Powerful Insights.
Proven Delivery.®

What Is the Path Toward Effective Risk Data Aggregation and Risk Reporting?

Issue

In January 2013, the Basel Committee on Banking Supervision (Basel Committee) released a publication entitled "Principles for Effective Risk Data Aggregation and Risk Reporting."[1] This document was a follow-up to the request for comments on this same topic in June 2012.[2] The initial consultative paper stemmed from a recommendation made by the Financial Stability Board (FSB).[3] The FSB's paper was aimed at addressing 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 during the financial crisis.

While our paper is focused on the Basel Committee's 14 Principles, there are many regulatory initiatives focused on data, IT systems and reporting – some of these are discussed further below.

The Basel publication 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 banks identified as global systemically important banks (G-SIBs) by the FSB in November 2011 and November 2012.[4] At their discretion, however, national regulators may choose to apply the spirit of the Principles to a wider range of institutions. For example, there is some evidence that banks other than G-SIBs and G-SIFIs in the United Kingdom and Europe are already being asked to provide, on demand, specific risk information by their regulatory authorities, which increasingly appear to be using the "show me" test to validate representations during visits to banks and/or to address specific risks through scenario-based stress testing of what might happen in a significant internal or market event.

Existing G-SIBs will be expected to perform self-assessments in 2013, which will lead to company and supervisor agreed-upon remediation plans. The Basel Committee will begin tracking their progress toward completion in 2013. G-SIBs designated in subsequent FSB annual updates will need to meet the Principles within three years of their subsequent designation. There were no significant changes made to the Principles during the consultative period.

---

[1] Principles for Effective Risk Data Aggregation and Risk Reporting, Basel Committee for Banking Supervision, http://www.bis.org/publ/bcbs239.htm.

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

[3] The FSB was established to coordinate national financial authorities and international standard setting bodies and to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies in the interest of financial stability.

[4] Update of group of global systemically important banks (G-SIBs), http://www.financialstabilityboard.org/publications/r_121031ac.pdf.

protiviti®
Risk & Business Consulting.
Internal Audit.

The 14 Principles as outlined in the paper are as follows:

- **Principle 1: Governance** – A bank's risk data aggregation capabilities and risk reporting practices should be subject to strong governance arrangements consistent with other risk Principles and guidance established by the Basel Committee.
- **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.
- **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.
- **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, as relevant for the risk in question. All data which permits identifying and reporting risk exposures, concentrations and emerging risks should be included.
- **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. Timeliness will also depend on bank-specific frequency requirements for risk management reporting, under both normal and stress/crisis situations, based on the characteristics and overall risk profile of the bank.
- **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 stress/crisis situations, requests due to changing internal needs and requests to meet supervisory queries. The ability for a bank's processes and reporting to be flexible enough to accommodate new and changing factors/developments enables an institution to remain nimble and responsive.
- **Principle 7: Accuracy** – Risk management reports should accurately and precisely convey aggregated risk data and reflect risk in an exact manner. Reports should be reconciled and validated.
- **Principle 8: Comprehensiveness** – Risk management reports should cover all material risk areas within the organization. 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.
- **Principle 9: Clarity and usefulness** – 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. Reports should include meaningful information tailored to the needs of the recipients.
- **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 and efficient decision-making across the bank. The frequency of reports should be increased during times of stress/crisis.
- **Principle 11: Distribution** – Risk management reports should be distributed to the relevant parties while ensuring confidentiality is maintained.
- **Principle 12: Review** – Supervisors should periodically review and evaluate a bank's compliance with the 11 Principles above.

- **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 Principles for effective risk data aggregation and risk reporting practices. Supervisors should have the ability to use a range of tools, including Pillar 2.[5]
- **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.

Impact on Banks

Per the publication, supervisors expect that G-SIBs' data and IT infrastructures will be enhanced in the coming years to ensure that their risk data aggregation capabilities and risk reporting practices are sufficiently robust and flexible to address all potential needs through the normal course of business and during times of stress/crisis.

