Aggravation or Aggregation: Risk Data and Compliance

Sponsored by:

LEPUS

SAS
THE POWER TO KNOW.
Aggravation or Aggregation: Risk Data and Compliance

Up until the financial crisis of 2008, enterprise-wide risk data management was perceived by banks and other financial institutions as a mere utility centre. The unprecedented pace at which the crisis transformed into a monster threatening to bring down the financial system, and the scale of failures across the industry, exposed the lack of appropriate tools available to aggregate risk data efficiently. Since then, effective risk data aggregation, which sprawling multinational firms must have to achieve a holistic view of risk exposures, has become the primary point of focus for financial institutions. In response to the crisis, and in order to mitigate and contain any future episodes of economic distress, the Basel Committee on Banking Supervision (BCBS) has issued new regulations on risk data aggregation with the aim to bolster the risk IT and reporting capabilities of banks.

The Basel Committee published its Principles for effective risk data aggregation and risk reporting (BCBS239)\(^1\), in January 2013, which contains 14 core principles that Global Systemically Important Banks (G-SIBs) will need to comply with by January 2016. Furthermore, the committee also “strongly suggests” that national regulators must apply these principles to banks identified as Domestic Systemically Important Banks (D-SIBs) three years following their designation as D-SIBs\(^2\). These principles are expected to act as a mechanism to define the initiatives banks have to undertake to build and maintain more robust and effective risk management IT infrastructure. The figure below outlines these principles.

Figure 1:

---


BCBS 239 is not merely a set of principles aimed at improving data aggregation capabilities, but also encompasses a set of high-level best practices looking at a larger strategic regulatory agenda that seek to ensure that banks have adequate tools at their disposal to monitor and manage risks at the group level going forward³.

With the need to address challenges of aggregating risk data accurately and reporting it on a timely basis becoming more important than ever, implementing more responsive and flexible solutions has become paramount for financial institutions. This technical white paper, based on a survey of 27 major financial institutions, including G-SIBs and D-SIBs from diversified geographical regions such as North America, Europe and APAC, aims to explore the initiatives undertaken to comply with the BCBS 239 principles. The analysis of this research is broken down into following sections:

- BCBS 239 compliance initiatives;
- Risk data solutions;
- Risk data aggregation;
- Current state of process automation and future outlook; and
- Current progress of compliance projects.

**BCBS 239 Compliance Initiatives**

In the post crisis world, where compliance with numerous, complex regulations tops the strategic agenda of banks, formulating adequate responses within tight timeframes is proving to be tricky. In this sense, BCBS 239 constitutes a challenging task for financial institutions. Banks are now forced to understand not only the manner in which risk data should be organised and formatted, but also to evaluate the reliability and accuracy of the tools at their disposal to comply with this regulation. Clearly, banks have to significantly enhance their IT infrastructure, such as upstream systems, risk engines and reporting systems, to comply with this standard.

In terms of the approaches that banks are taking to comply with risk data initiatives, the vast majority of the surveyed institutions, 78%, are planning to make enhancements to existing solutions, rather than developing entirely new solutions; as indicated in Figure 2. The institutions that chose ‘other’ noted that they are either still assessing the impact of regulations or planning to adopt a strategy including all the three approaches mentioned in the figure below.

The fact that the majority of banks are extending existing systems rather than developing entirely new solutions throws some light on the culture and attitude towards technology at these banks. Focus still seems to largely centre on business profits and front-office requirements, rather than developing efficient reporting mechanism by infusing new infrastructure.

Some observers may rebut that argument by stating that banks don’t have the capacity or means to completely overhaul their entire risk data infrastructure, particularly in light of the tight deadline that regulators have given, and for many, extending existing solutions is simply the most pragmatic and realistic option at present. That rebuttal maybe rather too simplistic a view to be justified, as the regulatory deadline of January 2016 presents ample time and opportunity for banks to restructure and even replace their entire risk IT infrastructure. After all, the idea of this regulation is to build robust infrastructure and risk management frameworks. Extending existing solutions for short-term compliance purposes may defeat the purpose of this regulatory exercise and could point to a lack of conviction and resolve of banks to deal with risk data issues with a long term view.

