

Independent Data Professionals Group

Nicola Askham	data governance consultant & DAMA Committee Member
Ken O'Connor	data quality management consultant
Mady Korada	enterprise data management consultant – Inpreci
Julian Schwarzenbach	data consultant - Data and Process Advantage & Chair BCS Data Management Specialist Group
David Twaddell	enterprise data management consultant– Inpreci

Telephone: 020 3239 9209

Email: david.twaddell@inpreci.com

Address: 30 Albion Road, Leighton Buzzard, LU7 9AY, UK

27th September 2012

Dear Sirs,

Response to the *Principles for effective risk data aggregation and risk reporting - consultative document*¹ (published June 2012)

The financial crisis from 2007 revealed many banks were unable to aggregate risk exposures fully or quickly enough to prevent serious impacts on the stability of the whole financial system. To counter this, the Basel Committee's proposed *Principles for effective risk data aggregation and risk reporting - consultative document*, part of Basel III, are intended to strengthen banks' risk management capabilities. Basel III becomes law in 2013 with full compliance phased in by 2018

The consultation document gives a high prominence to data, data architecture and data quality. As independent data professionals, we welcome the publication of this consultative document and the opportunity to provide our views. We agree with the objectives of the document and with the principles set out. Our feedback primarily identifies areas of possible ambiguity and includes suggestions on how they may be clarified.

The method we followed was for each expert to review and comment on the whole document. Then we consolidated those comments into a consensus view. The summary below highlights our main points, and our detailed comments are provided under that.

If there are any questions on our comments, or other follow-up activity, please do contact us.

Yours faithfully,



David Twaddell

On behalf of the **Independent Data Professionals Group**

¹ <http://www.bis.org/publ/bcbs222.htm>

Summary of our response

We have classified our responses into several areas. Note that the *detailed response* below has the same classification as the *summary* and this detail section can be used to cross-reference to the specific Sections, Principles and paragraphs in the consultation document.

Benefits of good data management

We agree with the stated benefits that good data management will bring to banks. We also see additional benefits such as *improving the overall confidence in data, reducing speed to market for new products, and lowering the costs of data management.*

Data architecture

We recommend that desktop applications, such as spreadsheets etc, be explicitly included in the scope of data architecture and metadata management. Then they will be subject to the normal IT controls that manage the data in core systems – back-up, security, continuity, software development lifecycle, etc.

Data governance

Where ‘professional judgements’ are required we recommend they be subject to specific controls, in the way that ‘expert judgements’ are treated by Solvency II. Also these judgements may be used to correct defects in completeness and other quality metrics, not just accuracy as indicated by the document.

We assume there should have a continual process to assess changes to banks’ production environments to identify any impacts on risk data architecture.

Data management benchmark

We recommend that a clear and measurable benchmark for data management be identified or established, so that capability can be measured on a maturity scale. This benchmark would cover the principles laid out in the consultation paper, plus some additional material. We think the benchmark should be split into two sections: the first being a generic benchmark covering all bank data, and the second being specific to risk data. We think most principles will apply at the generic level. We think such an initiative could reduce the implementation effort for banks across the board, and reduce the risks of an incomplete implementation by any bank.

Data quality

The document contains several inconsistencies in the way data quality metrics are used. For example:

- ‘Accuracy’ is used in some places in a way that is inconsistent with its definition in the Annex.
- It is not clear what is meant by ‘reliable’ data.
- We think ‘Comprehensive’ is essentially a combination of ‘Complete’ and ‘Timely’, but if not then it should be defined more clearly.
- Example checks given for Completeness are more usually applied to Accuracy. This could be quite confusing.
- Accuracy and Integrity are normally treated separately as they mean different things
- Why not employ the same ‘appropriateness’ metric that solvency II uses?

In addition we believe that the existence of qualitative interpretations at executive levels should not replace the need for quantitative checks at the operation level.

We suggest consideration be given to using the ‘*provenance*’ data quality metric, as defined by ISO 8000 for Data Quality². This is a measure of how well the source of data is understood.

