MEMORANDUM

TO:	Basel Committee on Banking Supervision Baselcommittee@bis.org	FROM:	PJ Di Giammarino CEO, JWG PJ@jwg-it.eu www.jwg-it.eu +44 (0) 20 7870 8004
SUBJECT:	Consultation on principles for effective risk data aggregation and risk reporting		
DATE:	28 September 2012		

Introduction

JWG is a financial services think-tank which works with regulators, investment firms and their information technology supply chain to help determine how the right regulations can be implemented in the right way.

We are delighted to have the opportunity to respond to the BCBS' consultation on principles for effective risk data aggregation and risk reporting so that we may help shape this important regulatory framework.

Over the last 3 years, our research on the challenges firms and regulators face in managing risk information has resulted in a number of reports on risk aggregation. We have supplied consultation responses to the European Banking Authority (EBA) on their Data Point Model[1], and the Financial Stability Board (FSB) on their G-SIB Common Reporting Templates[2] and the LEI initiative[3]. JWG is also engaged with the LEI Private Sector Preparatory Group (PSPG).

Executive summary

The stated policy objectives of "*strengthening banks' risk data aggregation capabilities and risk reporting practices*" and "*enable the fundamental improvements to the management of banks*" are all encompassing. In order to help both firms and regulators apply these principles, we offer five key suggestions:

- Risk data ownership. Accountability should be explicitly assigned **to an individual that is empowered to determine the strategy, target operating model and plans for risk data management** (Principle 1)
- Risk data standards. A **specific call for risk data policies, data quality metrics and standards** should be included (Principle 2)
- Use case rulebook. Data accuracy and integrity should be improved though **a new regulatory tool: the 'regulatory use case' rulebook** (Principle 3)
- Risk reference data. We suggest **adding a 'risk reference data policy' paragraph, including stipulations on quality and use cases** (Principle 4)
- Timeliness. We ask the BCBS to **clarify exactly what timeliness means, what data is current enough** to be fit for purpose and what capabilities are required to produce this information (Principles 5 & 10).

[1] JWG response to EBA's consultation on data point model related to Implementing Technical Standards on supervisory reporting, June 2011
[2] JWG response to FSB's consultation on G-SIB I-I top 50 credit exposure template feedback, May 2012
[3] JWG response to FSB's consultation on LEI expert group execution strategy recommendations, April 2012

Without strong global leadership from the BCBS on these key principles we fear that global alignment of standards on risk data aggregation and reporting will remain theory rather than regulatory for some time to come. Perhaps even more worryingly, we are **likely to introduce both operational and systemic risk back into the system.**

JWG, as always, is very happy to elaborate on these issues further if required.

Governance [Principle 1]

As specified in paragraph 23, banks need to be aware of their own limitations in preventing holistic risk data aggregation, specifically outlined in their 'IT strategy.' This is easier said than done, requiring changes in both ownership and defined focus in order to be successful.

Even if assigned to the bank's board and senior management, the problem here is still ownership of risk management control. Delegating this simply to 'IT strategy' will likely not be specific enough to achieve the intended effect, as issues with ownership of risk data capabilities will continue without a specific person tasked to get the fundamental job of enabling improvement done.

Firms have disparate organisational models for managing risk information but, generally, there is confusion over precisely who is responsible for what. We find that there is scattered ownership across the front, middle and back-offices. We have heard the same story several times: *"Who's responsible for risk data depends on who you ask. Risk people will say it's IT. IT people will say it's Finance. Finance people will say it's Risk. Basically, anyone but me."* Or worse, each function owns a small piece but not enough to see the complete picture. It will certainly be difficult to improve risk data if no one is specifically mandated to take charge of it.