With this in mind, this survey asked the participant banks to indicate the primary business drivers that their respective organisations would benefit from through BCBS 239 compliance initiatives. As detailed in Figure 3, the research finds a high degree of variation in this regard across the industry. As expected, as outlined by the BCBS 239 paper, achieving a more holistic view of organisational risks tops the charts across the participating sample. It is closely followed by expected improvements to risk analytics capabilities and risk reporting to regulators. Given the fact that there is an increased regulatory focus on stress testing for regulatory and capital planning purposes, it is interesting to see that the importance accorded to improving their stress testing capabilities is, at 22%, on the lower end of the spectrum.
Judging by the responses in Figure 2, one might argue that banks are simply following the principles laid down the regulation by taking the least disruptive and easier available solution to remain responsive and ensure better risk management. However, from a pragmatic standpoint, banks should realise that to remain connected and compliant they need to innovate. Adopting next generation technology will allow them to achieve long-term benefits and build more robust risk management frameworks. All in all, exploring options provided by new and emerging technologies can enhance risk management capabilities and profitability in the face of changing market conditions. In this pursuit, seeking external expertise and investing in a domain where banks have limited knowledge could be hugely beneficial. With this in mind, this research looked at whether the surveyed banks have sought to adopt or evaluate any next generation technology solutions for risk data purposes, such as Big Data or In-memory; the details of which are given in Figure 4.

**Figure 3:**
What is the primary business driver at your firm that will benefit from your BCBS 239 initiatives?

- Improved stress testing capabilities: 26%
- Improved submissions to regulators: 22%
- More holistic view of organisational risks: 30%
- More reliable risk calculations: 12%
- Other: 11%

**Figure 4:**
What next generation technologies are you exploring to address issues with risk data aggregation and reporting?

- Big data: 52%
- In-memory: 44%
- Grid: 30%
- Data Virtualisation: 15%
- None: 19%
- Other: 7%
As illustrated in Figure 4, the vast majority of the surveyed banks are exploring next generation technology while only 19% of the banks are not looking into any of these innovative solutions. In this respect, Big Data tops the charts and is closely followed by In-memory techniques, with 52% and 44% of banks looking into these solutions, respectively. It is important to note that, Big Data and In-memory techniques can be used together to facilitate very large risk data sets which could then be explored through data visualisation techniques and also enable interactive stress testing on very large, aggregated portfolios like the group level banking and trading books.

These trends throw light on the efforts being made to understand different aspects of changing business conditions and new ways of improving data management and reporting capabilities. Furthermore, the findings indicate a drive to take advantages of the gains allowed by Moore’s law4, with 30% of the banks looking at solutions that could increase their computational power by adopting Grid computing. Considering data virtualisation could be the fastest way to feed consistent data to risk systems, as an interim step, while siloed source systems are in process of remediation, banks can leverage this technology to improve data consistency and real-time access to data. However, only 15% of the participating banks seem to be looking at data virtualisation at the moment. Furthermore, a small fraction of banks that chose ‘other’ are either considering investments in cloud technology or enhanced storage procedures.

**Risk Data Solutions**

The principles laid out in BCBS 239 aim to facilitate the implementation of robust risk data management frameworks at banks. Overall, this new obligation should be seen as an opportunity to build unified frameworks, eliminating data silos and increasing the overall quality and consistency of data that will lead to a single source of risk information. To achieve this, banks must consider a number of fundamental objectives when developing their risk data management framework, which include:

- To build a unified solution based on a common data model to present accurate, reliable and consistent data;
- To achieve a holistic view of risk data by eliminating data silos and achieve firm-wide data consistency for regulatory reporting; and
- To streamline risk data into a single source of information and eliminate conflicting information.

