Aggravation or Aggregation: Risk Data and Compliance
Introduction

Until the financial crisis of 2008, enterprisewide risk data management was perceived by banks and other financial institutions as a mere utility center. 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’s 2013 Principles for effective risk data aggregation and risk reporting (BCBS 239) 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 apply these principles to banks identified as domestic systemically important banks (D-SIBs) three years following their designation as D-SIBs. 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.

BCBS 239 is not merely a set of principles aimed at improving data aggregation capabilities. It 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 to monitor and manage risks at the group level.

---

With the need to address challenges of aggregating risk data accurately and reporting it on a timely basis, implementing more responsive and flexible solutions has become paramount for financial institutions. This white paper, based on a SAS-commissioned survey of 27 major financial institutions, including G-SIBs and D-SIBs from diversified geographical regions such as North America, Europe and Asia Pacific, 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.
- 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 time frames is proving to be tricky. In this sense, BCBS 239 constitutes a challenging task for financial institutions. Banks are now forced not only to understand the manner in which risk data should be organized and formatted, but also to evaluate the reliability and accuracy of the tools at their disposal to comply. Clearly, banks have to significantly enhance their IT infrastructures, such as upstream systems, risk engines and reporting systems.

In terms of the approaches that banks are taking to comply with risk data initiatives, the vast majority of the surveyed institutions – 78 percent – are planning to make enhancements to existing solutions, rather than developing entirely new solutions (see 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 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 toward technology at these banks. Focus still seems to largely center 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 that for many, extending existing solutions is simply the most pragmatic and realistic option. That rebuttal may be too simplistic, 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 framework. 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 banks to indicate the primary business drivers that their respective organizations 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 organizational 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 percent, on the lower end of the spectrum.
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.

As illustrated in Figure 4, the vast majority of the surveyed banks are exploring next-generation technology, while only 19 percent 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 percent and 44 percent 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 visualization 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 advantage of the gains allowed by Moore’s law, with 30 percent of the banks looking at solutions that could increase their computational power by adopting grid computing. Considering data virtualization 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 use this technology to improve data consistency and real-time access to data. However, only 15 percent of the participating banks seem to be looking at data virtualization 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:

- Building a unified solution based on a common data model to present accurate, reliable and consistent data.
- Achieving a holistic view of risk data by eliminating data silos and achieving firmwide data consistency for regulatory reporting.
- Streamlining risk data into a single source of information and eliminating 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 percent using a single solution across all risk divisions and 41 percent using separate solutions for different risk types. At the 15 percent of banks that chose “Other,” it was noted that they either don’t have a solution currently in place or that they are moving toward a single solution, the details of which are illustrated in Figure 5.

The above figure suggests that a plurality of the banks are moving toward 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 daily 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 the enterprise level. The significant minority of the sample that uses separate solutions to aggregate data to achieve a unified view are not taking the most efficient approach.

Further, this research sought to find out the key technical challenges that banks are facing when aggregating and consolidating data across risk types. At 81 percent 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 indicated that lack of skills and expertise in data aggregation, lack of data governance, cost and volume of data are additional key technical challenges.

Figure 5: How is your risk data solution being implemented across different risk types?

In light of these continued data challenges, this research sought to find out the time taken to conduct stress tests that are pivotal in presenting an accurate picture of the exposures banks face and evaluating their ability to withstand shocks. It is essential for financial institutions to perform stress tests regularly. This is particularly important during periods of economic stress, when markets can be highly volatile. By conducting frequent stress tests – ideally daily – banks can ensure that they are better prepared to manage their risk exposures and respond to changing market conditions. However, drawing conclusions from the above figure, where inconsistent data is a key technical challenge, performing daily regulatory stress tests at an enterprise level is likely to be challenging. 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 percent, enterprise-wide regulatory stress tests require between one and five days. While 15 percent of the surveyed banks take five to 10 days, 19 percent require 10 to 15 days to conduct enterprise-wide regulatory stress tests. A further 4 percent take 15 to 20 days. Interestingly, less than 10 percent were capable of conducting enterprise-wide stress tests on an overnight or intraday basis. This is a troubling statistic given the increasing frequency of regulatory stress testing and the need for rapid scenario modeling 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 a 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.
Figures 7 and 8 show how these difficulties reflect upon data and infrastructure challenges that the participant banks face in conducting stress tests. These tests are computationally burdensome and often require powerful risk calculation engines to run simulations at different times for thousands of scenarios. Clearly, sheer volumes of data and data inconsistencies are hindering banks’ ability to conduct daily stress tests. 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, reorganizing 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 analyze 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 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. 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 modeled 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 Figures 9 and 10.

