily aimed at restoring the strength and viability of global markets, enabling firms to better withstand future episodes of economic distress; a notion that is widely accepted by banking institutions[1].

Despite recognizing these benefits, in order for banks to comply with these principles successfully, they need strong risk governance processes that are supported by enhanced data, strong data governance program, as well as sound data integration and management technology infrastructure; requiring significant investment by many institutions. Furthermore, risk governance processes should be coupled with efficient strategies to eliminate redundancies across data initiatives and develop a single data management framework to meet multiple business needs and regulatory demands[2]. These are critical investments that must be addressed to meet the January 1, 2016 deadline set by the Basel Committee and FSB. With this in mind, banks are seeking to facilitate the use of more consistent and granular data, as well as proven technology solutions to more effectively manage risks and grow their business models[3].

All in all, banks are facing increasing pressure from regulators to improve their reporting capabilities, with the Basel Committee's *Principles for effective risk data aggregation and risk reporting* (BCBS239)[4], released in January 2013, is a particular point of focus at present.

This report, based on a survey of 27 major financial institutions, from diversified geographical regions, explores existing capabilities and strategies being taking to comply with the BCBS 239 principles. In doing so, it analyses the following areas:

---

1 Institute of International Finance (2011), *Risk IT and Operations: Strengthening capabilities,* Report (June 2011).

2 Ernst & Young (2012), *financial regulatory reform - What it means for bank business models*, Report (November 2012).

3 Camhi, J. (2013), "Big Data: Where to Begin?" Bank Systems and Technology, available at: http://www.banktech.com/business-intelligence/big-data-where-to-begin/240152033 (accessed on 03 March 2014).

4 Basel Committee on Banking Supervision (2013), "Principles for effective risk data aggregation and risk reporting", BIS Report No. BCBS239, January 2013, available on: http://www.bis.org/publ/bcbs239.pdf (accessed on 27 Feb 2014).

- **Data aggregation capabilities;**
- **Data quality;**
- **Counterparty risk transparency;**
- **Data transparency and business comprehension; and**
- **Risk data initiatives.**

Data Aggregation Capabilities

Data aggregation is the transfer of data from one system to other using different mechanisms; such as, hand coded ETL processes, non-enterprise class data integration tools and Web services. However, existing processes raise many concerns as banks come under pressure from increasing data demands and regulatory changes. As such, it is recommended that banks consider making strategic investments in proven data integration technologies to capture, govern, and deliver required data for BCBS 239 compliance.

BCBS 239 sets a challenging standard for risk data aggregation and reporting for all Globally Systemic Important Banks (GSIB). Firms striving to comply with this standard will be keen to understand how risk data is organised and what execution capabilities are at their disposal. The Bank of International Settlements' (BIS) study[5] into existing data integration capabilities reveals that financial institutions are fully aware of the problems faced in this space. The study indicated that some of the key weaknesses around existing data aggregation capabilities boil down to the following factors[6]:

- Manual workarounds;
- Lack of a holistic view of risk;
- Flawed risk data governance processes;
- Opaque definitions of data ownership;
- Incomplete and inconsistent counterparty information;
- Weak controls around data quality assurance; and
- Not enough documented policies and procedures around risk data aggregation.

Complementing the aforementioned factors, it turns out that none of the banks participating in this research are fully satisfied with the completeness of data required for modelling and reporting at their respective firms. The majority of banks, 59%, indicate the need for improvement in this area, while the remaining 41% require

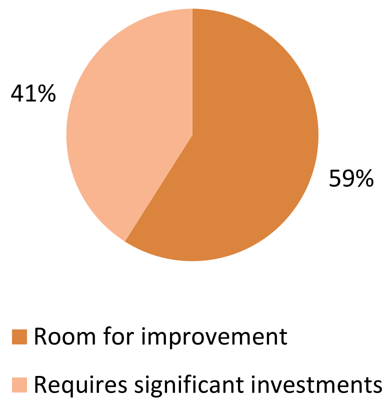
---

[5] Basel Committee on Banking Supervision (2013), "Progress in adopting the principles for effective risk data aggregation and risk reporting", BIS Report No. BCBS268, December 2013, available on: https://www.bis.org/publ/bcbs268.pdf (accessed on 25 Feb 2014).

