On June 26, 2012, the Basel Committee on Banking Supervision (Basel Committee) released a consultative paper entitled “Principles for Effective Risk Data Aggregation and Risk Reporting.”\(^1\) Stemming from a recommendation made by the Financial Stability Board (FSB), the paper attempts to address one of the key lessons learned from the financial crisis, i.e., banks’ information technology (IT) and data architectures were inadequate to support the broad management of financial risk.\(^2\)

The paper lays out high-level principles for governance of risk data and reporting capabilities. Initially, these principles, which are expected to be implemented by 2016, will be applied to global systemically important banks (G-SIBs) and systemically important banks (SIBs). The initial step toward implementation is expected to be company self-assessments in 2013, which will lead to company and supervisor agreed-upon remediation plans. At their discretion, national regulators, however, may choose to apply the principles to a wider range of institutions.

Comments on the consultative paper are requested by September 28, 2012.

**Applicability**

While banks may consider a broader application of the principles and expectations set forth in the paper, they are intended to apply specifically to banks’ risk management data, including all key internal risk management models, such as Pillar 1 regulatory capital models, Pillar 2 capital models and value at risk models, to name but a few. Additionally, all of the stated principles are applicable to risk management processes that have been outsourced to third parties.

**Points on Which Comments Are Being Requested**

These principles fall into four main categories: governance and infrastructure, risk data aggregation, risk reporting capabilities, and supervisory review. These are summarized below:

**Governance and Infrastructure**

- **Principle 1: Governance** – A bank’s risk data aggregation capabilities and risk reporting practices should be subject to strong governance consistent with other principles and

\(^1\) Principles for Effective Risk Data Aggregation and Risk Reporting, Basel Committee for Banking Supervision, [http://www.bis.org/publ/bcbs222.pdf](http://www.bis.org/publ/bcbs222.pdf).

\(^2\) Ibid.
guidance established by the Basel Committee. This governance framework should be approved by the board of directors and should, among other considerations, include agreed-upon service levels for both outsourced and in-house risk data-related processes and documented policies on data confidentiality, integrity and availability and on risk reporting. Company structure and organization should not hinder data aggregation at the consolidated or any other relevant level within the organization.

- **Principle 2: Data architecture and IT infrastructure** – A bank should design, build and maintain data architecture and IT infrastructure that fully supports its risk data aggregation capabilities and risk reporting practices not only in normal times, but also during times of stress or crisis, while still meeting the other principles. Risk data aggregation capabilities and risk reporting practices should be considered explicitly as part of business continuity planning. Documented logical and physical data models should be established and roles and responsibilities with respect to ownership and quality maintenance of data should be clearly assigned.

**Risk Data Aggregation**

- **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 minimize the probability of errors. Controls supporting risk data should be as robust as those for accounting data. Metrics should be in place to monitor the accuracy of data, with requisite escalation procedures for addressing data quality issues.

- **Principle 4: Completeness** – A bank should be able to capture and aggregate all material risk data, including off-balance sheet risk exposures, 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. Metrics should be in place to measure the completeness of risk data.

- **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. A bank should also evaluate the different data repositories used for collection of data to make sure that real-time data is utilized.

- **Principle 6: 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. Capabilities should include the ability to customize and drill down, as requested, and produce “flash” summary reports.

**Risk Reporting**

- **Principle 7: Accuracy** – Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Banks should maintain defined requirements and procedures for reconciling reports to risk data, automated and manual reasonableness checks, and procedures for identifying and addressing data integrity issues.
• **Principle 8: Comprehensiveness** – Risk management reports should cover all material risk areas within the organization – e.g., credit, market, liquidity, operational, as well as all significant components of those risk areas, such as a single name, country and industry sector for credit risk. Risk reports should also address risk-related measures (e.g., regulatory risk, economic capital) and identify emerging risk concentrations. 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. Banks should report to their boards of directors on forward-looking risks and not just historical risks; board risk reporting should include forecasts and scenarios for key market variables and their resulting impact on a bank’s capital and risk profile.

• **Principle 9: Clarity** – Risk management reports should communicate information in a clear and concise manner. Reports should be easy to understand yet comprehensive enough to facilitate informed decision-making, and should include an appropriate balance between risk data, analysis and interpretation, and qualitative explanations. Boards should be expected to provide feedback to management when risk reports are not providing the right level and types of information they need for informed decision-making.

• **Principle 10: Frequency** – The board and senior management (or other recipients as appropriate) should set the frequency of risk management report production and distribution. Frequency requirements should reflect the needs of the recipients, the nature of the risk reported, and the speed at which the risk can change, as well as the importance of reports in contributing to sound risk management and effective/efficient decision-making across the bank. The frequency of reports should be increased during times of crisis and banks should expect and be able to respond during crisis periods to requests on even an intraday basis.