Metadata

It would be useful to say what the ‘dictionary’ of concepts should describe. Is it source, usage and characteristics (as in the Solvency II ‘data directory’)? We think the dictionary should be linked to the ‘taxonomies and architecture’, so that meanings can be linked to metadata.

Other

We think the Annex is very useful and could be extended to include definitions for ‘certainty’ ‘tolerance’, ‘materiality’, ‘business owner’, and other concepts.

We also noticed a few spelling mistakes in the text which we hope you don’t mind us pointing out!

² http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50801&commid=54158

Scope

It would be helpful to provide examples of data and 'data sets' likely to be in scope. We think that compliance costs to banks could be double or treble expectations if the scope is not made clear.

In particular:

- Is original risk data in scope, or if there is a well-controlled and trusted data-warehouse then can scope start from there?
- Is any data that is *material* to risk models in scope, i.e. not just the data that is *used* in the internal models?
- Is data sourced from external suppliers in scope?

Unforeseen effects

The effect of aggregations of smaller banks should be considered. Taken together a group of smaller banks may be material to the overall risk picture. We recommend that sound risk data management policies, as laid out by the Consultation Paper, be established in all banks.

We identify a potential unforeseen consequence of regulating data where datasets that are not in the scope of regulation may become neglected. These datasets may suffer poorer quality as a result. We recommend the management of data quality across all bank datasets, proportional to the materiality of those datasets to the bank, with any additional regulatory requirements on top of that. This will reduce the risks relating to data not identified as material when it should be.

Detailed response

Benefits of good data management

Section / Principle	Original Text	Consolidated comments
8	<p>The adoption of these principles will enable fundamental improvements to the management of banks. These principles are expected to support a bank's efforts to:</p> <ul style="list-style-type: none"> • Enhance the infrastructure for reporting key information, particularly that used by the board and senior management to identify, monitor and manage risks; • Improve the decision-making process throughout the banking organisation; • Enhance the management of information across legal entities, while facilitating a comprehensive assessment of risk exposures at the global consolidated level; • Reduce the probability and severity of losses resulting from risk management weaknesses; • Improve the speed at which information is available and hence decisions can be made; and • Improve the organisation's quality of strategic planning and the ability to manage the risk of new products and services. 	<p>- Improve confidence in the risk data upon which decisions are being made.</p> <p>- Reduce costs - whilst there will be an up-front cost, having a more robust data management framework, as proposed by this Consultation Paper, should Reduce the costs over time associated with finding and fixing poor quality data.</p> <p>- Improve operational response times, e.g. take new products to market more quickly</p>
9	<p>Strong risk management capabilities are an integral part of the franchise value of a bank. Effective implementation of the principles should increase the value of the bank. The Committee believes that the long-term benefits of improved risk data aggregation capabilities and risk reporting practices will outweigh the initial investment costs incurred by banks.</p>	<p>The DRCG supports the Committee's view that benefits outweigh initial and ongoing costs.</p>

Data architecture

Section / Principle	Original Text	Consolidated comments
36	<p>A bank's risk data aggregation capabilities should ensure that it is able to produce aggregate risk information on a timely basis (in respect of a reference date) to meet all risk management reporting requirements.</p>	<p>Clarify that timeliness means not simply that reports can be re-run in good time, but that report data can be re-constituted in good time with all the appropriate data (e.g. most recent data transactions are included)</p>
Principle 6	<p>Adaptability – A bank should be able to generate aggregate risk data to meet a broad range of on-demand, ad hoc risk management reporting requests, including requests during crisis situations, requests due to changing internal needs and requests to meet supervisory queries.</p>	<p>This is more a quality of overall architecture, not just data architecture. Useful to clarify this (so that application and infrastructure architects can be alerted)</p>
28	<p>28. A bank should aggregate risk data in a way that is accurate and reliable.</p> <p>(a) Controls surrounding risk data should be as robust as those applicable to accounting data.</p>	<p>See comment on use of work 'reliable' above</p> <p>(b) We recommend that desktop applications are treated as</p>