Many of the difficulties facing banks regarding the timeliness at which regulatory stress tests are carried out seem to reflect data quality challenges. Fifty-nine percent of the sample stated that data quality issues are a major challenge in developing stress scenarios, while 52 percent related it to the time required to execute stress tests. This time frame is 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 to gain immediate results. While 44 percent of banks attribute these challenges to inflexible source systems, 33 percent point to the development of stress scenarios as a challenge in itself. For 14 percent, accessibility issues are a concern. Among the 15 percent of banks that 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.

Figure 8: What are the main challenges you face in developing new stress scenarios?

![Figure 8: Main Challenges in Stress Scenario Development](image)
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 at 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 organization’s ability to prove data lineage, with 67 percent of the banks seeing room for improvement and a further 22 percent still requiring significant investment in this space. These results indicate that a total of 89 percent 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.

Comparing Figures 9 and 10, it is interesting to see the risk data for risk management is produced more frequently on an intraday and daily basis, compared to compliance purposes. However, this trend seems to reverse on a weekly and monthly basis. Data produced for market risk dominates the intraday 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

Figure 9: How frequently is risk data produced for COMPLIANCE purposes?

Figure 10: How frequently is risk data produced for RISK MANAGEMENT purposes?
Data aggregation involves a variety of tools and methodologies to migrate and consolidate data and present it in an easily comprehensible format. This can be achieved using an array of middleware solutions 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, 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, entirely automated processes are very rare in liquidity risk, which has the highest impact in times of stress or volatility.

This research also asked whether current approaches would change going forward (see Figure 13). It is evident from Figures 12 and 13 that, although the banks are inclined not to rely on manual processes entirely for aggregating risk data and are moving toward automated processes, half still expect to rely on a degree of manual intervention going forward. This trend is visible across all three risk types.
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 is shown in Figure 14.

At this point, the banks’ market risk initiatives are either partially completed or nearing completion. The projects are complete at only 15 percent of the banks. It is a similar story on the credit risk side. The projects are partially completed at 56 percent of banks and nearing completion at 22 percent. Only 7 percent of the banks report that they are complete, and another 7 percent have not started any projects yet. In liquidity risk, the projects are almost complete at 30 percent of the banks and partially complete at 52 percent. Seven percent have not started any projects, and 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.

As expected, 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 that 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 in which banks are investing in this space, the details of which are illustrated in Figure 16.
In a bid to improve the resolution of banks and enhance their risk IT capabilities, the Basel Committee on Banking Supervision published *Principles for effective risk data aggregation and risk reporting* (BCBS 239). The BCBS 239 principles, aimed at improving risk data aggregation and reporting capabilities, set a challenging agenda for banks to improve their IT infrastructure.

As it transpires, the BCBS 239 compliance initiatives at the majority of the surveyed institutions involve making enhancements to existing solutions rather than developing entirely new ones. Despite this, the surveyed banks are looking at incorporating more innovative solutions and are adopting or evaluating next-generation technology solutions such as big data and in-memory processing.

Additionally, in order to facilitate more efficient and effective enterprise risk data management, most of the banks are moving toward 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 most banks, data inconsistencies remain a key technical challenge in this space, while many 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 more frequently produced on an intraday 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. The participant banks seem to lack such a policy.

The initiatives taken up by the participating banks are only partially complete, with the expenditure focused on investment in developing internal staffs and on technology solutions (both hardware and software). As expected, a majority of the surveyed banks still see room for improvement in the trajectory of initiatives.

Figure 16: What are the key areas of expenditure of these initiatives?

The figure above suggests that 70 percent of banks are more inclined to invest in training their internal staffs, followed by 56 percent and 52 percent of investments in software and hardware technologies, respectively. Forty-one percent identified technology as a key area of expenditure, namely employing consultancies. At 44 percent, the key expenditure is on the external staff, such as SMEs. The 4 percent 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 toward investing in external staff members for additional support that may be needed while training internally. 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 the seriousness shown by these banks to not only comply with regulations, but also enhance their risk management frameworks.
In summary, this analysis uncovered that the surveyed banks encounter huge problems in terms of data inconsistency and quality and are relying heavily on process automation to minimize 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 treat data management as a valuable asset rather than a mere utility center. 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 toward investing in external staff members for a bit of additional support that may be needed while training.

This research has led to recommendations of 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 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.
• The use of data virtualization, 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 the Survey

The information provided in this report was derived from an online survey, commissioned by SAS, of major financial institutions, including G-SIBs and D-SIBs, from diversified geographical regions such as North America, Europe and Asia Pacific. The survey was fielded in the first and second quarter of 2014. Some survey questions allowed for multiple responses, leading to totals exceeding 100 percent. The goal of the survey was to collect information from representatives of the surveyed institutions on the initiatives underway or being planned to comply with the BCBS 239 principles.