• **Principle 11: Distribution** – Risk management reports should be distributed to the relevant parties, recognizing the differing needs of various audiences but with a focus on maintaining the security of the information, and include meaningful information tailored to the needs of the recipients while ensuring confidentiality is maintained.

**Supervisory Review**

• **Principle 12: Review** – Supervisors should periodically review and evaluate a bank’s compliance with the 11 principles above. Additionally, new data technology should be evaluated to identify appropriately new capabilities that could enhance achievement of the principles.

• **Principle 13: Remedial actions and supervisory measures** – Supervisors should have and use the appropriate tools and resources to require effective and timely remedial action by a bank to address deficiencies in its risk data aggregation capabilities and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2. Supervisors should be prepared to set limits on risks or growth in the face of significant weaknesses in risk management capabilities and should demand robust risk data before allowing banks to enter into new business ventures or complete an acquisition.
• **Principle 14: Home/host cooperation** – Supervisors should cooperate with relevant supervisors in other jurisdictions regarding the supervision and review of the principles and the implementation of any remedial action, if necessary.\(^3\)

**Expected Points of Consideration**

For some institutions, the investments in financial, IT, and human resources to achieve compliance with these principles will be significant. Anticipated points of consideration with these principles are expected to include:

- **Evaluation of current processes** – Institutions will need to evaluate their current risk data and aggregation processes against these principles and determine where they have known gaps. They will need to develop plans to address these gaps within the next year. Beginning in 2013, their national supervisors, in coordination with the FSB, will begin to assess their plans for achieving these guidelines.

- **Coordination of guidelines and requirements** – Institutions will need to evaluate how these principles will work in coordination with their other global and national requirements and guidelines, such as the data requirements for living wills. They will need to ensure their plan for compliance is fully integrated with all guidelines and requirements.

- **Independent validations** – The guidelines call for independent validations of the risk data aggregation capabilities and risk reporting processes to be performed. Institutions will need to determine if they have knowledgeable and adequate resources to perform in-depth validations or seek additional qualified resources.

- **Data and IT infrastructure** – Given the nature, size and complexity of the institutions’ portfolios, enabling their data infrastructure to allow for the flexibility in risk aggregation reporting may require extensive review and multiple coordination points. This would include available data classifications, IT infrastructure, IT strategy plans, business owner requirements and senior management initiatives. Access to real-time data will need to be evaluated to determine if access to actual production data is needed, which could potentially impact system performance. Additional evaluation will be needed for vendor support, maintenance and handling of critical data. Depending on an institution’s current state, this evaluation may require significant remedies and resources.

- **Cataloging models** – Institutions will need to create a comprehensive model inventory for all models utilized that fall into the Pillar 1 or Pillar 2 categories. All models in the inventory should be classified as high-, medium- or low-risk. High-risk models will require full validations on at least an annual basis; medium- and low-risk models may be reviewed as required.

- **SATA taxonomies and architecture** – Organizations will need to develop data definitions diligently that will be needed to support the reporting requirements and data analysis required by the regulatory requirements. Data design needs to be optimized to avoid duplicating data repositories across an organization and creating potential conflicts with how data is used throughout the organization. A well-thought-out logical data design with an eye on transactional and non-transactional data stores will create a more efficient platform for data analysis and aggregation.

---

\(^3\) Ibid.
• **Governance and controls** – The governance and controls throughout each process and at multiple levels of the organization will need to be top notch to ensure accuracy, integrity, timeliness and completeness of the risk data aggregation and risk reporting processes.

• **Reporting capabilities** – Institutions will need to evaluate their current reporting capabilities and determine if their current systems and processes can support these principles. If not, they will need to build in additional capacity and flexibility. To ensure their capability to meet the distribution, frequency and audience-tailored reporting will be required.

**Summary**

These principles are not intended to be evaluated within silos and must be considered within the context of risk data, risk reporting and risk management. While enhancing the risk management processes may be the initial step in achieving success within the spirit of these principles, institutions may find the process in achieving this success to be valuable in determining other areas that would benefit from building these principles into those processes, such as financial and operational processes.

**About Protiviti**

Protiviti ([www.protiviti.com](http://www.protiviti.com)) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

**Contacts**

Carol Beaumier  
Executive Vice President – Global Industry Programs  
Global Leader – Financial Services Practice  
+1.212.603.8337  
carol.beaumier@protiviti.com

Cory Gunderson  
Managing Director – U.S. Financial Services Practice Leader  
Global Leader – Risk & Compliance Solutions  
+1.212.708.6313  
cory.gunderson@protiviti.com

Andrew Clinton  
+44.207.024.7570 (U.K.)  
andrew.clinton@protiviti.co.uk

Giacomo Galli  
+39.02.6550.6303 (Italy)  
giacomo.galli@protiviti.it

© 2012 Protiviti Inc. An Equal Opportunity Employer. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.