[6] Danko, J. (2014), "Risk Data Aggregation & Risk Reporting: Will You Be Compliant With BCBS 239 Principles In Time?", The Financial Services Blog (Oracle), February 2014, available at: https://blogs.oracle.com/financialservices/entry/effective_risk_data_aggregation_risk (accessed on 25 Feb 2014).

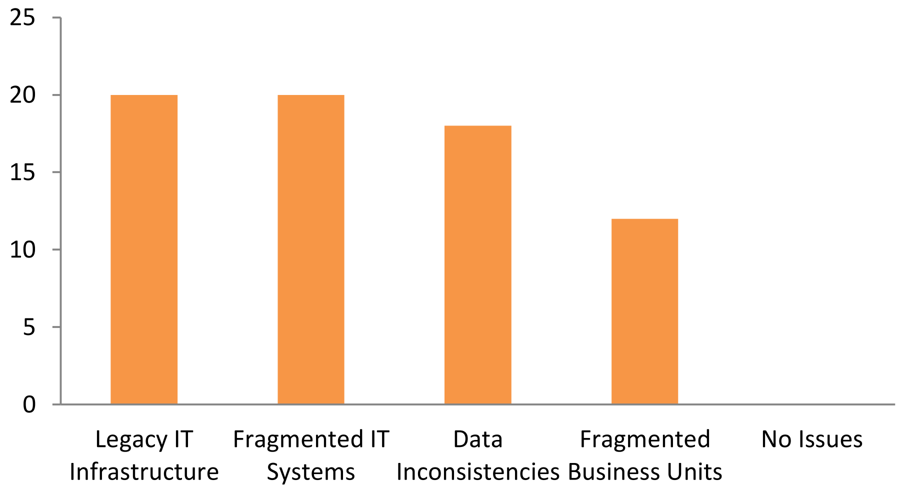
significant investments in order to address the issue of data completeness, as illustrated in Figure 1**.**

Figure 1: How satisfied are you with how complete the data required for modelling and reporting is at your firm at present?



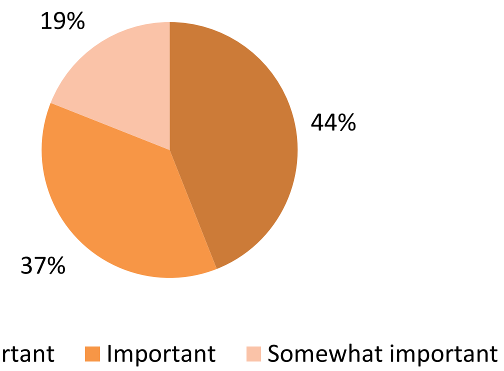
A regional breakdown of the surveyed banks suggests that UK and US institutions tend to be more critical of their progress in obtaining a complete view of risk. Similar discrimination applies to tier-1 global banks that are more likely to indicate the need for significant investments to improve existing data integration capabilities. In sum, all of the surveyed banks are facing challenges in their data integration and collection processes required to support existing risk management frameworks and compliance needs. As shown in Figure 2, legacy IT infrastructure, data inconsistencies and fragmented IT systems pose key challenges to the overwhelming majority of the participating banks. Interestingly, fragmented business units have a less pronounced impact on data collection and aggregation processes across the surveyed banks.

Figure 2: What technical challenges still remain with the data collection and integration processes required to support your risk management and compliance needs?



Complementing these findings, it is worth noting that several participating banks highlighted 'Other', bank-specific challenges that are not detailed in the above figure. To this point, problems have been associated with existing data quality gaps, integrity measures, ownership, and overly bureaucratic technology groups. Against this backdrop, all of the banks are making efforts to overcome challenges rooted in data integration and aggregation processes. As it transpires, the majority of the surveyed banks find it highly important or important to address their data integration gaps to fulfil arising business needs. As shown in Figure 3, none of the participating banks ignore the importance of reconciling data integration gaps.

Figure 3: How important is it to address your data integration gaps to fulfil your business needs?

