Allan D. Grody, President
Financial InterGroup Advisors
169 East 69th Street - 18th floor
New York, NY 10021
Tel. 212 585 0409
Mobile 917 414 3608

Robert M. Mark, PhD, Chief Executive Officer
Black Diamond Risk
3478 Buskirk Ave, Suite1007
Pleasant Hill, California 94523
Tele. 925 746-7186
Mobile 925 2127348

May 29, 2007

Re: Federal Register/Vo. 72, No. 39/Wednesday, February 28, 2007 Request for Comment on Supervisory Guidance for Basel II Implementation

Office of the Comptroller of the Currency
250 E Street, SW Mail Stop 1-5
Washington, D.C., 20219
Docket # OCC-2007-004
regs.comments@occ.treas.gov

Jennifer J. Johnson
Secretary
Board of Governors of the Federal Reserve System
20th Street & Constitution Ave., NW
Washington, D.C., 20551
Docket # OP-1277
regs.comments@federalreserve.gov

Robert E. Feldman Executive Secretary
Attention: Comments
Federal Deposit Insurance
550 17th Street, NW Washington, D.C., 20429
comments@fdic.gov

Regulation Comments
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW Washington, D.C. 20552
Attention # 2007-06
regs.comments@ots.treas.gov

Dear Madam and Messrs.:

As practitioners and academics in risk management we offer our comments regarding your agencies request to respond to the Notice of Proposed Regulation "Proposed Supervisory Guidance on Advanced Measurement Approaches for Operational Risk".

Very truly yours,

Allan D. Grody

Dr. Robert M. Mark

Response to the Notice of Proposed Regulation "Proposed Supervisory Guidance on Advanced Measurement Approaches for Operational Risk" as recorded in the Federal Register/Vo. 72, No. 39/Wednesday, February 28, 2007

Prepared by
Allan D. Grody and Robert M. Mark, PhD

May 29, 2007

Overview

Federal regulators have introduced new operational risk requirements within the previous mandate to calculate operational risk capital for globally active financial enterprises. For example, the proposed US implementation of final regulatory guidelines for Basel II related to operational risk (Federal Register, Notice of Proposed Regulation, 2007[1]) calls for a "*consistent and comprehensive capture and assessment of data elements needed to identify, measure, monitor, and control the bank's operational risk exposure. This includes identifying the nature, type(s), and underlying cause(s) of the operational loss event(s).*"[2]

Basel II states with respect to understanding and approving the bank's tolerance for operational risk that "*Banks use several approaches to define operational risk tolerance, including establishing expectations for control self assessments, establishing targeted ceilings for operational losses, developing key risk indicators, or establishing other qualitative expectations for operational risk management. These approaches will continue to evolve and banks are encouraged to develop effective metrics to define their operational risk tolerance.*" [3]

Unfortunately, we have not yet achieved a meaningful calibration of operational risk capital nor have we engaged in comprehensive debate on how to measure operational risk. Specifically, a primary reason for failing to arrive at a reasonably useful measure of operational risk is that we have not yet defined the fundamental nature of the measurement unit (or units) of operational risk. We have for all practical purposes deliberately postponed the measurement of operational risk by defining it in terms of a "qualitative" **assessment process** rather than a quantitative **measurement process**. This has left financial institutions to ponder how to link operational loss events to their frequency and severity measures of operational risk. If available (and not much is yet available) then operational risk loss data is rather inelegantly utilized to determine the parameters of a typically poorly articulated operational risk model for calculating the 99.9% confidence interval over a one year horizon.

---

[1] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007, Proposed Supervisory Guidance for Internal Ratings-Based Systems for Credit Risk, Advanced Measurement Approaches for Operational Risk, and the Supervisory Review Process (Pillar 2) Related to Basel II Implementation; Notice Beginning at Page 9084

[2] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices. Page 9170

[3] Ibid, Page 9173, footnote 13

A mapping of loss events into business lines and event types is well on its way in the largest, most internationally active financial institutions that are mandated to comply with the Basel II AMA operational risk approach. Nevertheless, missing from the typical mapping are the causal events at a sufficient level of granularity that resulted in the losses. This failure makes it more difficult to observe risk exposure and perform risk mitigation. Unlike market risk and credit risk, increasing operational risk has no upside and therefore, every operational loss event is a drain on capital, rather than a calibrated risk for a potential reward. A first step to calculating a risk based operational capital charge calls for understanding the causal events, measuring the risk inherent in the operations associated with these events, and doing so around a common risk measurement framework. We have, unfortunately failed to develop effective risk metrics in our rush to satisfy the regulators' well intentioned interest in calculating operational risk capital.