<p>(b) Where a bank relies on manual processes and desktop applications (eg spreadsheets, databases) and has specific risk units that use these applications for software development, it should have effective mitigants in place (eg end-user computing policies and procedures) and other effective controls that are consistently applied across the bank's processes.</p> <p>(c) Risk data should be reconciled to accounting data, as well as to a bank's sources and books of record, to ensure that the risk data is accurate.</p> <p>(d) A bank should strive towards a single authoritative source for risk data.</p> <p>(e) A bank's risk personnel should have sufficient access to risk data to ensure they can appropriately aggregate, validate and reconcile the data to risk reports.</p>	<p>part of the overall data architecture and are included in overall IT and data policies and controls.</p>
--	---

Data governance

Section / Principle	Original Text	Consolidated comments
23	A bank's board and senior management should be fully aware of any limitations that prevent full risk data aggregation, in terms of coverage (eg risks not captured or subsidiaries not included), in technical terms (eg model performance indicators or degree of reliance on manual processes) or in legal terms (legal impediments to data sharing across jurisdictions). A bank's IT strategy should include improving risk data aggregation capabilities and risk reporting practices to remedy any shortcomings against the principles set forth in this report, and to match the evolving needs of the business. A bank should identify data critical to risk data aggregation and IT infrastructure initiatives through its strategic IT planning process, and support these initiatives through the allocation of appropriate levels of financial and human resources.	<p>Data Quality reports to the Board and senior Management are implied in this paragraph but it would be better for it to be an explicit requirement.</p> <p>Also, a continual process needs to be established to monitor changes to the IT real-estate that may cause new limitations or changes to existing limitations.</p>
26	Roles and responsibilities should be established as they relate to the ownership and quality of risk data and information for both the business and IT functions. The owners (business and IT functions), in partnership with risk managers, should ensure there are adequate controls throughout the lifecycle of the data and for all aspects of the technology infrastructure. The role of the business owner includes ensuring data is correctly entered by the relevant front office unit, kept current and aligned with the data definitions, and also ensuring that risk data aggregation capabilities and risk reporting practices are consistent with firms' policies.	We recommend that, as well as establishing roles and responsibilities for <i>Data Owners</i> , <i>Process Owners</i> should also have some responsibilities for data they use and create.
30	There should be an appropriate balance between automated and manual systems. Where professional judgements are required, human intervention may be appropriate. For many other processes, a higher degree of automation is desirable to reduce the risk of errors.	The basis and justification of any human judgement should be documented in order to provide an audit trail of why/how an output was derived.
31	Supervisors expect banks to document and explain all of their risk data aggregation processes whether automated or manual (judgement based or otherwise). Documentation should include an explanation of the appropriateness of any manual workarounds, a description of their criticality to the accuracy of risk data aggregation and proposed actions to reduce the impact.	<p>Would be useful to clarify if all processes need to be documented between the ultimate source of data and the risk reporting process.</p> <p>The assessment of the criticality of manual work-arounds does not just apply to the accuracy of data, but to all other</p>

		qualities of data also (e.g. completeness, timeliness, etc).
		It could be useful to have examples of 'good' documentation
Principle 12	Review - Supervisors should periodically review and evaluate a bank's compliance with the eleven principles above.	If possible, please indicate the likely frequency of reviews