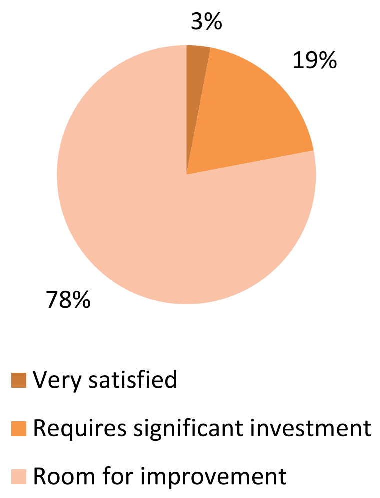


Data Quality

The Basel Committee has suggested that banks must resolve any limitations pertaining to risk IT systems that support data quality. Furthermore, regulators require banks to have an accountability function or governance program set out to identify, manage, and monitor ongoing levels of data quality. Banks are also required to ensure that data quality checks are satisfactorily robust, documented, and measured. All in all, if banks are willing to produce high quality risk data, they are advised by the Basel Committee to build up strong risk data governance and architecture, coupled with robust data integration and aggregation capabilities. Thus, it is imperative for banks to establish independent functions validating their data aggregation processes. According to the Basel Committee, data quality remains a critical area for improvement in terms of unifying and rationalising the dictionaries and taxonomies of risk data repositories, as well as establishing quality controls over risk data.

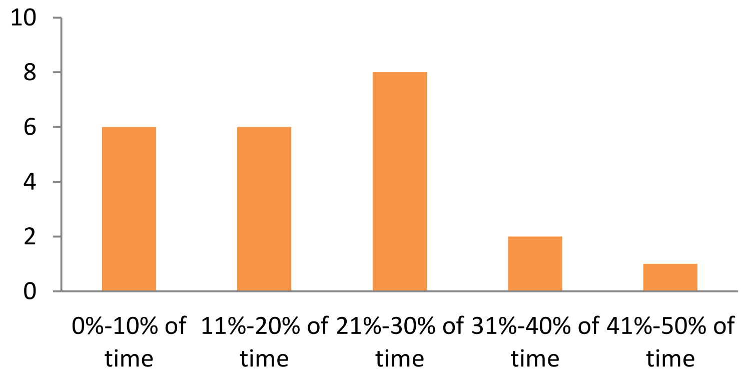
As shown in Figure 4, only 3% of banks are very satisfied with their data quality management frameworks and ways they ensure that Risk and Compliance obtain trustworthy data with which to make decisions. The vast majority of the surveyed banks, 78%, see room for improvement in delivering sufficiently robust data for Risk and Compliance, while a further 19% of banks require significant investments in this space.

Figure 4: How satisfied are you that your data quality management frameworks are sufficiently robust to ensure that Risk and Compliance have trustworthy data to base decisions on?



A growing number of tools and techniques can be used to support data quality management frameworks in order to ensure that Risk and Compliance departments receive reliable data[7]. We received mixed responses from the surveyed banks regarding the time spent on fixing data quality issues in Risk and Compliance systems. As it transpires, the percentage of user time varies from 5% to 50% across the participating banks. A significant 44% of the surveyed banks usually devote 30-35% of user time on amending data quality, while a further 33% dedicate 20-25% of their time to addressing key issues around data quality. A more detailed breakdown is provided in Figure 5, below.

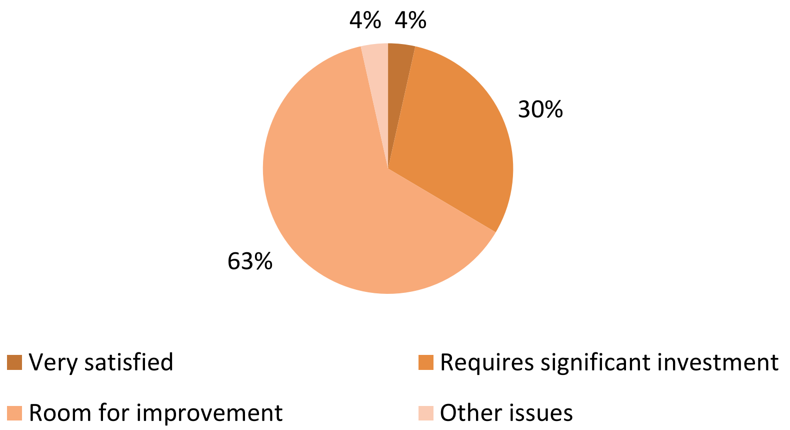
Figure 5: Approximately what percentage of user's time is spent fixing data quality issues in existing risk and compliance systems?



