A survey of data management for risk management

May 2016
# Table of Contents

1. Introduction ..................................................................................................... 3
2. Composition of survey .................................................................................. 4
3. Organisation of data management ............................................................... 5
4. Data architecture .......................................................................................... 12
5. Drivers for change ....................................................................................... 16
6. Regulation ...................................................................................................... 18
7. Data quality ................................................................................................... 24
8. Conclusion ...................................................................................................... 25
About InteDelta ............................................................................................... 26
About Asset Control ........................................................................................ 27
1. Introduction

No area of banking has been so transformed in recent years as risk management. The pace of change that started with Basel II accelerated after the 2008 financial crisis with a plethora of new regulations that have revolutionised the way business is conducted and risk is managed. This regulatory-inspired change shows no signs of slowing.

In many ways, risk management is the most data-hungry area of banking, and the industry’s management of data has had to adapt swiftly to a fast-changing environment. In addition to meeting new regulatory requirements, banks have been under increased pressure to contain costs, improve efficiency and reduce their level of operational risk. Data management has had an integral part to play in this process.

The changing regulatory environment includes the Fundamental Review of the Trading Book (FRTB), BCBS 239 (“Principles for effective risk data aggregation and risk reporting”), the Asset Quality Review (AQR) and stress testing. These regulations have wide ranging implications for how banks manage risk, and data issues feature heavily in the areas to be addressed.

This paper explores the management of data in the banking market. The focus is on data management for risk management purposes, with particular emphasis on banks’ financial markets activities (i.e. excluding their retail and lending activities).

The paper covers:

- The organisation of data management for risk management functions – to what extent do firms adopt a centralised versus silo-based approach. Why are they organised in this way and how is this expected to change?
- Data architecture models – current and target end states. The use of Enterprise Data Management solutions within banks
- Drivers for change – internal versus regulatory and other external influences. The most important areas of regulation such as BCBS 239 and the Fundamental Review of the Trading Book are explored in some detail
- Data quality

The paper will highlight what we consider to be the “gold standard” with regard to the organisation of data management and the associated systems infrastructure. We will explore the extent to which banks have already achieved their target end states, and why different types of bank may be aiming for different end states.
2. Composition of survey

InteDelta interviewed a cross-section of 13 banks between late 2015 and early 2016. The types of institutions and their geographical focus are shown below.

**Figure 2.1:** Type of institutions in survey

- Investment bank/global bank: 15%
- Large regional bank: 69%
- Small regional bank: 16%

**Figure 2.2:** Bank locations in survey

- Europe: 46%
- North America: 23%
- Asia: 15%
- Middle East: 8%
- Australasia: 8%

---

**Glossary**

- AQR: Asset Quality Review
- BCBS: Basel Committee on Banking Supervision
- BCBS239: BCBS paper on “Principles for effective risk data aggregation and reporting”
- CCP: Central Clearing Counterparty
- CSA: Credit Support Annex
- CVA: Credit Valuation Adjustment
- EDM: Enterprise Data Management
- ES: Expected Shortfall
- D-SIB: Domestic Systemically Important Bank
- FRTB: Fundamental Review of the Trading Book
- G-SIB: Global Systemically Important Bank
- HQLA: High Quality Liquid Assets
- IOSCO: International Organization of Securities Commissions
- ISIN: International Security Identification Number
- KPI: Key Performance Indicator
- PFE: Potential Future Exposure
- SA-CCR: Standardised Approach for Counterparty Credit Risk
- VaR: Value at Risk
3. Organisation of data management

Within banks, the organisation of data management for risk management purposes does not conform to a single model. Each bank has arrived at its own organisational structure through a process of change to meet its own needs. In many cases banks have been constrained from attaining their ideal operating model by systems or organisational considerations. Generalising about banks’ organisational models is difficult, but the two ends of the spectrum can be easily identified: a fully centralised operating model, and a complete silo approach.

Under a fully centralised model, a single function is responsible for the management of all types of data used across the bank for risk management purposes and also by the front office and finance functions. Under the most silo-based models, each function is responsible for the management of its own data. The majority of banks have features of both centralised and silo-based approaches.

Silos can exist in a number of different dimensions:

- **Type of data** – a bank may be highly centralised for the management of, say, market data, but less so for other types of data. Alternatively, the management of each type of data may be highly centralised but managed independently of each other. The key types of data used in risk management are summarised on page 11.