For most institutions, the investments in financial, IT and human resources to achieve compliance with these Principles will be significant. Each G-SIB's activities to achieve compliance with the Principles will vary; some of the more significant initiatives include the following:

- **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 determine a single authoritative source of risk data to be utilized for each risk type (credit, market, operational, etc.) rather than one source across all risk types. Additionally, institutions have been given discretion with regard to monitoring the accuracy and completeness of risk data for risk data expectations, and they no longer need to reconcile risk data to accounting data.
- **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.
- **Governance** – Board responsibilities require direct oversight of the Principles, while senior management is tasked with execution and timely implementation.
- **Independent validations** – Institutions will need to determine whether they have knowledgeable and adequate resources to perform in-depth independent validations of data governance, sources and uses, including analytics performed on risk data, or seek additional qualified resources to perform effective challenge to their processes. Institutions are not required to have their own independent validation unit within internal audit to verify risk data capabilities and risk reporting. There is more flexibility to integrate independent validation activities into planned independent review activities.
- **Documentation and transparency** – Institutions were given new expectations to strengthen controls on expert judgment, especially as it relates to documentation and transparency.
- **Approximations** – Institutions have new expectations to follow regarding the use of approximations where actual risk data is not available.
- **Data and IT infrastructure** – Given the nature, size and complexity of an institution's portfolios, enabling its data infrastructure to allow for flexibility in risk aggregation reporting may require extensive review and multiple coordination points. Institutions will have to meet increased requirements on the timeliness of risk data aggregation under both normal and stressed conditions.

[5] Basel II: International Convergence of Capital Measurement and Capital Standards: A Revised Framework - Comprehensive Version, http://www.bis.org/publ/bcbs128.htm.

- **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. Additionally, they will need to enhance their forward-looking stress testing reporting capabilities to provide early warning capabilities for exceeding risk limits.
- **SATA (Serial Advanced Technology Attachment) taxonomies and architecture** – Organizations will need to develop data definitions diligently that will be needed to support the reporting requirements and data analysis mandated by the regulatory requirements.

Our Point of View

Enhancements to existing data and IT infrastructures will be needed in order to achieve compliance with the data aggregation and risk reporting Principles set forth by the Basel Committee. Our point of view is focused on the major challenges institutions will face in addressing these Principles and the challenges presented with integration of these Principles and compliance with current and future regulations. These challenges include:

- **Inadequacy of current data systems to accommodate reporting requirements**. Some systems reside within subsidiaries or business lines, thus aggregation of data and having a common view of counterparty exposure are extremely difficult. Additionally, the ability of institutions to manage and capture their data efficiently will enable them to share data more effectively and utilize data sharing and knowledge for the benefit of the organization as a whole.
- **M&A activity is compounding the inadequacy of the current data and reporting systems in place**. Many legacy systems reside in various business lines and subsidiaries and do not communicate or integrate data easily. Under these circumstances, aggregating information to have a common view of counterparty exposure across business lines is extremely difficult.
- **Establishing a holistic, overarching governance structure within the institution to ensure proper project monitoring, escalation of issues and decision-making capacity is a key challenge**. Capacity is another major challenge that G-SIBs will confront. Most of these institutions have "full plates" at the moment in addressing Basel III, stress testing[6] and resolution plans along with executing their business strategy. The ability to undertake additional self-assessments of their risk data, risk reporting and IT infrastructures in 2013 is severely limited by the initiatives already in progress or planned, and further hampered by numerous and ongoing regulatory changes.
- **Institutions will need to balance regulatory priorities by creating a comprehensive plan and team to address the Principles along with current and future regulation**. Institutions will need to enable a cross-functional team to evaluate all regulatory and compliance impacts and create a flexible future state plan to address all current and potential future regulatory pronouncements. Of note, future state needs are changing or are in a state of redevelopment – for example, in the United States, Notices of Proposed Rulemaking on Basel III, the Dodd-Frank Act, and CCAR rules are still evolving, and an end-state is not yet fully known. Globally, there are a significant number of regulatory change initiatives, such as changes to the Capital Requirements Directive (CRD 4) and the Capital Requirements Regulation, the European Market Infrastructure Regulations (EMIR), and the Recovery and Resolution Directive (RRD), as well as proposed amendments to the Markets in Financial Instruments Directive (MiFID). Additionally, there are changes pending to the FSB-initiated Regulatory Oversight Committee (ROC) and Legal Entity Identifier (LEI) initiative.
- **Time frames will pose an automatic challenge for all institutions**. They will have limited capacity to achieve compliance with the breadth of initiatives within the allotted time frame set forth by regulators. It may take institutions a substantial amount of time to evaluate and address risk data, risk governance, risk reporting and IT governance problems, especially those that are

[6] Federal Reserve Announcement on CCAR and CapPR, http://www.federalreserve.gov/newsevents/press/bcreg/20121109b.htm.

enterprisewide and span various business lines. Institutions will need to develop and execute plans quickly to address large overarching data issues.