[7] Marotta, P.A. (2013), "Data-Management and Data-Quality Best Practices", *Verisk Review*, Vol. 11 (Fall 2013).

Furthermore, only 4% of banks are currently satisfied with the tools being used to identify and manage data quality. At this point, 30% of the surveyed banks seek significant investments in this area, with 4% of the banks stating that tools identifying and managing data quality are non-existent. The same bank is also spending the largest amount of time (50%) on fixing data quality issues in its Compliance and Risk systems. The overwhelming majority of the participating banks indicate room for improvement with the application of dedicated tools to manage data quality, as illustrated in Figure 6.

Figure 6: How satisfied are you with the current tools used to identify and manage data quality?



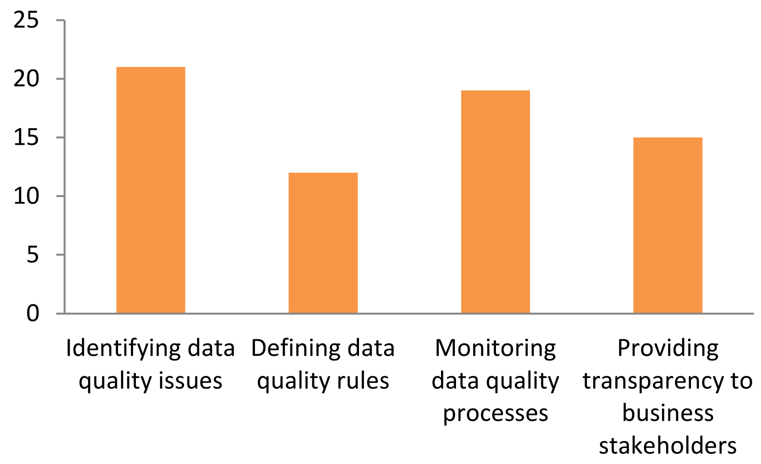
Data quality was found to be a key risk management issue in the banking sector long before the global financial crisis and publication of BCBS 239. The surveyed banks have indicated several, bank-specific issues centred on ensuring that data quality meet BCBS 239 requirements. To this point, data quality is hampered by the ad-hoc intervals for niche and exotic portfolios, as well as the manual delivery systems that don't use the same data hierarchies. Against this backdrop, according to Informatica (2014)[8], banks tend to invest heavily in data governance programs in order to improve data quality management. These programs are supported by specific roles, processes, standards and policies. However, in doing so, banks are believed to engage in manual data management as well as using unproven open-source tools for data quality processes. IT experts argue that these choices prevent banks from benefiting from past data governance investments and hinder compliance with BCBS 239 principles.

As shown in Figure 7, 78% of the surveyed banks see identifying data quality issues as the most important aspect of managing data quality and meeting business needs. In addition to this, monitoring the performance of ongoing data quality processes has been found equally important by 70% of the participating banks. Defining data quality rules constitutes the least important aspect of managing data quality with only 44% of the banks indicating its importance. Similarly, providing transparency to business stakeholders in data quality processes is regarded as most important to fit business needs only by 56% of the participating banks.

---

[8] Informatica (2014): http://www.informatica.com/uk/solutions/industry-solutions/banking-and-capital-markets/data-quality-and-governance-for-risk-management-and-compliance/

Figure 7: What aspects of managing data quality are most important to your business needs?