- **Business function** – a bank may have a centralised data management function for risk management but this does not serve the front office or finance functions.

- **Geography** – a large bank operating in multiple geographies may have a centralised data management function within each location but this may not be harmonised across all locations.

For the purposes of analysis we have assigned each surveyed bank a score of 1-5, where 1 indicates a fully centralised approach and 5 is a completely silo-based approach. For example, a fully centralised approach (score of 1) would have a centralised repository for all types of data which would feed all risk management, front office and operations functions across all geographies. Under a fully decentralised model (score of 5) each function would have its own data management solution for each data type and there would be little sharing of data across functions or geographies. Between these two extremes (scores of 2-4) banks have an element of centralisation (e.g. a data management solution for market data management within risk management in one location) and the lower the score, the higher the degree of centralisation.

Many banks are in a process of transition and we have therefore identified both their current and target end states.
None of the surveyed banks meet the criteria for the two most centralised categories at present, although, when their change programmes are complete, 31% of banks will fall into these categories. At the other end of the spectrum, 54% of banks are currently classified in the two most siloed categories, but this will reduce to 38% when banks have completed their change programmes. There is a clear pattern of movement towards a more centralised approach. The rationale for the banks’ organisational choices and the drivers for change are discussed in Section 5 of this paper.

The current overall degree of centralisation shown in Figure 3.1 masks some areas of data management which are more centralised than others. Firstly, data management is more centralised within risk management than across the enterprise as a whole.
Considering data management within just the risk management function, less than a quarter of banks fall into the two most siloed categories, compared to 54% when looking at the institution as a whole. Organisationally, it is easier to achieve centralisation between the various risk management silos than across the entire organisation, including the front office and finance divisions. Nevertheless, this model leads to duplication of effort and gives rise to operating difficulties, particularly in reconciling P&L and positions between risk management, the front office and finance.

We asked banks to quantify the level of duplication in data management between the various silos:

**Figure 3.3: Degree of centralisation in data management within risk management**

![Pie chart showing centralisation levels]

- 23% completely centralised
- 15% centralised
- 62% siloed

**Figure 3.4: Degree of duplication in data management**

![Pie chart showing duplication levels]

- 23% little duplication
- 39% some duplication
- 38% considerable duplication
Most banks recognise that duplication should – ideally – be avoided and that it can lead to considerable reconciliation problems and operational inefficiencies. This does not avoid the need for independence of the risk management function from the front office, and this was often cited as a reason for not pursuing a more integrated approach with the front office. One of the surveyed banks is implementing changes to make the risk function more independent from the front office, which may actually increase the degree of duplication, but this is seen as a price worth paying for a greater degree of independence. Such approaches may increase with the advent of BCBS 239 and the need for prudent valuation. A fully centralised model is more efficient, reduces reconciliation problems and lowers operational risk. Independence may still require the front office to give up ownership of aspects of its data, which may be difficult to achieve.

A second area in which aspects of data management may be more centralised than Figure 3.1 implies relates to the type of data under consideration.

The survey showed that the management of market data is considerably more centralised than other data types:

![Figure 3.5: Degree of centralisation for market data](image)

When considering just market data management, only 30% of banks fall into the two least centralised categories, compared to 54% of banks for data management in general. The same market data is required by multiple functions both within risk management (i.e. market and credit risk management) and by the front office, finance and operations. For a bank wishing to centralise its data management, market data is the obvious place to start. In many institutions this is as far as the centralisation has advanced.
The considerations for centralising non-market data are described below:

- **Trade data** – trade data is generated by the front office but needed across risk management, finance and operations. Some banks have developed a trade data repository to serve all functions within the institution. Most banks, however, take feeds directly from front office systems into the respective risk management, finance and operational systems. Trade data requirements can be very specific for each area needing the data. This means that the establishment of a central function and system to serve all areas of risk management – plus finance and operations – can be challenging; although in doing so the number of required interfaces from front office systems is reduced considerably.