Our research has shown that there are three generalised models firms employ to organise risk data management:

Figure 1: **Attributes of risk data management organisational models**

Organisational type	Distribution	Attributes
Model A: 'Chief Data Officer' figurehead	17%	▶ Disparaged by some firms, but heavily promoted at conferences ▶ Little influence, budget or accountability ▶ Average lifespan of 2 years
Model B: Senior heavyweight	50%	▶ Generally not in technology – either in operations or finance ▶ Serves as focal point for 'run the bank' issues ▶ Customer of the IT function ▶ Takes the lead on 'change the bank' initiatives
Model C: Service function	33%	▶ Reference data shared service ▶ Responsible for getting new identifiers and reference data aligned across silos and owning the infrastructure ▶ Sometimes within the finance department

Source: JWG analysis of risk data processing models based on February/March 2011 survey. 16 firms reporting.

Regardless of organisational construction, when the right data is required for spotting a problem before it turns into a crisis, there needs to be a 'go to' person for risk data.

We believe the problem is larger and more specific than just IT, more properly characterised by having a 'data strategy', owned by a single person. We recommend that paragraph 23 be modified to note that **accountability should to be assigned to an individual that is empowered to determine the strategy, target operating model and plans for risk data management**.

Data architecture and IT infrastructure [Principle 2]

We strongly agree with the call in paragraph 25 for integrated data taxonomies and architecture with singular identifiers and naming conventions across the banking group to support full risk data aggregation capabilities and reporting practices. In practice, however, a focus on these issues exclusively for risk offers only a partial approach to a much wider problem.

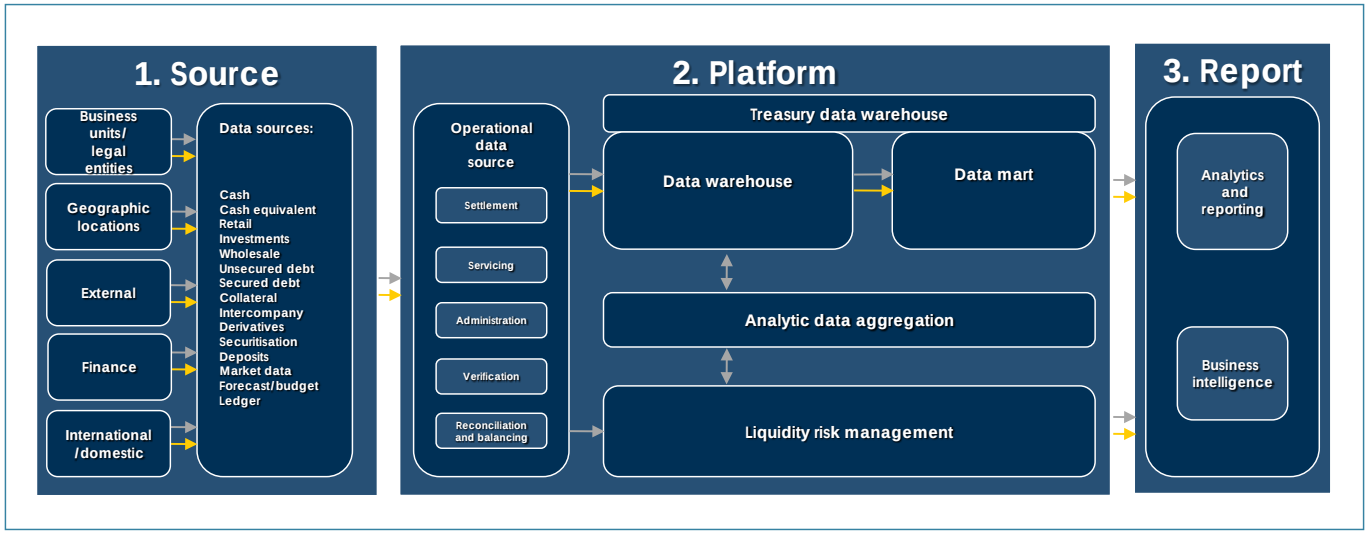
Whilst attempts have been made to create a single data taxonomy (e.g. The EBA's Data Point Model), this effort will not create a data model for all risk management, globally. In today's global banking environment there are hundreds of external regulatory demands on a bank's metadata that are divergent from the DPM.

There are differing regulatory expectations on what risk data aggregation capabilities are required at source, platform and report level. Therefore, building a single architecture requires an understanding of the fact that the metadata will differ drastically accordingly to its particular regulatory use case. Whilst in a regulatory vacuum, it would be possible to use singular identifiers, semantic consistency and unified naming conventions, but business demands make this difficult.