Counterparty Risk Transparency

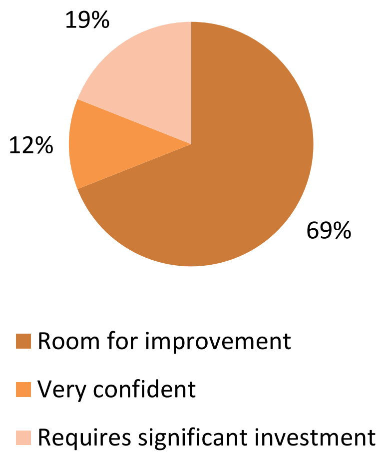
According to the Basel Committee's principles for effective risk data aggregation and risk reporting[9], any bank must generate up-to-date risk data in a timely manner while aiming for the best accuracy, integrity, completeness and adaptability. The Basel Committee acknowledges that different types of data require different, time-varying approaches, and that counterparty credit risk exposures may be needed faster in a stressed situation. Therefore, banks are advised to build their risk systems to be fully capable of producing aggregated risk data in a timely manner during episodes of financial crises.

The global financial crisis divulged that banks lacked the ability to aggregate counterparty risk exposures and were unable to identify concentrations of counterparty risk in a timely manner, and with sufficient levels of accuracy. This failure was evident across business lines and between legal entities, as well as at the group level. As shown in Figure 8, the majority of the surveyed banks still see room for improvement in relation to effectively utilising counterparty and legal entity data. All in all, around 80% of respondents are not entirely confident that their master and reference data is adequate to measure and monitor counterparty risk.

---

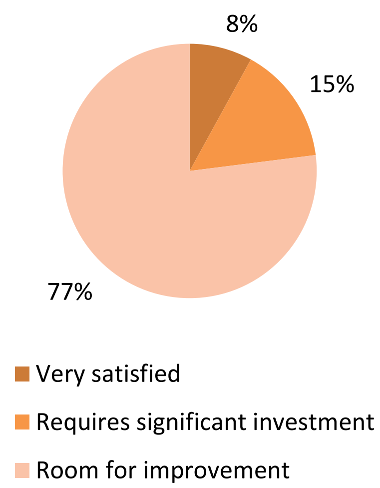
[9] Basel Committee on Banking Supervision (2013), "Principles for effective risk data aggregation and risk reporting", BIS Report No. BCBS239, January 2013, available on: http://www.bis.org/publ/bcbs239.pdf (accessed on 27 Feb 2014).

Figure 8: How confident are you that your counterparty and legal entity master and reference data to measure and monitor counterparty risk?



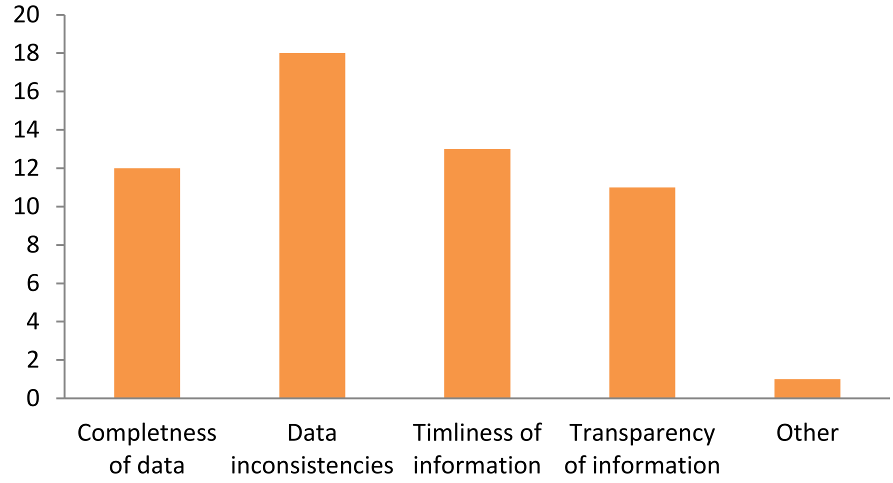
It is expected that the participating banks, which indicated a need for improvement or significant investments in counterparty and legal entity data, would indicate similar requirements for the quality and completeness of their counterparty/legal entity hierarchy information. However, the survey reveals that over 90% of the surveyed banks are less than satisfied with their counterparty entity hierarchy. As shown in Figure 9, the overwhelming majority of the participating banks require improvements in the quality and completeness of relevant counterparty risk data. At this point, only 8% of the surveyed banks are satisfied with their data for counterparty/legal entity hierarchy information.