Data management benchmark

Section / Principle	Original Text	Consolidated comments
4	<p>Many in the banking industry⁵ recognise the benefits of improving their risk data aggregation capabilities and are working towards this goal. They see the improvements in terms of strengthening the capability and the status of the risk function to make judgements. This leads to gains in efficiency, reduced probability of losses and enhanced strategic decision-making, and ultimately increased profitability. Supervisors observe that making improvements in risk data aggregation capabilities and risk reporting practices remains a challenge for banks, and supervisors would like to see more progress, in particular, at G-SIBs. Moreover, as the memories of the crisis fade over time, there is a danger that the enhancement of banks' capabilities in these areas may receive a slower-track treatment. This is because IT systems, data and reporting processes require significant investments of financial and human resources with benefits that may only be realised over the long-term.</p>	<p>We recommend that a clear and measurable benchmark for risk data management be established, so that banks capability can be measured on a maturity scale (i.e. 1 to 5). This benchmark would include the principles laid out in the consultation paper, plus some additional material.</p> <p>We further recommend splitting the benchmark into two sections, the first being a generic benchmark covering all data, and the second being specific to Risk data. Most principles are likely to apply at the general level.</p>
5	<p>The Financial Stability Board (FSB) has several international initiatives underway to ensure continued progress is made in strengthening firms' risk data aggregation capabilities and risk reporting practices, which is essential to support financial stability. These include:</p> <ul style="list-style-type: none"> • The development of the Principles for effective risk data aggregation and risk reporting included in this report. This work stems from a recommendation in the FSB's Progress report on implementing the recommendations on enhanced supervision, issued on 4 November 2011: <p>"The FSB, in collaboration with the standard setters, will develop a set of supervisory expectations to move firms', particularly SIFIs, data aggregation capabilities to a level where supervisors, firms, and other users (eg, resolution authorities) of the data are confident that the MIS reports accurately capture the risks. A timeline should be set for all SIFIs to meet supervisory expectations; the deadline for G-SIBs to meet these expectations should be the beginning of 2016, which is the date when the added loss absorbency requirement begins to be phased in for G-SIBs."</p> <ul style="list-style-type: none"> • The development of a new common data template for global systemically important financial institutions (G-SIFIs) in order to address key information gaps identified during the crisis, such as bi-lateral exposures and exposures to countries/sectors/instruments. This should provide the authorities with a stronger framework for assessing potential systemic risks. 	<p>The proposed Common Data Template for Global Systemically Important Financial Institutions should include a template for defining and measuring the quality of data concerned, and a governance framework, not just data definitions.</p> <p>Ideally there would be a common system for data definitions, perhaps an extension on LEI.</p>

Independent Data Professionals Group – Response to Principles for effective risk data aggregation and risk reporting - consultative document, June 2012

	<ul style="list-style-type: none"> • A public-private sector initiative to develop a Legal Entity Identifier (LEI) system. The LEI system will identify unique parties to financial transactions across the globe and is designed to be a key building block for improvements in the quality of financial data across the globe. 	
20	<p>A bank should have in place a strong governance framework, risk data architecture and IT infrastructure. These are pre-conditions to ensure compliance with the other principles included in this document. In particular, a bank's board and senior management should take ownership of implementing all the risk data aggregation and risk reporting principles and have a strategy to meet them within a timeframe agreed with their supervisors. For a G-SIB this means by 2016 at the latest.</p>	<p>There is a need to help banks understand what a '<i>strong governance framework, risk data architecture and IT infrastructure</i>' actually is. This could be defined in the Benchmark mentioned in our paragraph 4 comments.</p>
22	<p>A bank's risk data aggregation capabilities and risk reporting practices should be:</p> <p>(a) Fully documented and subject to high standards of validation. This validation should be independent and include review of compliance with the principles in this document. The validation should review the appropriateness and effectiveness of the bank's risk data aggregation capabilities and risk reporting practices, and the quality of the governance surrounding the processes. Independent validation could mean a review by the internal audit function. However, best practice would suggest that an independent validation unit with specific IT, data and reporting knowledge may be better positioned to perform this review. When such an independent validation unit exists, the internal audit function would still review its validation work as part of the audit plan.</p> <p>(b) Considered as part of any new initiatives, including acquisitions and/or divestitures, new product development, as well as broader process and IT change initiatives. When considering a material acquisition, a bank's due diligence process should assess the risk data aggregation capabilities and risk reporting practices of the acquired entity, as well as the impact on its own risk data aggregation capabilities and risk reporting practices. The impact on risk data aggregation should be considered explicitly by the board and inform the decision to proceed. The bank should establish a timeframe to integrate and align the acquired risk data aggregation capabilities and risk reporting practices within its own framework.</p> <p>(c) Unaffected by the bank's group structure. The group structure should not hinder risk data aggregation capabilities at a consolidated level or at any relevant level within the organisation (eg sub-consolidated level, jurisdiction of operation level). In particular, risk data aggregation capabilities should be independent from the choices a bank makes regarding its legal organisation and geographical presence.⁹</p>	<p>The 'high standards' should be further defined or referenced by the Consultation Paper.</p> <p>The level and nature of documentation required to comply with '<i>fully documented</i>' should be made explicit.</p>
25	<p>A bank should establish integrated¹⁰ data taxonomies and architecture across the banking group, which includes information on the characteristics of the data (metadata), as well as use of single identifiers and/or unified naming conventions for data including legal entities, counterparties, customers and accounts.</p>	<p>It would be very useful to include examples of what metadata includes, such as:</p> <ul style="list-style-type: none"> - business definition of the data and usage. - lineage back to source - how data is transformed into new data - where data is stored, and in what form - when data is updated, and by whom - who can access data (security) - how data can be accessed (application architecture)