With this in mind, this research sought to establish how banks are implementing their risk data solutions across risk types. The approaches used in the implementation of risk data solutions vary across the sample, with 44% using a single solution across all risk divisions and 41% using separate solutions for different risk types. At the 15% of banks that chose ‘other’ it was noted that they either don’t have a solution currently in place or that they are moving towards a single solution, the details of which are illustrated in Figure 5.

---

4 “Moore’s law or how overall processing power for computers will double every two years”, available on: [http://www.mooreslaw.org/](http://www.mooreslaw.org/).
Figure 5:

How is your risk data solution being implemented across different risk types?

A visual inspection of the above figure suggests that a majority of the banks are moving towards implementing a single solution across all divisions in order to achieve a unified view. However, a significant minority are implementing different solutions for each type of risk. This trend seems to highlight the lingering conundrum around handling colossal amounts of largely unstructured data generated on a daily basis that needs to be structured and consolidated at various levels to draw meaningful information.

Implementing different solutions for each risk type may not be conducive to achieving a holistic view of risks given the magnitude and complexities involved in this pursuit. This argument is further strengthened by the fact a Bank of International Settlements’ (BIS) study, has identified that this approach leads to integration and aggregation challenges at enterprise level. The approach taken by a significant minority of the sample that uses separate solutions to aggregate data to achieve a unified view is not the most efficient approach that should be taken.

Further to this, this research sought to find out the key technical challenges that banks are facing when aggregating and consolidating data across risk types. At 81% of the surveyed banks, data inconsistencies remain a key technical challenge in this space. Additionally, a significant proportion of the banks still have difficulties owing to separate systems used for each risk type and inflexible source systems. The institutions that chose ‘other’ have opined that lack of skills and expertise in data aggregation, lack of data governance, cost and volume of data are additional key technical challenges.

---

Observing Figure 6, it is evident that data modelling and data management challenges are rife across the industry. Clearly, finding appropriate solutions to overcome data consistency issues still seems to be a significant hurdle for banks. One other very important point that was highlighted during the course of this research is the issue around the lack of skills and expertise in data management that seems to plague the financial sector.

In light of these continued data challenges, this research sought to find out the time taken by the participating banks to conduct stress tests that are pivotal in presenting an accurate picture of the exposures banks face and evaluate their ability to withstand shocks. It is essential for financial institutions to perform stress tests on a regular basis. This is particularly important during periods of economic stress, when markets can be highly volatile. By conducting frequent stress tests, ideally on a daily basis, banks can ensure that they are better prepared to effectively manage their risk exposures and respond appropriately to changing market conditions. However, drawing conclusions from the above figure, where inconsistent data is a key technical challenge, performing regulatory stress tests at an enterprise level on a daily basis is likely to be challenging. At the surveyed banks, the time required to carry out enterprise-wide regulatory stress tests varies markedly, the details of which are illustrated in Figure 7.
At a significant proportion of the sample, 41%, enterprise wide regulatory stress tests are carried out between 1-5 days. While 15% of the surveyed banks take 5-10 days, 19% require 10-15 days to conduct enterprise wide regulatory stress test. A further 4% take 15-20 days. Interestingly, less than 10% of the surveyed banks have developed capability of conducting enterprise-wide stress tests on an overnight or intra-day basis. This is a troubling statistic given the increasing frequency of regulatory stress testing and the need for rapid scenario modelling in times of economic stress.

Moreover, developing enterprise-wide stress tests requires financial institutions to employ a wide range of scenarios based on both historical data and hypothetical events to ensure that they are capable of withstanding future shocks. However, developing simulations that are sufficiently sophisticated to do so at the enterprise level, and in timely manner, can be highly challenging, not least because of the technical challenges highlighted in Figure 6. With this in mind, this survey sought to find out the main challenges faced by the participating banks when developing stress scenarios.