How did we get to a point today where most, if not all experienced practitioners agree that we are not yet on the right path to accurately measuring operational risk? How… well we simply abrogated the difficult task of measurement to the easier path of a subjective assessment. We have also misunderstood how to accommodate relevant data such as reference data.

Reference data, as used in Basel II refers in part to both internal and external (third party) data that is used to establish the underlying criteria from which credit risk analysis is performed and credit risk exposure is modeled.[4] In fact, reference data is a much broader term used by operations management. For example, reference data represents the data elements comprising: financial products and their changing specifications (corporate actions); identification of supply chain participants i.e. counterparties, financial intermediaries, corporations, issuers, etc; financial markets and currency designations; valuation and market prices; and referential information i.e. credit ratings, external loss event data, economic data, financial reports, etc. Reference data is costly to acquire and maintain, duplicative across the industry, and comprises 70% of the data content of financial transactions.[5]

Faulty reference data has been a persistent impediment to systemic risk mitigation across the global capital and investment markets.[6] However, its consequences are not yet fully appreciated in fulfilling the new requirements of identifying casual factors in operational loss events. Risk managers should now be focusing on the importance of reference data as they ponder the underlying dynamics of operational loss events.

---

[4] Ibid, Page 9100

[5] Grody, Allan D., Harmantzis, Fotios and Kaple, Gregory J., "Operational Risk and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation". Available at: http://ssrn.com/abstract=849224

[6] Group of Thirty, Global Clearance and Settlement, Final Monitoring Report, May, 2006

The failure to take a broader view in analyzing reference data has led to negative consequences for both market risk and credit risk calculations. For example, historically most organizations failed to identify a comprehensive well defined separate "operational risk bucket" to place operational losses in. Many operational losses were most likely identified as either a credit risk (e.g. a counterparty misidentification, an improper delivery vs. payment address, an improper account allocation, etc.) or a market risk (e.g. wrong product identification, missed stock-split date, improper conversion rate, etc.). Now, within the new mandate of Basel II, faulty reference data should find its way into the right operational risk bucket. The key is to implement an appropriate operational risk management framework which contains causal relationships that drive these operational loss events.

Another opportunity to set the financial industry on the right operational risk path was opened up within the Basel II accord when it was revealed that insurance, as well as operational risk mitigates other than insurance[7] were available to be used to mitigate operational risk.[8] Nevertheless, it failed to recognize the practical aspects of how insurance was already used in the industry. Risk mitigation does not come neatly packaged as an insurance policy, but rather as partially self insured captives of the large financial institutions, operating as infrastructure entities such as payment systems, transaction netting cooperatives, matching facilities, central securities depositories and clearing houses, each with its own combination of paid-in capital, self insurance, underwritten primary insurance, and/or re-insurance. To date, these structures have only been applied to the value portion of transactions (principally quantities, transaction prices and amounts), but whose risk mitigating techniques can be applied to the matching and "clearing" of the reference data components of these transactions as well.

To further define our views in these three critical areas, **Measuring Operational Risk, Redefining Data in the Context of Operational Risk, and Redefining Risk Mitigation** we offer in the following pages commentary and suggestions for some new considerations.

Measuring Operational Risk

Measuring operational risk has proven to be a significant challenge. This challenge includes accounting for long modeling time horizons, lack of adequate levels of loss data, significant divergence of expert opinion, and lack of uniform global regulatory and data standards. Further, if the measurement approach used is not objective or there has been a failure to secure well designed internal and external loss data, then the measures of operational risk will be flawed.

[7] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices. Page 9184
[8] Ibid, Page 9180

A major operational risk challenge is the endless number of ways in which any particular operational risk might be classified in terms of both its nature and its underlying cause.[9] For example, people risk would include the case where persons are able to manipulate weak controls, evade risk controls, and enter false information into the system of record. A trader may misrepresent actual trades such as systematically falsifying trading bank records and documents as well as taking a position beyond the authorized limits without being detected. In isolated cases, the temptation has been for traders who have caused losses to cover them up and then engage in high-risk, but potentially high-reward, trading strategies to recoup the losses before they are noticed.