Regulators are becoming increasingly severe in what they are demanding from firms' data aggregation capabilities. In our 2011 research report, '*Clearing the Risk MI bar?'*[4], firms were challenged to aggregate and analyse data according to existing regulatory timelines. As such, they will have to make the jump from being able to aggregate their exposures on a periodic or daily basis to being able to fully calculate where their risk lies on a real-time basis.

From a technology standpoint, firms need to be able to articulate the capabilities required within their technical operating model as illustrated in Figure 2. In order to bring their capabilities in line with regulatory expectations, regulators should work with the industry to define firm-wide risk data policies and data quality metrics or definitions. These definitions should specify what standards should be used for measurement, and when they should be applied.

Figure 2: **Risk data processing**



Source: JWG analysis of risk organisational models based on February/March 2011 survey, 16 firms participating

We support the inclusion of strong roles and responsibilities for the ownership and quality of risk data for business and IT functions, as indicated in paragraph 26. However, we believe more clarity is required on

[4] JWG Analysis Report: '*Clearing the Risk MI Bar?'*, May 2011

terms like "*adequate controls*", "*correctly entered"* and exactly what "*consistent with firms' policies*" looks like. We therefore **recommend that Principle 2 includes a specific call for risk data policies, data quality metrics and standards.**

Accuracy and integrity [Principle 3]

JWG is pleased to see paragraph 29 calling for banks to have a 'dictionary' of risk aggregation concepts used, so that data can be defined consistently across an organisation. This is, in essence, a key piece of infrastructure which needs to be developed for the industry if banks are to have a sound, digestible and effective risk data picture.

Despite the thousands of data points collected by regulators across the globe today, there is no agreed regulatory data dictionary in place. As big market infrastructure changes and hundreds of new data intensive rules are implemented, there is little time for the development of appropriate standards that allow information to be aggregated and compared. This is no small task, especially as both financial and technological innovation continually shifts the goal posts on what information is required.

Because regulators collect their information on firms by jurisdiction, and because there is little common view of the international, systemic landscape, there are no universal semantic models for these data concepts. An example of this can be seen in defining "*sector*" in prudential versus financial reporting requirements. Where in one regulatory reporting template a SIC code is requested, another may require a NAICS code. This means firms have few common standards to adhere to because there is no clear view of what 'good' looks like.

In many instances, reference data used internally within firms follows different formats with limited commonality in fields between vendor, regulator and firm. To support comparability between firms, standardised reference data is required. To illustrate the problem: if firm A refers to its counterparties with acronyms and the firm B refers to theirs with full company names, the counterparty exposure cannot be consolidated or compared without considerable manual intervention or 'scrubbing'. As illustrated in Figure 3, the amount of data cleansing needed to aggregate multiple exposures to these entities could be quite significant for a regulator to be able to trust an aggregate view of firms' counterparty risk metrics.

In short, whilst the data may be captured, it is not possible to transform it into the information required to accurately identify and monitor risk without the universal rules that outline how it should be translated and linked. It should be noted that, before Basel II came into being, there was no explicit regulatory or operational requirement for banks to aggregate their data across siloes or to present it externally across businesses, products and jurisdictions.

Common identifiers are required to fill these gaps. The problem is that such identifiers must be mandated as an independent regulatory requirement to fulfil their potential maximum utility. Examples of identifiers which are currently widely used, such as the International Securities Identification Number (ISIN), show that, even with a legal mandate for use, adoption rates can flounder[5], significantly reducing the overall utility of their purpose.

In addition to common identifiers, regulators and firms must agree the methods by which the data is defined and collected. In a number of risk data collection exercises, we note the heavy reliance on spreadsheets – not only to transmit, but also to model and communicate the information required. It is interesting that a common point of failure (i.e., the use of spreadsheets) is being perpetuated by those who wish to introduce better controls. Consensus needs to be reached on when modelling tools, shared

[5] Consultation response to 6 October FSB consultation paper: 'Understanding Financial Linkages: A Common Data Template for Global Systemically Important Banks'

requirements databases and spreadsheets are appropriate, and also when more robust transmission mechanisms like XBRL and XML are required.