- **Design and implementation costs will vary dramatically based on an institution's current state versus proposed future state**. There will also be costs associated with accessing knowledgeable resources. Management may have to reallocate time, budget and effort to enable future compliance once the initial self-assessment is completed.

Timely compliance with the Principles requires institutions to undertake a comprehensive infrastructure assessment promptly. For many institutions, this initiative will be a time-consuming, complex and global effort. Among the challenges will be their capacity, historic or current M&A activity, balancing regulatory priorities, ability to meet regulatory time frames, and costs to develop and comply with a future state. However, undertaking a comprehensive risk data infrastructure assessment now will provide management with a better picture to conceive and implement a well-thought-out compliance strategy, as well as offer enough time for effective remediation actions. Immediate action today will become extremely valuable later, as the compliance deadline for the Principles approaches. Additionally, management may benefit from the self-assessment, as it may present simultaneous opportunities to enhance ERM frameworks, productivity and IT operating efficiencies as a result of remediating gaps discovered through the self-assessment. In addition, enhanced risk information available to risk decision-makers in a timely manner allows for quicker and consistent decisions in an "on-demand" environment.

How We Help Companies Succeed

Our Risk and Compliance professionals can help your institution develop and maintain an understanding of what regulatory institutions are seeking from the Principles and facilitate a smooth transition to the new data aggregation and risk reporting standards. Our approaches to compliance with the Principles include but are not limited to:

- Understanding the Principles and their relation to the institution's current risk data, risk reporting and IT infrastructure, and other data and risk regulatory requirements
- Assisting in the creation or stabilization of a strong project management discipline to align overarching project goals with business leaders and management in a timely manner
- Creating and developing a plan for executing a risk data, reporting and IT infrastructure assessment within individual business lines and enterprisewide
- Assisting with self-assessments by utilizing our deep understanding of both the business and technical requirements of complex risk data and reporting infrastructures; identifying gaps in the risk data, reporting and IT infrastructure; and developing and establishing a flexible plan to address them
- Developing an integrated plan to enable the institution to evaluate all regulatory compliance initiatives holistically, aligning with its ERM framework, risk appetite, IT governance and overall business strategy
- Helping clients create policies and procedures surrounding their future state plans and preparing internal employees for changes through the development of training and supporting materials
- Developing reporting templates and unique data dictionaries to be utilized enterprisewide, and assisting in the determination of where risk data, reporting or IT governance nuances are needed for individualized business lines
- Implementing the designed future state risk data, reporting or IT governance plans within business lines or enterprisewide
- Assisting with audits of implemented changes in risk data, reporting and/or IT governance to evaluate actual implementation within business lines and/or enterprisewide

Examples

Top 15 Global Bank: CRO Risk Dashboard Design – We assessed the periodic information reporting packages received by the chief risk officer and benchmarked content against leading industry practices. We then redesigned the content and format, streamlining more than 600 pages received monthly into a concise, action-oriented 70-page monthly report. We consolidated data from multiple subsidiary banks across geographies to define a single, unified and cascading reporting package across various risk types, including credit, market and operational risks.

Top 10 US Bank: Credit Risk Data Governance Design and Implementation – We assisted in developing and implementing a robust data governance program to support credit activities from a strategic, regulatory and management reporting perspective. Our activities were centered on data quality monitoring and management along with data management and control, and we helped the institution establish a data culture. We created a comprehensive data governance framework and multilayer data governance organizational structure, and assisted in prioritizing the most critical data elements from a population exceeding 1,000 elements, mapping data lineage from a system and process perspective and creating a data authority matrix. In addition, we:

- Developed a proprietary data quality scoring methodology leveraging our Risk Index Methodology.
- Created a formal robust data governance policy document, data dictionary and quick reference tools.
- Created and implemented a detailed data element change process and an effective quality control process.
- Created and delivered a comprehensive training program to drive adoption of new processes, which produced new multivariable data quality scorecards.

Protiviti is well-positioned to assist clients in working through these Principles in relation to their current infrastructure, strategy and initiatives, and can help support the entire compliance process.

About Protiviti

Protiviti (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
Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Cory Gunderson
Managing Director
+1.212.708.6313
cory.gunderson@protiviti.com

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

Shaheen Dil
Managing Director
+1.212.603.8378
shaheen.dil@protiviti.com

Michael Schuchardt
Managing Director
+1.415.402.3620
michael.schuchardt@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.