**Figure 8:**

**What are the main challenges you face in developing new stress scenarios?**

Many of the difficulties facing banks regarding the timeliness at which regulatory stress tests are carried out seem to reflect the data quality challenges facing the surveyed banks. With 59% of the sample stating that data quality issues are a major challenge in developing stress scenarios and a further 52% relating it to the timeframe required to execute stress tests; which are expected to shorten further, as regulators anticipate that firms would have access to both clean data and modern risk analytics systems that enable in-memory computing and interactive stress testing with immediate results. While 44% of banks attribute these challenges to inflexible source systems, 33% of firms point to the development of stress scenarios as a challenge in itself. At a further 14%, accessibility issues are a concern. At the 15% of banks who chose ‘other’ the following challenges have been identified:
- Granularity level to apply stress test parameters
- Implementing new stress scenarios
- Pricing model performance
- Cost of conducting enterprise wide regulatory stress tests

Looking at Figure 7 and Figure 8, these difficulties reflect upon data and infrastructure challenges that the participant banks face in conducting stress tests as these tests are computationally burdensome, and often require powerful risk calculation engines to run simulations at different time points for thousands of scenarios. Clearly, sheer volumes of data and data inconsistencies are hindering the ability of the participant banks to conduct stress tests on a daily basis. Banks have to devote enough software cores to ease the simulation runs, and the challenges are further compounded by infrastructure inflexibility to accommodate additional hardware.

**Risk Data Aggregation**

In the financial services industry, data is available from a number of sources, such as exchanges, external vendors and internal systems. Risk data aggregation involves consolidating this sourced data and reformatting, reorganising and adding value to the available information for risk management purposes. The general premise of risk data aggregation is that in retrieving and combining data from internal applications with external information such as credit ratings and market data, risk managers are provided with the ability to combine global analysis of disparate risk data to better analyse risks at an operational level. This enables banks to develop quantitative risk measures that incorporate multiple types, or sources, of risk across all products within the firm.

Although the main goal is to estimate the amount of capital that a firm believes is necessary to absorb potential losses associated with each of the included risks, and to comply with the global regulatory agenda, financial institutions also use this information to price trades and conduct business and, therefore, it is very important that they have a consolidated view of this data.

Regulatory changes under BCBS 239 will significantly affect the way data is modelled and distributed; as such, banks have to concentrate on streamlining and aggregating risk data for compliance, risk management and reporting purposes. With this in mind, this section of the report explores the frequency at which data for different major risk types (market, credit and liquidity risks) is produced for compliance and risk management purposes, respectively; the details of which are given in Figure 9 and Figure 10.
Comparing Figure 9 and Figure 10, it is interesting to see the risk data for risk management is produced more frequently on an intra-day and daily basis, compared to compliance purposes. However, this trend seems to reverse, on a weekly and monthly basis. It is interesting to note that data produced for market risk dominates the intra-day activity compared to credit and liquidity risks. This trend highlights an important point that, given that the volume and complexity involved in producing data for credit and liquidity risks is significantly higher than for market risk, banks have further to go to develop this capability in the credit and liquidity risk space.

Furthermore, these trends throw some light on the consistency of policy frameworks at the participant banks. Although there is no statement to infer from, and to arrive on a
Conclusion about why this trend is so predominant at the participating banks, conventional wisdom points to the complexity involved in credit and market risk management, which includes the volumes of historical data that need to be captured, aggregated and evaluated under a consistent policy framework. At present, the participant banks seem to lack such a policy. Another reason could be simple, and much of this exercise may revolve around regulatory reporting requirements.

Further to this, this survey sought to find out whether the participating banks are satisfied with their ability to prove data lineage as required by BCBS 239. As seen in Figure 11, an overwhelming majority of the surveyed banks expressed dissatisfaction with their organisation’s ability to prove data lineage, with 67% of the banks seeing room for improvement and a further 22% still requiring significant investment in this space. These results indicate that a total of 89% require improvements in this space and highlights the need for a sense of urgency for banks to complete projects before the regulatory deadline of January 2016.

**Figure 11:**

How satisfied are you with your organisation’s ability to prove data lineage as required by BCBS 239?