Figure 3: **Example data anomalies**

Qantas Airways Ltd.

	ID	Trading status	Address 1	Address 2	Address 3	City	State	Country	Postcode	Entity type	UP ID	UP name	UP reg country
V		ACTIVE	203 Coward Street	Mascot, N.S.W. 2020		Mascot		Australia	2020	Other Corporate		Qantas Airways Ltd.	Australia
R		Appointed Representative	Qantas House	401-403 King Street		London			W6 9NJ				
F		OPEN	LEVEL 9, BUILDING A, QANTAS CENTRE, 203 COWARD STREET			MASCOT		AU	2020				

ING Bank N.V.

	ID	Trading status	Address 1	Address 2	Address 3	City	State	Country	Postcode	Entity type	UP ID	UP name	UP reg country
V		ACTIVE	Amstelveense weg 500	1081 KL Amsterdam		Amsterdam		Netherlands	1081	Commercial & Investment Banks		ING Groep NV	Netherlands
R		EEA Authorised	60 London Wall			London			EC2M 5TQ				
F		OPEN	AMSTELVEENSE WEG 500			AMSTERDAM		NL	1081				

Same Different Blank V = vendor R = regulator F = firm

Source: JWG analysis of customer data management data quality survey 2010

Lastly, we note an increase in regulatory demands for up-to-the-minute aggregation analysis of 'raw' data. While this practice gives the regulator the ability to run stress tests of their own, it does not give the industry much comfort that the information used for these stress tests is fit for purpose. The 'raw data' collection requirements should be elaborated within the 'use case rulebook' to align multiple stakeholder interests in a single source for risk aggregation standards.

In a nutshell, there must be a clear consensus of what data, codes and data collection methods are mandatory for successful oversight. Use cases which spell out not only what information is required, but how that information will be used, when and under what circumstances is the standard way of achieving this alignment.

For a firm's data dictionary to be effective, regulators will need to work together with the industry to define the rules and quality metrics for each data point required. Accordingly, **we recommend that a new paragraph be added to Principle 3 that addresses the need for a new regulatory tool: the 'regulatory use case' rulebook.** The approach to creating this rulebook is detailed in the following section.

Principle 3 addition: The need for a 'regulatory use case rulebook'

Developing and maintaining use cases is not easy, nor can it be managed via a few workshops, but it is something that the industry has experience with. We recommend that regulators engage with a group of market participants to set an initial agenda and put together a project plan. This group could then meet regularly to review iterative drafts of a use case rulebook, and an accompanying technical specifications manual which would incorporate industry analysis and opinion, to ensure resultant

commitments that (i) were achievable, (ii) incentivised market participants to adopt them and (iii) met regulatory objectives.

The advantages of this approach are that:

- It reduces lead time and regulatory burden of creating and responding to consultations
- It begins with, and is constantly held to, a view of feasibility and clear measures of success
- It promotes innovation and, as such, increases chances of successful adoption
- Is developed upon a foundation of collaborative feedback and analysis
- Is developed iteratively in line with supervisory and market objectives.

There are plenty of precedents for this approach. The European Commission elicited a commitment to developing a European CCP for Credit in 2009, by engaging ISDA to coordinate a commitment letter formulated and agreed to by a number of significant financial institutions. In addition, the OTC Derivatives Supervisors Group (ODSG) has received eight commitment letters since 2005, from G16 member dealers, buy-side institutions and their financial market infrastructure, to a detailed roadmap for market infrastructure change. The programme management of these letters has often been entrusted to a third party, such as Sapient, resulting in the successful delivery and implementation of market standards and infrastructure, such as CCPs (ICE, CME, LCH) post-trade services (central settlement, trade repositories, middleware, portfolio compression and reconciliation) and industry protocols (innovations and 100/500 standard coupons).