- **Derived data** – derived data is required by the front office, risk management and finance, and includes interest rate and credit curves and volatility surfaces. A large institution may have several thousand such curves and surfaces. There are clear advantages to centralising its calculation. Failure to do so can result in difficulties agreeing on prices and model calibrations. Much derived data is, however, specific to a particular function and even where common derived data is required, the quants from the respective departments may not agree on how it should be calculated. The centralisation of the management of derived data can therefore be challenging. The importance attached to derived data has increased as a result of recent regulatory and business initiatives, for example:
  - Calculation of CVA – requires construction of credit spread curves including the use of proxy curves where liquid CDS spreads cannot be found
  - Use of proxy data under the Fundamental Review of Trading Book

- **Reference data** – reference data will often fall into the same category as market data in terms of the need to share it across the enterprise. Failure to have a centralised record of reference data can lead to increased duplication and reconciliation problems, for example if a bank does not have a common unique customer identifier. Reference data may, however, be specific to one particular function (for example, the customer hierarchy may only be of interest to credit risk management) and its generation is often embedded within disparate business processes across the bank. For these reasons, reference data may be more challenging to centralise than market data.

- **Netting and collateral data** – data relating to netting and CSAs is typically generated by the legal department or front office and is used in the calculation of counterparty risk and regulatory capital for counterparty risk. This data has fewer interested parties than other types of data and as a result banks may not see a need to remove its management from the generating departments. Nevertheless, there is an increased focus on credit mitigation through collateralisation and netting, because:
  - an increasing proportion of transactions are cleared through CCPs
  - non-cleared derivatives will soon be subject to the BCBS/IOSCO rules for initial margin
  - banks are increasingly focusing on collateral optimisation
  - the new standardised approach for the calculation of regulatory capital for counterparty risk (SA-CCR) is more sensitive to netting and collateral

The effective management of netting and collateral data can as a consequence be expected to move up banks’ agendas.
Figure 3.6 summarises the overall degree of centralisation by data type that we observed from the survey, although the situation within a specific bank may be very different.

**Figure 3.6: Degree of centralisation by data type**

- **Low centralisation**
  - Netting and collateral data

- **Medium centralisation**
  - Derived data
  - Trade data
  - Reference data

- **High centralisation**
  - Market data

Many smaller banks do not currently see the need to put highly structured data management processes and governance in place. One of the surveyed banks commented “Data is shared, but not in a very structured way. Data comes from a wide variety of sources but there is no real control over it.”

While many Tier 2 banks may view a completely centralised model as desirable and achievable, for Tier 1 banks, the complexity of their operations often means that such a high degree of centralisation is not pursued. Such global banks may have multiple data management functions but with a high degree of centralisation within each function. For example, this may include separate global data management functions for each data type (time series data, static data, derived data, etc.).

Some banks view a common data management function serving both the front and middle office as a desirable target state as it ensures commonality of data and minimises reconciliation issues. Other banks take the view that the need to maintain independence between front office and risk management would be compromised if a common data management function were put in place.

In general, the “gold standard” that banks are aspiring to is to maximise the degree of centralisation whilst recognising that total centralisation may not be practical for their organisation. Many smaller banks have not yet moved very far along the path to centralisation. Banks at the Tier 1/2 boundary are perhaps the most centralised, or are planning to become so, although they may consciously decide not to centralise in areas where they see that this may lead to a loss of risk management’s independence from the business. The largest global banks may find that their organisational structures are too complex to achieve the totally centralised solutions that Tier 2 banks may be able to achieve, but will seek to centralise as much as is practical.
Types of data used in risk management

Transaction and position data
Generated by front office systems, transaction data describes the attributes of a transaction. It is required for transactions to be priced and modelled. Some risk calculations work with position data (e.g. the total exposure to Japanese Yen) rather than disaggregating to the individual transaction level.

Market data
Market data is the collection of externally observable rates and prices that drive the prices of financial instruments, for example FX rates, yield curves, equity and commodity prices.

Market data is required to price transactions at the time of trading and to revalue them for financial accounting and risk management purposes, for example in the calculation of Value at Risk (VaR), Potential Future Exposure (PFE) and the performance of stress tests.

Long histories (time series) of market data need to be maintained by banks. Recent and proposed regulations such as Basel III and the FRTB have increased the period over which risk calculations need to be performed and therefore the length of time series that need to be stored. Our survey indicated that most banks store time series for 7-10 years.

Derived data
Derived data is data which is required to price and model financial instruments but which is not directly observable in the market, for example zero yield curves, volatility surfaces and historic volatilities. Derived data also includes the calculation of proxy data, such as:

- Derived CDS spreads for use in a CVA calculation where there is no liquid CDS for a counterparty name
- Calculation of proxies prescribed under the Fundamental Review of the Trading Book where a bank does not have sufficient time series internally stored

Some derived data may be obtained from market data vendors, but banks may also need or choose to calculate their own derived data from available, observable market data.