Figure 9: How satisfied are you with the quality and completeness of your counterparty/legal entity hierarchy information?



While un-aggregated counterparty risk data is relatively easy to generate, it is not necessarily that straightforward to integrate, enrich, aggregate and distribute in a reliable, robust and timely fashion[10]. Figure 10 indicates the main concerns in this area across the participating banks.

Figure 10: What concerns do you have about your existing counterparty information in terms of complying with BCBS 239?



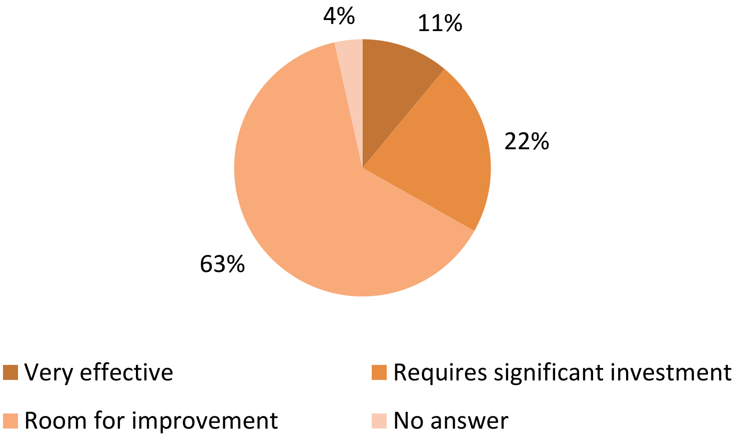
The above figure reveals that data inconsistencies constitute a key concern for the participating banks seeking to ensure that counterparty risk data is compliant with BCBS 239. Going further, completeness of data, timeliness and transparency of information have been found problematic by 40-45% of the surveyed banks. One bank has also pointed to the lack of measurement for completeness and integrity of relevant data to ensure compliance with BCBS 239.

Data Transparency and Business Comprehension

This section investigates how well the surveyed banks manage data transparency and business comprehension in order to assess key risks and comply with existing regulations. As shown in Figure 11, 11% of the surveyed banks are very effective in tracing and reporting on the manner in which data is collected, processed, transformed and calculated in compliance with regulatory requirements. However, the majority of the surveyed banks, 63%, still see room for improvement in this area. Moreover, 22% of the participating banks require significant investments to effectively trace and report on how data is collected and processed for regulatory purposes.

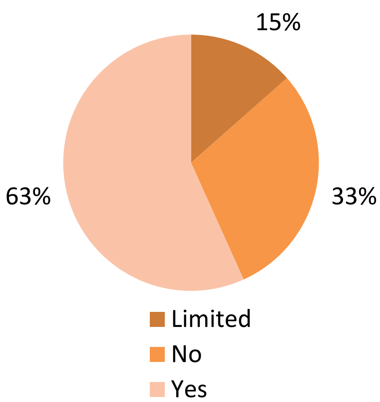
[10] Som, S. (2014), "Getting Ready For BCBS 239 - Aggregating And Reporting Risk Data Effectively", Financial IT blog, *Innovations in Technology*, 05 Feb 2014, available at: http://www.financialit.net/ (accessed on 27 Feb 2014).

Figure 11: How effective is your organization's ability to trace and report on data in order to satisfy regulatory requirements?



Metadata is the fastest-growing category of data in the banking industry. However, banks need to be smart about the approach they take and which metadata they capture. Furthermore, it is argued that banks should develop more practical approaches to tackling risk identification of exposed sensitive content. At this point, banks need to capture metadata non-intrusively by limiting service disruptions. There is a need for an effective normalisation of metadata so that analysis, computation, and storage are possible while still presenting meaningful, actionable information for decisive action and review[11]. Against this backdrop, 15% of the surveyed banks utilise metadata to a limited degree for the purpose of risk data management as compared to 52% of the participating banks that fully use metadata. At this point, one third of the surveyed banks do not utilise metadata at all for this purpose, as shown in Figure 12.