Collaboration is key to the success of these use cases. It is vital that leadership, via home-host cooperation, is established in the review, implementation and supervisions of these use cases. The challenge is that multiple stakeholder groups with varying perspectives need to be brought together in a manner which levels the playing field and aligns their interests. It is important that a forum be created that allows multiple jurisdictions' viewpoints to be represented yet remains the single source for risk aggregation standards.

Completeness of risk data [Principle 4]

As stated in Principle 4, we concur that a bank should be able to capture and aggregate all material risk data across the banking group, from a variety of origins, to give a proper picture of risk. Yet, we believe that an essential part of the groundwork is missing for this discussion - specifically the need to place this discussion about risk data in the larger, holistic context.

Without the ability to assemble and pinpoint the correct, contextualised data, firms will not be able to produce information to the specifications of the regulator, or to fulfil their own requirements to chart risk internally. Figure 4 illustrates the relationship between different types of risk data and other datasets within the organisation.

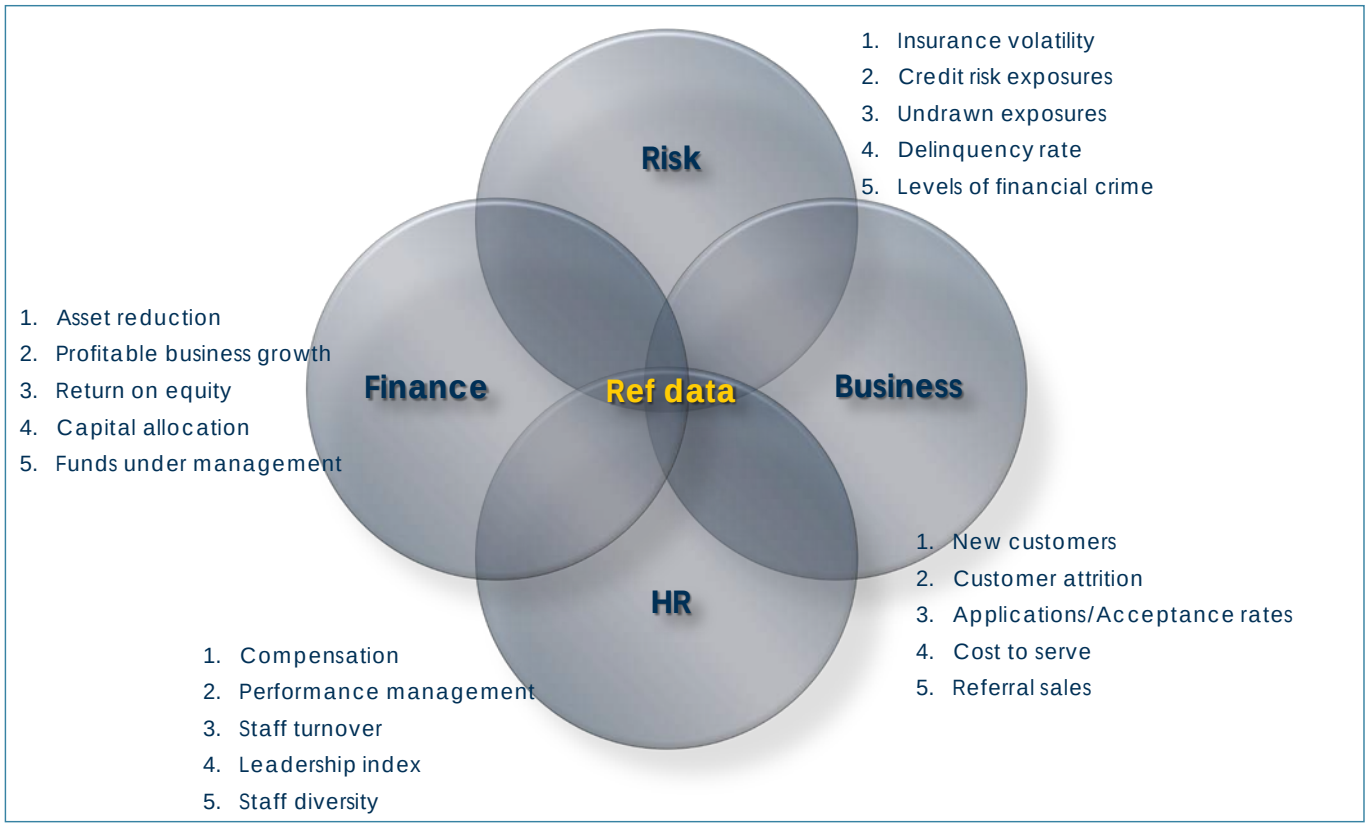
Clearly, the scope of what constitutes risk data could be very, very broad. There are many sources for what can be required for risk purposes. As discussed above, use cases are required to make clear the interdependencies between risk data and other datasets in the organisation.