Reference data
Reference data is the collection of data that defines aspects of a security or counterparty. For example, a security identifier such as an ISIN code or the data that specifies a counterparty hierarchy. Reference data changes relatively infrequently. Reference data may also include counterparty hierarchies and corporate actions.

Netting and collateral data
Netting and collateral data is used mainly in the calculation of counterparty exposure. Netting data is used to determine “netting sets” that define which transactions can legally be netted against one another to reduce counterparty exposure. Collateral data refers to information contained within a CSA which specifies which transactions are collateralised and the terms under which collateral will be called for (e.g. the Initial Margin and the Minimum Transfer Amount).
4. Data architecture

The quality and architecture of systems is one of the prime considerations in data management. For a completely silo-based approach, managing data in the originating systems may be sufficient. As soon as a bank embarks upon any sort of data management centralisation, a central repository of data becomes essential. Market best practice is to designate the central repository as a Golden Copy®.

The proportion of surveyed banks that have a Golden Copy of data used in risk applications, in both their current and target states, is as follows:

**Figure 4.1: Prevalence of Golden Copy of data in current state**

- No: 31%
- For some data: 69%

**Figure 4.2: Prevalence of Golden Copy in target state**

- No: 23%
- For some data: 15%
- For most data: 62%
Banks may manage their data using generic database technology or they may implement a more sophisticated Enterprise Data Management (EDM) solution, which places greater controls around the sourcing, management and validation of data.

Enterprise Data Management refers to the ability to effectively source, verify, combine and integrate data for internal applications, end users and external reporting. It focuses on the creation of common master data sets that satisfy organisational quality criteria including accuracy, timeliness and completeness. EDM aims to provide a common data foundation for a diverse set of internal and possibly also external stakeholders. It often encounters organisational difficulties as it cuts across different business silos and has to prioritise requirements and harmonise data definitions coming from different areas of a firm.

The goal of EDM is to achieve a common data foundation, create trust and confidence in data assets, and secure the integrity of the data used in business processes. In financial services, with its product proliferation, dynamic nature of a lot of data and heavy requirements on internal and external reporting, EDM can prove particularly valuable.

EDM systems seek to support an EDM practice. Common features include:

- Integration with internal and external data sources
- Mapping rules to combine different sets of content and to recast them into a common data model
- Validation rules to screen data sources and to detect anomalies, missing values and inconsistencies
- Distributing data sets to downstream applications depending on subscription lists
- Keeping an audit trail on data changes and providing lineage to trace the origins of data values
- Monitoring incoming and outgoing data feeds against operational SLAs
- Providing a common data dictionary and workflow processes for data cleansing
- Analytics for automation of derived data (e.g. bootstrapping, curves, surfaces)
- Linking to external model libraries (e.g. MATLAB, R)
The proportion of surveyed banks with an EDM solution in their current and target states is as follows:

**Figure 4.3:** Prevalence of EDM solutions in current state

- 69% have no EDM solution
- 31% have an EDM solution for some data

**Figure 4.4:** Prevalence of EDM solutions in target state

- 46% have an EDM solution for most data
- 45% have an EDM solution for some data
- 9% have no EDM solution

Over two thirds of banks currently have a Golden Copy for at least some of the data used in risk calculations. This rises to 85% when banks achieve their target end state. Less than a third of banks currently have an EDM system, but this rises to just over half when banks achieve their end state.

A strong correlation exists between the degree of data management centralisation that banks are seeking to achieve and the presence of an EDM solution:
Most banks with a low degree of centralisation still see the merit in implementing a Golden Copy for at least some of their risk data. 30% of such banks have implemented a solution which would be classified as an EDM system, although such solutions are not necessarily being used to their full potential due to the highly silo-based organisation of the banks. As banks attain a higher degree of risk data centralisation the need for an EDM solution clearly increases.

Small and medium sized banks frequently implement a single vendor solution as their front office, operations and risk management platform. One such bank commented “We use the same system for front office, market and credit risk. Our data management architecture follows this system.”

As noted in Section 3, many Tier 1 banks do not strive to completely centralise their data management function due to the high complexity of their organisation. Such banks may have multiple data management functions and choose a best of breed vendor systems for each data type. For example, they may choose separate solutions for security master management, market data and the calculation and management of derived data. The vendor solutions chosen by the largest banks for just one data type are often the same solutions that can be used as an EDM solution for all data types in a smaller and less complex environment.