Data quality

Section / Principle	Original Text	Consolidated comments
1	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 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 the stability of the financial system as a whole.	We understand that the quality of data was also partially inadequate to support the management of financial risks, in which case this point should be made explicitly.
27	Banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks accurately (ie meeting data aggregation expectations is necessary to meet reporting expectations). Compliance with these principles should not be at the expense of each other. These risk data aggregation capabilities should meet all of the following principles below simultaneously (ie no trade-offs that materially inhibit risk management decisions).	The use of the word 'accurately' here is not entirely consistent with its definition in the Annex, or its use in Principle 3. Might be better to use the word 'reliably' here instead.
Principle 3	Accuracy and Integrity – A bank should be able to generate accurate and reliable risk data to meet normal and stress/crisis reporting accuracy requirements. Data should be aggregated on a largely automated basis so as to minimise the probability of errors.	In our view 'reliable' data covers all the qualities of data, including accuracy, completeness, etc. In other words, data is 'reliable' if its accuracy, completeness, timeliness, etc, can be credibly measured and demonstrated. Use of the word 'reliable' here is not entirely consistent with our definition. In our view 'integrity' should have its own definition and principle. Normally, accuracy and integrity are separate qualities of data.
32	Supervisors expect banks to develop metrics to monitor the accuracy of data and for appropriate escalation channels and action plans to be in place to rectify poor data quality. Supervisors could expect banks to monitor and report on the number of data items that are received, compared to the number of items expected.	The check for number received against number expected is usually part of the Completeness quality. A more appropriate check for Accuracy would be to check that the value of each record or transaction received reconciles with the value expected. Where exact accuracy cannot be exactly assessed then a check for the 'validity' of data is often useful.
Principle 4	Completeness – A bank should be able to capture and aggregate all material risk data across the banking group. Data should be available by business line, legal entity, asset type, industry, region and other groupings that permit identifying and reporting risk exposures, concentrations and emerging risks.	Recommend some guidance on what is meant by "material" for greater clarity

35	Supervisors expect banks to produce aggregated risk data that is complete and to develop metrics to measure the completeness of their risk data. Where risk data is not entirely complete, the impact should not be critical to the bank's ability to manage its risks effectively. Supervisors expect banks to affirm that their data is materially complete, with any exceptions identified and explained.	<p>It should be possible for banks to make corrections to incomplete (or inaccurate) data by means of properly controlled 'expert judgement'. The Consultation Paper should include a Principle to describe how such expert judgements should be managed (in line with Solvency II regulations).</p> <p>We assume completeness checks will be required on datasets used in aggregations, as well as the final aggregated datasets.</p>
42	Accurate, complete and timely data is a foundation for effective risk management. However, data alone does not guarantee that the board and senior management will receive appropriate information to make effective decisions about risk. To manage risk effectively, the right information needs to be presented to the right people at the right time. Risk reports based on risk data should be accurate, clear and complete. They should contain the correct content and be presented to the appropriate decision-makers in a time that allows for an appropriate response. A bank's risk management reports should contribute to sound risk management and decision-making by their relevant recipients, including, in particular, the board and senior management. To ensure the usefulness of these reports, they should comply with the following principles. Compliance with these principles should not be at the expense of each other.	<p>Solvency II defines a data quality of 'appropriateness' which covers the requirement to provide the right information to the right people at the right time. It would be useful to align the language and concepts between Solvency II and Basel.</p> <p>We find it confusing to have requirements for 'accurate, complete and <i>timely</i>' data and 'accurate, <i>clear</i> and complete' reports. These juxtapositions should be clarified.</p>
Principle 8	Comprehensiveness - Risk management reports should cover all material risk areas within the organisation. The depth and scope of these reports should be consistent with the size and complexity of the bank's operations and risk profile, as well as the requirements of the recipients.	<p>'Comprehensiveness' is effectively a combination of 'Completeness' and 'Appropriateness' (as we define it)</p> <p>A clear and consistent set of quality dimensions (and definitions supporting them) is required.</p>
52	The balance of qualitative versus quantitative information will vary at different levels within the organisation and will also depend on the level of aggregation that is applied to the reports. Higher up in the organisation, more aggregation is expected and therefore a greater degree of qualitative interpretation will be necessary.	<p>The existence of qualitative interpretations at executive levels should not replace the need for quantitative checks at the operation level. Qualitative interpretations should always be based on sound quantitative measurements where they are available.</p> <p>There is a risk that high impact data errors get lost in the aggregation process. Would recommend a clear requirement to handle this.</p>