Current State of Process Automation and Future Outlook

Data aggregation involves a variety of tools and methodologies to migrate and consolidate data and present it in a format that it is easily comprehensible. This can be achieved using an array of middleware solutions that are available today to integrate data held within disparate systems. Automating this process, with the help of other Enterprise Application Integration tools, is fundamentally based on techniques that make dispersed and typically heterogeneous classes of information available to multiple applications as though there were one common data resource. Therefore banks have to consider investing in appropriate tools.
In a similar sentiment, BCBS 239 recommends that banks consider making strategic investments in appropriate data management technologies to efficiently integrate, capture, govern, and deliver required data for compliance purposes. This section of the report explores the extent to which the surveyed banks rely upon manual processes to aggregate risk data. As seen in Figure 12, at the participant banks, the reliance on manual processes to aggregate risk data is very limited across these risk types. However, the large disparity between entirely automated and largely automated processes is an illustration of what the BCBS 239 report seeks to address, and highlights the point that manual processes still remain and inhibit firms’ ability to deliver on the principles. Furthermore, it is important to highlight the fact that the extent of entirely automated process across liquidity risk, which has the highest impact in times of stress or volatility, is very low.

**Figure 12:**
To what extent do you rely on manual processes to aggregate risk data?

Furthermore, this research asked the surveyed banks to indicate if current approaches would change going forward, the details of which are illustrated in Figure 13. It is evident from Figure 12 and Figure 13 that, although the participating banks are disinclined towards the reliance on manual process entirely for aggregating risk data and are striving to depend on automated processes, half of the participating institutions indicated that they still have to rely on a degree of manual intervention going forward. This trend is visible across all the three risk types.
Figure 13:
To what extent do you expect to rely on manual processes to aggregate risk data going forward?

![Bar chart showing the percentage of banks expected to rely on manual processes for risk data aggregation.](image)

**Progress of Compliance Projects**

This section of the report explores the progress of BCBS 239 initiatives across all three major risk types at the participating banks, which are shown in Figure 14.

Figure 14:
How close are your organisation’s risk data aggregation and reporting initiatives to being complete?

![Bar chart showing the progress of BCBS 239 initiatives across all three major risk types.](image)
At this point, the initiatives undertaken by the participating banks on the market risk front are either partially completed or nearing completion. Only at 15% of the banks, the projects are fully completed. It is a similar story on the credit risk side. At 56% of banks the projects are partially completed and at a further 22% they are nearing completion. Only 7% of the banks report that they are complete and another 7% have not started any projects yet. Coming to liquidity risk, at 30% of the banks, the projects are almost complete and at a further 52% they are partially complete. While 7% have not started any projects, it is worth highlighting that none of the participating banks have completed any projects in this space.

Overall, at a majority of the banks, compliance projects are only partially complete. With this in mind, this survey asked the participating banks to indicate the level of satisfaction with the trajectory of these initiatives, the details of which are illustrated in Figure 15.

Figure 15:
How satisfied are you with the trajectory of these initiatives?

As expected, with reference to the trajectory of initiatives, a majority of the surveyed banks still see room for improvement. Although some might argue that level of satisfaction is too subjective a term to define the progress and success of large scale compliance initiatives which are firm specific, it may actually act as a milestone to evaluate their progress going forward. All in all, with a majority of the banks requiring improvements, this survey sought to identify the key areas that banks are investing in in this space, the details of which are illustrated in Figure 16.
Figure 16:
What are the key areas of expenditure of these initiatives?