The Risk Committee of the Bank for International Settlements (BIS) acknowledged that developing a common measurement framework for operational risk is a major challenge when it stated in a 2003 consultative paper that *"Reflecting the different nature of operational risk, for the purposes of this paper, management of operational risk is taken to mean the 'identification, assessment, monitoring and control / mitigation' of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the 'identification, measurement, monitoring and control' of risk".*[10]

Thereafter, operational risk was firmly focused on assessment (i.e. categorization, as in red/amber/green, high/medium/low, a scale as in 1 to 10, etc.) but not on a measurement approach that is highly predictive of the actual operational risk losses. In the absence of a consistent and comparable risk measurement method, risk management does not have a means of conveying to operating management the risk parameters that have been approved for its operations since there is no consistent and comparable basis of measurement through which such risk can be "budgeted" and thereafter monitored. Reliance is placed almost exclusively on qualitative performance management mechanisms such as Risk Control Self Assessments (RCSA), Key Performance Indicators (KPI) and Key Risk Indicators (KRI).

There are a number of identifiable KRI metrics that tend to be strongly correlated with operational risk exposure. For example, in the case of system risk, a KRI may include the age of computer systems, the percentage of downtime as a result of system failure, etc. Ideally, a KRI is supposed to be an entirely objective measure of some risk-related factor in a financial institution's activity.

A well designed KRI can be used to monitor changes in operational risk for each business and for each loss type. A KRI provides a mechanism to alert management to a rise in the likelihood of an operational risk event. Unwelcome changes in a KRI can be used to prompt remedial management action, or can be tied to incentive schemes so that managers are given an incentive to manage their businesses in a way that is sensitive to operational risk exposures.

---

[9] Crouhy , Galai and Mark; 2005, Risk Management (McGraw Hill)

[10] Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, February 2003

Devices such as a KRI and RCSA tool are unquestionably valuable but suffer from their inherent subjectivity. Line managers generally set their own trigger or threshold points to differentiate between categories of risk in the case of a KPI and KRI. Nevertheless, the major limitation of indicators and self-assessments is that they don't carry financial values. They are only an indication or an admission of a possible issue or risk with little or no information as to its size or historical correlation with actual loss events or financial consequence. Consequently, indicators and assessments are non-additive and, therefore, cannot be aggregated to provide consistent and comparable 'top-down' profiles of operational risk at all levels of the enterprise. This constitutes a serious problem in the risk management of operations.

Partial solutions to this problem are already imbedded in Basel II's suggested framework. For example, the regulators allow for and define Scenario Analysis[11] as *"A systematic process of obtaining expert opinions to derive reasoned estimates of the likelihood and loss impact of plausible high severity Operational Loss events"* consistent with the regulatory soundness standard. Within an institution's operational risk framework, scenario analysis may be used as input or may be used to form the basis of an operational risk analytical framework. However, in scenario analysis there is no mechanism to associate at any granular level the causal factors within the operations directly to the loss event generated from this analysis, nor is there any mechanism to value the risk exposures to this scenario within the operations.

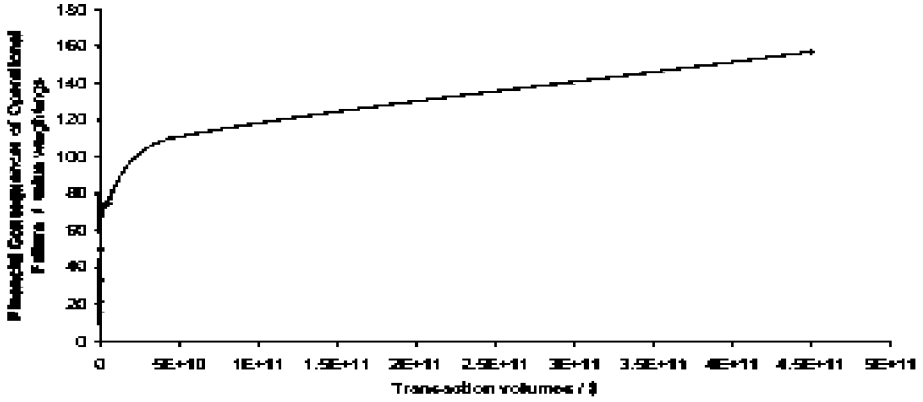
Predictive risk models lose their initial subjectivity and gain accuracy over time by adjusting the risk model through the continuous examination and analysis of the correlation between measurements of risk and actual loss experience. The outputs of a KRI, RCSA, and Scenario Analysis are severely limited, since they are subjective in nature and not expressed in value-bearing units of measure that typically correlate directly with actual loss experience. Consequently, no statistical device has yet been made available that would have the effect of fully reducing the subjectivity inherent in such tools and methods and thus, over time, increase their accuracy.