---

1 This graph combines both the current state and target state for each bank. Centralisation is defined as Low if the score (as defined in Section 5) is 4 or 5, Medium if it is 3 and High if it is 1 or 2. A bank is defined as having a Golden Copy or EDM solution if such a solution is in place for some but not necessarily all data.
5. Drivers for change

Data management, particularly in relation to risk management, is undergoing a period of significant change. This change has both internal and external drivers, the latter being mainly regulatory.

Considering first the internal drivers:

Figure 5.1: Internal factors as drivers of change in data management

Just over half of the surveyed banks considered internal factors to be a significant driver of change for data management. Of the banks that did not consider internal factors to be driving change, the majority had either already gone through a programme of change to achieve their target end state, or were prioritising regulatory-driven change. Of the banks that cited internal drivers as somewhat or highly significant, the drivers can be classified as follows:

Figure 5.2: Internal drivers for change in data management
83% of banks cited operational efficiency and cost as the biggest internal driver to improving their data management infrastructure. Despite this, banks were unable to provide detailed analysis of the cost/benefit of the change initiative. A number of banks commented that although the centralisation and automation of their data management infrastructure would result in a like-for-like reduction in cost, many of the benefits of more accurate and timely data were intangible and could not be quantified easily. Furthermore, improvements to operational efficiency were often implemented alongside regulatory-driven changes or improvements to reduce operational risk. This makes like-for-like cost savings difficult to ascertain but many banks isolate some specific cost savings, such as the ability to re-use the same data across the organisation and therefore reduce the cost of data vendor services.

Banks citing the need to reduce operational risk included a bank which was implementing changes to reduce the number of reconciliation breaks between risk management and the front office. Another bank which cited the need to improve independence was concerned that the data used by risk management was not sufficiently independent of the front office.

Although internal drivers were important for change, regulation was considered to be far more significant, as shown below:

![Figure 5.3: Regulation as a driver of change in data management](image)

85% of banks surveyed regarded regulation as a highly significant driver of change in data management and no banks regarded regulation as having an insignificant impact. The specific areas of regulation having the biggest impact on data management are described in the next section.

There is a strong synergy between the centralisation and automation of data management and banks’ ability to efficiently and cost-effectively respond to regulation. One of the survey participants commented that “banks that regard each new piece of regulation as an ad hoc project without ever addressing the fundamental weaknesses of their data organisation or architecture will face a higher cost of regulatory compliance.”
6. Regulation

As evidenced by Figure 5.3, regulation is the biggest driver of change affecting data management for risk management. The graph below shows the areas of regulation cited as being most significant.

**Figure 6.1: Impact of regulation on data management**

[Bar chart showing impact of BCBS 239, FRTB, Stress testing, and Basel III]

**BCBS 239 (“Principles for effective data aggregation and reporting”) and the Fundamental Review of the Trading Book (FRTB) are the areas of regulation which most banks cited as having the most impact on data management, followed by stress testing and Basel III.**

In many banks the business and risk management functions were still assessing the impact of regulation and this had yet to be translated into detailed requirements for implementation within data management. It is therefore likely that our survey has under-reported the eventual impact of regulation on data management, particularly for FRTB and BCBS 239. One of the banks operating in a smaller jurisdiction found it difficult to assess the impact of certain regulations as “we are still waiting for our regulator to tell us what they want us to do”.

In addition to the regulations shown in Figure 6.1, which were referred to by multiple banks, individual banks cited other areas of regulation as having a significant impact on data management, specifically:

- Asset Quality Review (AQR)
- Dodd-Frank/EMIR
- High Quality Liquid Assets (HQLA)
- Interest rate risk in the banking book
- Volcker regulations

In light of the results of the survey, and the level of importance assigned to each, we now discuss BCBS 239 and the FRTB in more detail.
BCBS 239

“Principles for effective data aggregation and reporting”, usually referred to by its document reference number of BCBS 239, is guidance issued by the BCBS to improve the control environment around data used for risk management purposes. The BCBS paper’s introduction explains why this is required:

“One of the most significant lessons learned from the global financial crisis that began in 2007 was that banks’ information technology (IT) and data architectures were inadequate to support the broad management of financial risks. Many banks lacked the ability to aggregate risk exposures and identify concentrations quickly and accurately at the bank group level, across business lines and between legal entities. Some banks were unable to manage their risks properly because of weak risk data aggregation capabilities and risk reporting practices. This had severe consequences to the banks themselves and to the stability of the financial system as a whole.”