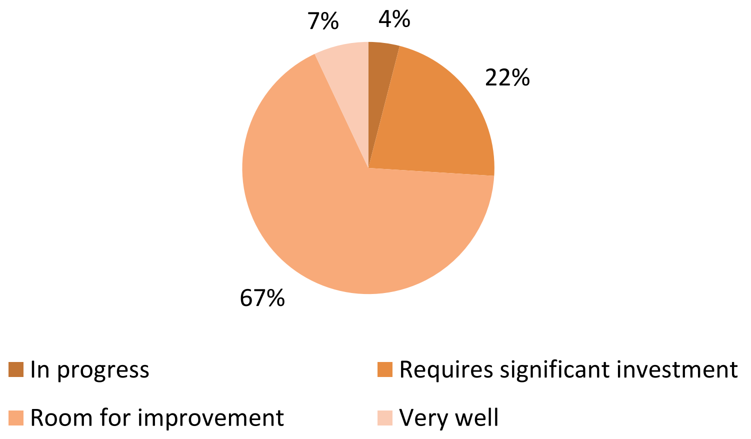
Figure 12: Does your organization utilize metadata for the purpose of risk data management?



[11] Varonis (2014), "Varonis Leads Industry Conversation on Metadata, Wins HubSpot's 30-Day Blog Challenge", Varonis Newsletter, 12 Feb 2014, available at: http://ir.varonis.com/releasedetail.cfm?ReleaseID=826387 (accessed on 28 Feb 2014).

The majority of the surveyed banks indicate the need for further improvements in managing business descriptions of risk data. As shown in Figure 13, only 7% of respondents are doing it very well, whereas 22% still require significant investments into managing business descriptions. In addition to this, one bank is in the process of linking business definitions to a meta-glossary.

Figure 13: How well does your organization manage business descriptions of the risk data?

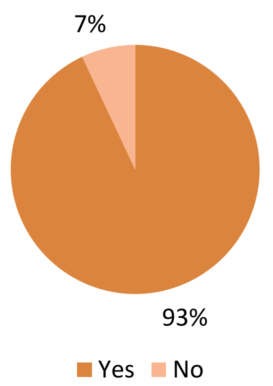


Risk Data Initiatives

The financial industry has been the subject of global regulatory changes as well as serious introspection on risk practices by banks themselves. This has led to a range of responses by banks introducing new compliance programs, governance changes and risk management rigour. These initiatives are underpinned by the need for improved capabilities in data collection, processing, reporting and analysis.

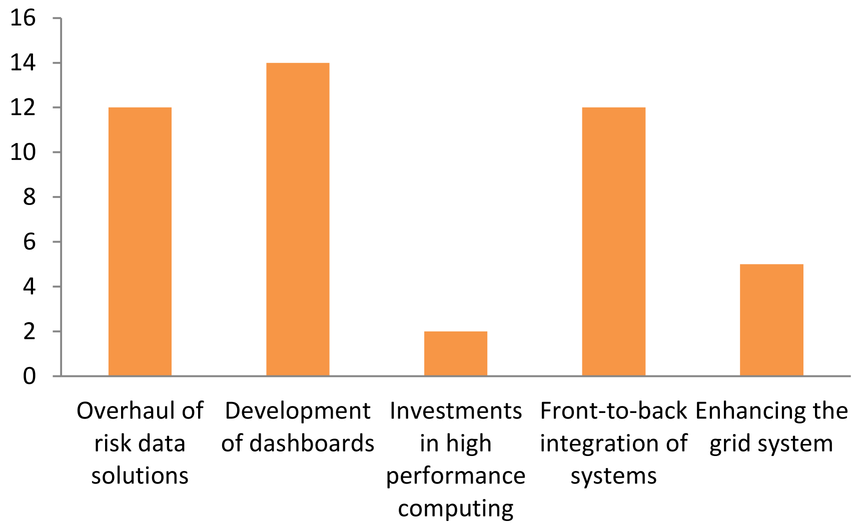
As it transpires, 93% of the participating institutions are undertaking or planning any initiatives to improve their existing risk data management and reporting technology, as illustrated in Figure 14.

Figure 14: Are you currently undertaking/planning initiatives in respect to risk data and reporting technology?