As shown in the diagram below, reference data forms the core of the risk data discussion due to its foundational role in risk, finance and business and HR data. Firms need to be able to reference common identifiers across the institution in order to fully examine them and have an 'apples to apples' understanding of the issues.

In order to do this, firms will need to define how their risk information is managed in the context of their entire firm. There is little in the way of an overarching strategy as to how all of this information fits together: How does risk data align with finance data? How is HR information or commercial data involved? What does my firm-wide view of data look like from the centre of all of it? And how can I find and use the data

relevant to whatever function is necessary, be it risk exposure aggregation, transaction reporting or real-time post trade reporting? We have not, as yet, found a firm able describe how the management of their risk information plays into the bigger picture of data management at their firm.

Figure 4: **Enterprise view of risk data**



Source: JWG analysis of the potential scope of risk data policy

Addressing this will mean ensuring that completeness of reference data becomes part of a firm's overall data policy. **We suggest adding a 'risk reference data policy' paragraph to Principle 4, including stipulations on quality and use cases.** It must include clear definitions of what "*high quality*" data looks like, including what "*completeness*" and the "*measures*" to determine it are. Furthermore, this should include defined and realistic use cases to exhibit consistent linkages between reference data and how it forms part of a firm's internal risk view.

Timeliness and frequency [Principles 5 and 10]

The timely and accurate provision of key risk data is an indispensable variable in overall risk data quality and efficacy. Consequently, we are pleased to see these standards elevated to principle level in this document.

Despite this, we feel that Principles 5 and 10, regarding timeliness and frequency, are not specific enough, leaving many questions unanswered about what exactly "*timely basis*", "*rapidly produce*" and "*frequency*" mean. With so many potential differing timeliness requirements, including different provisions by data type (liquidity risk data, credit and trading exposures, etc.), and crisis and non-crisis speed requirements, this picture becomes increasingly complicated and opaque.

An example of issues with timeliness requirements is exhibited in the FSB's Common Data Template for Global Systemically Important Banks. In the template, three day timeframes are proposed, that may be, for some banks, unachievable by a multiple of two to four times. Due to the global nature of the template, timing will have to be globally reconciled, i.e., what exactly is a 'global day'? If the report is requested at 6am on a Friday in the UK, what are the implications for a firm's branches in Japan or the USA in calculating deadlines for aggregating that information? If that Friday is a public holiday in the USA and on the following Monday it is a public holiday in Japan how will the information be calibrated? Additionally, what would be the impact of a region unable to produce a report on a given day due to external circumstances (such as a disaster, fire, etc.).

The above difficulties of information collection from different time zones and calendars could result in there being only 24 hours for a firm to be able to fully aggregate their information from across the globe. Such a situation would inevitably mean considerably higher costs in meeting such a deadline. As it stands, many firms are struggling with quickly aggregating their high-level exposures on a weekly, monthly and quarterly basis for just their internal systems. The pressing question is what happens when more risk data demands are added to this already confusing situation?

We recommend that, for the purposes of Principles 5 and 10, **the BCBS clarify exactly what timeliness means, what data is current enough to be fit for purpose and what capabilities are required to produce this information.**

Conclusion

Principles for risk data aggregation are a great step forward for the industry. However, if we do not articulate more clearly what is required, we risk creating an inconsistent picture from which regulators will be forced to make difficult judgements.

Implementing the recommendations above will help ensure that, when the final principles are produced, the industry will truly be ready to make risk data aggregation and reporting a reality in a faster, better, cheaper and, ultimately, safer manner.