The lack of a value-bearing operational risk measurement methodology and the inability to correlate actual loss events with operational risk exposure measures has been an impediment to successfully developing risk management techniques for operational risk within the context of the Basel II framework. Therefore, creating such a value-bearing operational risk metric is of paramount importance. We offer the basic premise that operational processes drive exposure to operational risk. Banks construct operating environments comprised of people, technology, facilities, processes and controls to handle transactions and reduce operational risk. Operational risk increases as the volume and relative complexity of transaction throughput increase.

[11] Board of Governors of the Federal Reserve System, March 22, 2006, Basel II Capital Accord, Notice of Proposed Rulemaking (NPR) and Supporting Board Documents, Board memorandum.

In general, operational sophistication increases as transaction volumes increase primarily due to enhanced automation. The relative quality and effectiveness of risk mitigation measures also increase as transaction volumes increase. The net result is that the rate at which operational risk exposure is created decelerates relative to the rate at which transaction volumes increase. An approach, therefore, to measuring operational risk recognizes this relationship and progressively reduces the rate at which risk exposure is valued relative to increased transaction volume. This concept is reflected in the graph displayed in Figure 1 and is also discussed in a paper published by the Federal Reserve Bank of Boston in January 2003. [12]

Scaling Operational Risk Measurement – Figure 1



Source: ARC Technical Paper, April, 2007[13]

Our further premise is that all financial processes are inherently associated with values. If a process fails then the transaction volume and associated values, whether they are revenue, cost or market related (as in valuing security positions) should drive the amount of loss that can be potentially incurred. For example, assigning transaction volumes to predetermined value bands and assigning a standardized risk weighting to each band would allow for a direct correlation with operational risk measurements, tying operational risk to the financial and operating performance of the bank.

These value bands that are assigned to the curve shown in Figure 1 are designed to demonstrate the linkage between the financial consequences of operational failure (converted into value band weightings) and associated transaction volumes. As a consequence, an increase in transaction volumes will directly result in an increased risk of operational failure.

[12] Capital and Risk: New Evidence on Implications of Large Operational Losses", P. de Fontnouvelle, V. DeJesus-Rueff, J. Jordan, E. Rosengren, Federal Reserve Bank of Boston, September 2003
[13] See http://www.ARC1.co.uk

The graph in Figure 1 illustrates the idea that the rate of change in financial consequences with respect to transaction volumes decreases with an increase in transaction volume along the volume band spectrum. Hence a change in transaction volumes in the lower end of the spectrum will result in a more dramatic change of financial consequence, but as the transaction volumes become more substantial, the same change will result in a proportionally smaller increase of financial consequence. This continues to be the case until the curve asymptotically tends towards obtaining a zero derivative where the curve is capped. In this case, any further change in the transaction volumes will result in a zero rate of change for the financial consequences of failure, due to the fact that the total amount of losses that a bank can withstand is limited by its capital.

We believe that developing business "process maps" for each business is an important element of operational risk management. For example, a bank might map the business process associated with the bank's dealings with a stream of payments, or a process with counterparties. The bank might extend these process map descriptions to create a full "operational risk catalogue" for all the bank's businesses. This catalogue would categorize and define the various operational risks arising from each organizational unit in terms of people, process, data and system/technology and map these to the value bands described previously. It would include analyzing the resulting "risk units" calibrated from associating risk factors with process volumes and with value bands. These calibrations could then be benchmarked with other processes, and with other organizational units similarly calibrated. Accordingly, similarly calibrated risk units associated with processes and organizational units within a single bank can be benchmarked against other financial institutions for relevance and for calibration as a standard. Over time such measures will become a predictive measure of loss events and hence a mechanism for the actions banks needs to take to manage and mitigate operational risk.