The overhaul of existing risk data solutions, development of dashboards and integration of the front-to-back systems are the most common initiatives being undertaken by the surveyed banks. As shown in Figure 15, only two banks are investing in high performance computing and a further five banks are enhancing grid systems as part of their risk data initiatives.

Figure 15: What are the main areas of focus for these initiatives?

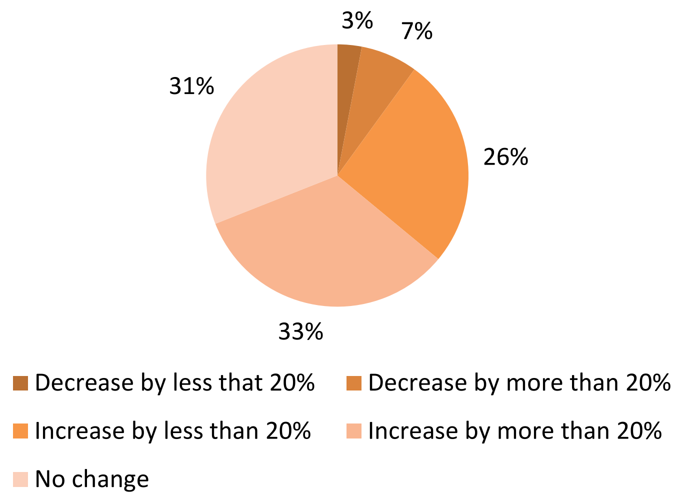


In addition to these areas of expenditure, there are a number other initiatives that are taking place at individual banks, these include:

- New Business Intelligence and Data Quality tools;
- Merging data sourced for market and counterparty risk;
- Enhancing the data integration chain;
- Providing a single front end portal for market and counterparty risk;
- reviewing inflight projects and developing new IT strategy'
- Automation of material risk reporting; and
- Developing control and governance processes.

Given the magnitude of risk data initiatives, 60% of the surveyed banks predict an increase in relevant IT investments in 2014. Only 7% of the banks see a decrease of investments in risk data and reporting by more than 20%. Moreover, Figure 16 suggests that one third of the surveyed banks would not see significant changes to IT investments supporting risk data initiatives in 2014.

Figure 16: How are investments in risk data and reporting IT changing in 2014?



Conclusion

The *Principles for effective risk data aggregation and risk reporting* (BCBS239)[12] aim to strengthen risk data aggregation and risk reporting practices at banks in order to improve risk management practices. In addition, improving banks' ability to rapidly provide comprehensive risk data by legal entity and business line will enhance banks' decision-making processes and improve their resolvability. At this point, an important question arises as to whether banks are ready for BCBS239?

As it transpires, all aspects of data capabilities and integration remain problematic. Completeness of data for modelling and reporting, as well as the implementation of dedicated tools for the identification and management of data quality constitute key areas that require significant investments. In contrast, the surveyed banks feel less concerned about the quality and completeness of their counterparty/legal entity hierarchy information, as well as counterparty and legal entity master and reference data utilised for measurement and monitoring of counterparty risk.

A brief analysis of the banks' responses indicates that the majority of the surveyed banks are currently not ready to meet BCBS 239 requirements; 63% of the participating banks require significant investments in areas of data integration, counterparty risk transparency, and data quality processes. On average, only 26% of the surveyed banks are somewhat satisfied with their compliance with BCBS 239. In addition to this, 11% of the participating banks see the need for improvement in order to be fully compliant with BCBS 239.

[12] Basel Committee on Banking Supervision (2013), "Principles for effective risk data aggregation and risk reporting", BIS Report No. BCBS239, January 2013, available on: http://www.bis.org/publ/bcbs239.pdf (accessed on 27 Feb 2014).

In summary, the surveyed banks are aware of the shortcomings associated with their data aggregation capabilities. This report has confirmed that the banks encounter problems with completeness and quality of risk data. To this end, automated processes of data aggregation are believed to improve the quality and completeness of risk data. All in all, BCBS 239 constitutes a tremendous opportunity to revise banks' structure, strategies and businesses, and consider modernizing and building out a foundation to support the data integration, data quality, reference data, and data governance needs. This will help establish a foundation to efficiently and effectively provide data and information across the entire enterprise for years to come.