BCBS 239 outlines a range of principles that banks should adopt in their management of data. These range from data governance and infrastructure to the aggregation of data and risk reporting.

BCBS 239 applies to all banks that have been identified as **Global Systemically Important Banks** (G-SIBS) but with a strong recommendation that it should also apply to **Domestic Systemically Important Banks** (D-SIBS). Despite only applying to these categories of banks, the principles are being adopted as best practice by the market.

From a data management perspective, the key areas that many banks will need to demonstrate and potentially enhance to comply with BCBS 239 are:

- Data governance
- Data quality
- Reporting

One of the main points of BCBS 239 is Principle 2: Data Architecture & IT Infrastructure: “A bank should establish integrated data taxonomies and architecture across the banking group, which includes information on the characteristics of the data (metadata)…” This has proved one of the thorniest points for banks to comply with, if judged from the progress report and banks ‘self-assessment’ published in December 2015.

Additional key systems requirements include:

- Data accuracy and integrity (Principle 3) that puts the quality and control processes for risk data on the same footing as that used in financial statements: “Controls surrounding risk data should be as robust as those applicable to accounting data.”

- A common data dictionary as discussed above in the section on EDM systems. “As a precondition, a bank should have a “dictionary” of the concepts used, such that data is defined consistently across an organisation.”

- Adaptability (Principle 6), i.e. the ability to browse the data and satisfy ad-hoc requests with quick turnaround: “A bank’s risk data aggregation capabilities should be flexible and adaptable to meet ad hoc data requests, as needed, and to assess emerging risks.”

- Data quality management requirements as explained in principle 7 on Accuracy. This includes full transparency on the validation rules used in an EDM system: “Automated and manual edit and reasonableness checks, including an inventory of the validation rules that are applied to quantitative information.”
• Reporting requirements to group data and to easily report on data on many different dimensions: data should be available by business line, legal entity, asset type, industry, region and other groupings

62% of the surveyed banks identified specific areas of BCBS 239 that would impact them. Of these banks, 50% cited data governance as a significant implementation issue.2

25% of the banks which identified specific issues in connection with BCBS 239 specified risk reporting as giving rise to particular issues.

Other issues cited by banks were:
• Single view of data
• Reconciliations
• Granularity of data

Fundamental Review of the Trading Book
The FRTB proposes major changes to the calculation of regulatory capital for market risk. As with BCBS 239, the BCBS has introduced the FRTB to address deficiencies in the capital regime that became apparent during the financial crisis and were not adequately addressed in the “Basel 2.5” reforms. The FRTB makes major changes to the calculation of regulatory capital using banks’ own models, as well as the simpler and more prescriptive standardised approach.

The key components of the FRTB are:

• Changes to the trading book/banking book boundary – the current market risk regime relies on a bank’s own assessment of “intention to trade” in determining whether an asset should be included in the trading or banking book. Supervisors have found these criteria difficult to police and open to regulatory arbitrage. The FRTB introduces a series of rules to clarify which assets can be held on the trading book versus the banking book and when transfers between the books are permissible

• Treatment of credit – the FRTB introduces a harsher treatment of credit products

• Moving to Expected Shortfall – under the FRTB the use of VaR in the calculation of regulatory capital will be replaced by the alternative Expected Shortfall (ES) statistic, which is deemed to give a more stable model output and is less sensitive to extreme outlier observations

• Stressed calibration – Basel 2.5 introduced an additional capital charge based on “stressed VaR” which was calculated alongside the usual VaR. The FRTB now proposes a move to a single (Expected Shortfall) measure calibrated to a period of significant financial stress

• Incorporation of market liquidity – during the financial crisis, banks were often unable to promptly exit or hedge certain illiquid positions, which demonstrated the inadequacy of the 10-day VaR treatment for market risk. The FRTB proposes to address the liquidity issue through the introduction of variable liquidity horizons

• Relationship between internal models-based and standardised approaches – the FRTB proposes strengthening the relationship between the revised models-based and revised standardised approach. Criteria for the adoption of the internal-models based approach have been strengthened, and even where a bank has approval to use internal models it will also need to calculate and report capital under the standardised approach

2 Note also the comment at the beginning of this section which may mean that the survey potentially under-reports the eventual impact of this regulation
The FRTB requires banks to perform more stringent risk calculations and this is expected to place a significant burden on banks’ data management capabilities such as:

- **Length of time series** – calculations must be based on longer (10 years) time series of data including a period of significant stress. Within the time series data must be:
  - Continuously available historical observations – to be considered to have continuously available “real” prices, a risk factor must have at least 24 observable “real” prices per year with a maximum period of one month between two consecutive observations
  - Of sufficient frequency
  - Of high quality
  - Supported by real prices (not proxies) at which institutions have conducted a transaction
  - Be subject to established processes and controls

- **Non-modellable risk factors** – “modellable risk factors” are factors for which a bank has sufficient products to give an appropriate historical time data series. Risk factors which do not meet this definition are deemed “non-modellable risk factors” and a separate capital charge will be calculated using a stress scenario approach. The rules for a risk factor being modellable can be restrictive (e.g. requiring “continuously available real prices” and a sufficient set of representative transactions). The capitalisation of non-modellable risks may require greater reliance on proxy data

- **Liquidity horizon** – the FRTB requires banks to take into account the specific liquidity of each asset and to perform the risk calculation for a time horizon over which the asset could be realistically hedged without moving the price

- **Assets transferred to trading book** – the FRTB restricts the assets that can be held on the banking book which may mean that a bank needs to transfer assets from the banking to trading book upon which the data requirements for the risk calculations are substantially increased

The FRTB imposes statistical tests for banks to be able to use their own models to calculate capital. If these tests are failed, the bank is forced to calculate capital using the standardised approach, which may result in a large increase in capital. As noted above, if a risk factor is deemed to be non-modellable, an alternative risk calculation must be deployed – which can also lead to a capital increase. ISDA has estimated that if major banks moved to the revised Standardised Approach, capital requirements would be a factor of 4.2x the level currently held\(^3\).
Poor data management processes or systems can result in a bank having to adopt the standardised or non-modellable risk factor calculations, meaning the potential for a substantial capital increase.

Of the banks that were able to cite specific areas of data management that the FRTB would impact, the main areas cited as being problematic are shown below:

The FRTB requires the collection and processing of significantly more data than the existing calculation framework and methods need to be implemented to derive proxies for data that cannot be directly obtained.

As previously noted, the survey respondents at many banks commented that they were unaware of the impact of the FRTB from a data management perspective because the business is still assessing the impact. Accordingly, we believe that the eventual impact of the FRTB will be highly significant from a data management perspective. In January 2016, InteDelta published another survey that specifically focused on the FRTB implementation challenges⁴. The graph below is taken from that survey which shows the overall implementation challenges of the FRTB. Many of these are modelling-related but can be expected to have data implications.

---

From the perspective of a data management system, the key areas of functionality required for compliance with the FRTB include:

- Ability to track and report on long histories for market data
- Effective frameworks for market data validations and quality management
- Market data comparison of different sources
- Growing requirements on necessary data, i.e. a need for built-in vendor interfaces
- Built-in data normalisation and consolidation/ framework
- Ability to easily derive additional fields on instrument level, create new risk factors or apply shocks
- Integration with common analytics languages
- Searches and dashboards to show the modellability status of risk factors
- Consolidation of additional sources (e.g. multiple vendors and trade repositories) to provide additional observations for modellability
- Replacing non-modellable risk factors with modellable risk factors and a basis
- Per risk factor reference data for the liquidity horizon component of the ES calculation
- Support for calibrating the ES calculation to the period of most stress

**Preparation for future regulation**

Much of the current regulatory workload cuts across multiple areas of a bank: BCBS 239 and stress testing are enterprise-wide, the FRTB impacts both the trading and banking book and CVA blurs the boundary between market and counterparty risk. Future regulation is likely to have a similar focus on cross-asset class, cross risk-class and apply enterprise-wide. Banks that have broken down silos, both organisationally and in terms of systems, will be best placed to implement future regulation. Some banks seem not to be taking such a strategic approach, with one bank commenting that their approach is to make changes on a “regulation by regulation” basis.
7. Data quality

Achieving high quality data is one of the key goals of a data management function. This is reinforced by regulation such as BCBS 239, which places great emphasis on high quality data.