Metadata

Section / Principle	Original Text	Consolidated comments
29	As a precondition, a bank should have a “dictionary” of the concepts used, such that data is defined consistently across an organisation.	Would be useful to say what the dictionary should describe about concepts. Is it Source, Usage and Characteristics (as in the Solvency II 'data directory')? We think the dictionary should be linked to the 'taxonomies and architecture' mentioned in para 25, so that meanings can be linked to metadata.
56	A bank should develop an inventory and classification of risk data items which includes a reference to the concepts used to elaborate the reports.	We think this is a good idea, and recommend that this is part of the Data Dictionary previously referred to.

Other

Section / Principle	Original Text	Consolidated comments
Principle 5	Timeliness – A bank should be able to generate aggregate and up to date risk data in a timely manner while also meeting the principles relating to accuracy and integrity, completeness and adaptability. The precise timing will depend upon the nature and potential volatility of the risk being measured as well as its criticality to the overall risk profile of the bank. This timeliness should meet bank-established frequency requirements for normal and stress/crisis risk management reporting.	Typo - 'up to date' should say 'up-to-date'?
Annex 1		We think the Annex is very useful and could be extended to include definitions for 'certainty' 'tolerance', 'business owner', and many other concepts

Scope

Section / Principle	Original Text	Consolidated comments
12	The principles and supervisory expectations contained within this paper apply to a bank's risk management data. This includes data that is critical to enabling the bank to manage the risks it faces. Risk data and reports should provide management with the ability to monitor and track risks relative to the bank's risk tolerance/appetite. ⁷ The data should be forward-looking to provide early warnings of any potential breaches of risk limits that may be against the bank's risk appetite.	It would be helpful to provide examples of data and 'data sets' likely to be in scope. This should make clear what 'risk management data' covers. The compliance costs to banks could be double or treble expectations if the scope is not made clear. It will be useful to clarify if original risk data is in scope, or more simply copies of it (e.g. in a data-warehouse) taken for aggregation purposes.
13	These principles also apply to all key internal risk management models, including but not limited to, Pillar 1 regulatory capital models (eg internal ratings-based approaches for credit risk and advanced measurement approaches for operational risk), Pillar 2 capital models and other key risk management models (eg value-at-risk).	The Consultation Paper should make clear if the scope applies to all data that is material to internal risk models, i.e. not just the data that is used in the internal models.
15	Finally, all the principles included in this paper are also applicable to processes that have been outsourced to third parties.	The principles also apply to any applicable data sourced from external suppliers.

Unforeseen effects

Section / Principle	Original Text	Consolidated comments
11	These principles are initially addressed to SIBs ⁶ and apply at both the banking group and on a solo basis. Common and clearly stated supervisory expectations regarding risk data aggregation and risk reporting are necessary for these institutions. National supervisors may nevertheless choose to apply the principles to a wider range of banks, in a way that is proportionate to the size, nature and complexity of these banks' operations.	The effect of aggregations of smaller banks should be considered. Taken together a group of smaller banks may be material to the overall risk picture. We recommend that sound risk data management policies, as laid out by the Consultation Paper, be established in all banks.