A visual inspection of the figure above suggests that, 70% of banks are more inclined towards investing in training their internal staff followed by 56% and 52% of investments in software and hardware technologies, respectively. A further 41% suggested that the key areas of expenditure are spent on technology, namely employing consultancies. At 44%, the key expenditure is on external staff, such as SMEs. The 4% that chose ‘other’ indicated that they have not started any investments yet, as they have not determined the solution/path forward. Overall, these trends suggest a positive attitude towards BCBS 239 compliance as the banks are more willing to invest in three core components of data management: skills, technology and infrastructure. It is also encouraging to see an inclination towards investing in external staff for additional support that maybe needed whilst training internal staff. All in all, the discouragement found in the first section of the report seems to have faded and the investments seem to be in the right places and reflect upon the seriousness shown by these banks to not only comply with regulations, but also enhance their risk management frameworks.
Conclusion

In a bid to improve the resolvability of banks and enhance their risk IT capabilities, the Basel Committee on Banking Supervision, has established a set of *Principles for effective risk data aggregation and risk reporting* (BCBS239). The BCBS 239 principles, aimed at improving risk data aggregation and reporting capabilities, set a challenging agenda for banks in terms of improving their IT infrastructure.

As it transpires, the BCBS 239 compliance initiatives at the majority of the surveyed institutions revolve around making enhancements to existing solutions, rather than developing entirely new solutions. Despite this, the surveyed banks are looking at incorporating more innovative solutions and are currently adopting or evaluating next generation technology solutions such as, Big Data and In-memory.

Additionally, in order to facilitate more efficient and effective enterprise risk data management, most of the banks are moving towards implementing a single solution across all risk divisions in order to achieve a unified view of their risk exposures. Despite this, a significant minority still implement different solutions for each type of risk. Furthermore, at 81% of the surveyed banks, data inconsistencies remain a key technical challenge in this space while a significant proportion of the banks still have difficulties owing to separate systems for each risk type and inflexible source systems.

In the data aggregation space across market, credit and liquidity risk types, it is interesting to see the risk data for risk management is produced more frequently on an intra-day and daily basis, compared to compliance purposes. However, this trend seems to reverse on a weekly and monthly basis. Conventional wisdom points to the complexity involved in credit and market risk management which includes the volume of historical data that needs to be captured, aggregated and evaluated under a consistent policy framework; and at present the participant banks seem to lack such a policy.

In terms of status of completion of the compliance projects, the initiatives taken up by the participating banks are only partially complete, with the expenditure focused on investment on developing internal staff, technology solutions (both hardware and software). As expected, with reference to the trajectory of initiatives, a majority of the surveyed banks still see room for improvement.

In sum, the analysis of this report has ascertained that the banks encounter huge problems in terms of data inconsistency and quality and are relying heavily on process automation to minimise them. All in all, BCBS 239 presents a significant opportunity for banks to develop a robust risk management framework and significantly improve their risk data aggregation capability. However, it remains to be seen if banks will take advantage of this opportunity to push this improvement agenda to treat data management as a valuable asset rather than a mere utility centre. Overall, the trends offer a glimpse of hope for risk management technology and indicate a positive investment attitude, as banks are more willing to invest in three core components of data management: skills, technology and infrastructure. It is also encouraging to see an inclination towards investing in external staff for a bit of additional support that maybe needed whilst training their internal staff.
Looking at the findings of this survey, this research recommends the following best-practices that banks may use as a guide in formulating a response to comply with BCBS 239 principles.

- The use of Big Data and In-memory techniques to aggregate data together from siloed systems;

- The establishment of interactive stress testing systems that use In-memory and grid techniques that banks can use to accelerate the response to regulatory requirements and help run the business better; and

- The use of data virtualisation, integration and quality techniques to enable consistent terminology for data elements so that principles can be met more quickly while source system remediation continues.

About Lepus

Lepus was founded in 1997 to provide Research, Consulting and Marketing Services to the Finance Industry. Concentrating mainly on Investment Banking, Lepus also covers the Retail, Insurance, Asset Management, Corporate and Hedge Fund sectors. Lepus’ success is founded on its ability to provide its clients with a service which is expressly geared to their individual requirements.

Lepus has experience in all stages of project lifecycle – from overall strategy in a particular business/product area to extensive research capability. We have undertaken assignments both regionally and globally and where needed, we operate on an Associate basis, to provide the best capabilities for each project.

For more information on the Lepus Research, Lepus Consulting and Lepus Events services, please visit www.lepus.com or email marketing@lepus.com.