The survey group was asked to describe their most significant data quality issues. The issues raised were diverse but can be summarised as follows:

Some of the key issues raised by the surveyed banks in each of these areas were:

- **Governance and controls**
  - Business not sufficiently aware of where data is sourced from and does not take sufficient ownership
  - Controls over data governance are inconsistent across different silos
  - Poor controls over capture of reference data within the business
  - Unable to check data sufficiently quickly before it is released into the live environment

- **Consistency**
  - The most commonly cited concern was the inconsistency of data from different systems and different parts of the business
  - Two banks which operate global operations commented that inconsistencies in closing prices across different markets can be problematic

- **Incorrect prices**
  - Rogue price data
  - Inability to obtain prices for illiquid securities
  - Difficulties in confirming prices with sufficient independent sources

- **Completeness**
  - Difficulties in sourcing all relevant data, particularly for historic risk calculations (e.g. as required by FRTB) for more exotic instruments
  - Business areas fail to capture all relevant data

- **Transparency**
  - Uncertainties over traceability/lineage of data misstated
The impact of bad quality data can have a major effect on the business, for example in causing transactions to be entered at incorrect prices, misstating risk calculations and causing reconciliation breaks. The majority of banks in our survey reported that they quantify the P&L effect of data errors. However, this tends to be done by the product control or market risk management function and is not fed back to the data management function. One bank commented that “we do quantify the impact of data errors, but it’s not very systematic”.

8. Conclusion

Data management is an integral part of the risk management process. As risk management has changed so has data management, and this can be expected to continue into the foreseeable future. Our survey revealed two main drivers of change:

- Regulation – BCBS 239, FRTB and stress testing were the most frequently cited areas
- Internal drivers to produce a more efficient and cost effective data management function and to reduce operational risk

The implementation of regulatory change requires a specific response to each area of regulation, but many banks have also responded more strategically by reorganising their data management functions – moving them away from being silo-based, to a more centralised structure. A number of the banks surveyed have already achieved this and others are in transition. There are many challenges involved in such an initiative and many banks will not achieve a fully centralised model. Data management may be centralised within risk management, for example, but not for the enterprise as a whole. This may be for organisational reasons or to maintain independence between risk management and the business. Furthermore, many of the largest banks do not strive to achieve a totally centralised EDM function as their organisations are too complex, but centralised data management functions are often created for different types of data.

A centralised data management structure goes hand-in-hand with more centralised systems. Our survey revealed that over half of banks have implemented, or are planning to implement, an EDM solution. Such solutions can improve operational and cost efficiency and allow banks to meet current and future regulatory demands more easily. Many of the largest banks do not implement a single EDM solution, but choose a best of breed solution for each type of data.
About InteDelta

InteDelta helps financial institutions better manage their risk. Through our range of consulting and IT development products we provide assistance in areas such as:

- Risk management policies, methodologies and models
- Target operating model design
- Technology selection, implementation and development
- Market intelligence and benchmarking

Our areas of expertise cover the major risk categories faced by financial institutions: credit, market, liquidity and operational risk. Our consulting work has included many engagements involving the effective management of data. Our global client base covers all geographies and covers global and local banks, asset managers, service providers and technology vendors.

Further Information

If you would like to discuss any of the issues addressed in this report, please contact:

**Michael Bryant**  
Managing Director  
Email: michael.bryant@intedelta.com  
Tel: +44 (0)20 7887 2204

www.intedelta.com
About Asset Control

Asset Control has been the leader in providing supremely reliable, high performance systems for the management of financial data since 1991, helping financial organisations deliver high-quality reference, market and risk data to the people and applications that need it – on time, all the time.

Serving the world’s most successful financial institutions including top-tier banks and investment managers, as well as growing firms across global markets, our software and operational expertise makes processing and reporting possible sooner, with absolute accuracy, and total consistency.

Our systems track every data element from the point of capture to final delivery, giving banks and asset managers the ability to manage costs and achieve the highest standards of data governance. Whether it’s for regulatory compliance, portfolio valuation, or risk management, we deliver data with unequalled efficiency, transparency and integrity.

Contact

<table>
<thead>
<tr>
<th>Country</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>United Kingdom</td>
<td>101 Finsbury Pavement, London EC2A 1RS</td>
<td>+44 (0)207 7430 320</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Trambaan 1-K, 8441 BH Heerenveen, The Netherlands</td>
<td>+31 (0)88 678 7900</td>
</tr>
<tr>
<td>United States</td>
<td>1359 Broadway, Suite 601, New York, NY, 10018, USA</td>
<td>+1 212 445 1076</td>
</tr>
<tr>
<td>Singapore</td>
<td>Level 24 Tower 1, 1 Raffles Place, Singapore 048616</td>
<td>+65 6408 0750</td>
</tr>
</tbody>
</table>

General Enquiries: info@asset-control.com