Redefining Data in the Context of Operational Risk

It was not so long ago when discrete business activities were contained within legal entities within sovereign states. Legal entity financial statements were the single source of knowledge concerning that business's performance and condition. This is no longer the case. The information technology revolution has allowed business information to go global and, for internationally active businesses, it now transcends both the legal basis and geographical sovereignty of its regulators.[14]

Business performance management, risk management and data management have become inextricably linked. The new mantra is Enterprise Data Management (EDM).[15] In fact, building a superior EDM approach is a necessary condition for a successful Enterprise Risk Management (ERM) program. Data integration, data warehousing and the business intelligence applications that consolidate, aggregate, analyze and distribute

[14] Grody, A., Hughes, P., Business Information Challenge…Transforming Data into Knowledge, Financier Worldwide, May, 2007
[15] http://www.edmcouncil.org/

data and reconstitute it into business information are what business executives rely on to manage their businesses. It is left to their risk managers and finance directors to organize the data into financial statements and regulatory reports so that they can be used by the accountants, tax offices, regulators and auditors that need them.

This development raises a few rather important questions. How concerned should we be at this apparent divergence between the data contained within business information and financial statements? For example, should M&A dealmakers and new owners be as concerned with the quality of the business information they will acquire as they are with audited financial statements? And how will new owners know the quality of what they are acquiring if there are no generally accepted standards by which to measure the risk inherent in the data, or putting it into operational terms, how to value the quality of the data being used?

Financial institutions first need to clearly and precisely establish a comprehensive taxonomy for each of the myriad of operational risk elements. For example, in the case of operational losses, the external cost should include the gross cost of compensation and/or penalty payments made to third parties, legal liability costs, regulatory taxes or fines, and costs associated with loss of resources. These should also include the cost to fix, write-down, and resolve the underlying causes of the loss. However, these losses should not include infrastructure costs such as controls, preventive action, and quality assurance nor should they usually include investment in upgrades or new systems and processes.

Federal regulators and, in an indirect way, the financial services industry have already begun to concern itself with data quality. In the Federal Register, Notice of Proposed Regulation, 2007 it states *"For example, mergers and acquisitions potentially change the operational risk profile of the bank, pose challenges in implementing operational risk management, data and assessment, and quantification processes of the affected banks, and consequently raises supervisory issues regarding a bank's AMA system."*[16] . Data is behind business information. Data is the raw material from which information is developed, interpreted and distributed. Faulty data leads to defective or poor quality information which in turn leads to faulty business decisions. It also leads to increased operational risks. Underlying these operational risks are potential information lapses directly linked to data quality issues.

Financial transactions can be thought of as a set of computer encoded data elements that collectively represent 1) standard reference data, identifying it as a specific product defined by its initial offering terms and conditions, and bought and sold by specific identified counterparties and their beneficial owners, 2) variable transaction data such as traded date, quantity and traded price, and 3) associated referential information such as credit ratings, standard payment and settlement instructions, and corporate action information.

[16] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices. Page 9171, footnote 5

Transactions fail if data is faulty or the data recorded in sending and receiving systems are inconsistent and can't be matched. Regulatory and compliance failures result if supply chain or product reference data do not contain the correct reporting classifications. Financial accounting and reporting processes fail if account and cost center codes are faulty or are not correctly specified in transactions and reporting matrices. Losses of revenue can occur if sales volume or particular trades are incorrectly valued due to faulty price and rate related data.

The reference data components of a financial transaction identifies it as a specific financial product (security number, symbol, market, etc.), its unique type, terms and conditions (asset class, maturity date, conversion rate, etc.), its manufacturer or supply chain participant (counterparty, dealer, institution, exchange, etc.), its delivery point (delivery, settlement instructions and location), its delivery or inventory price (closing or settlement price), its market reference prices (last sale, bid/ask quote) and its currency. Analogous to specifications for manufactured products, reference data also defines the products' changing specifications (periodic or event driven corporate actions), occasional changes to sub-components (calendar data, credit rating, historical price, beta's, correlations, volatilities) and seasonal incentives or promotions (dividends, capital distributions and interest payments).

Reference data should be consistent across each financial transaction's life cycle and throughout its supply chain. When reference data that should be identical are not, it causes miscalculated values, misidentified products, and involvement with erroneous supply chain partners (trade counterparties, custodians, paying agents, et al). These individual transaction failures cause monetary loss, higher labor costs, and the potential for both transactional and systemic failure. The problem, simply stated is that each financial institution or supply chain participant has independently sourced, stored and applied reference data to their own copy(s) of their master inventory and counterparty data bases. When this is applied to the variable components of a financial transaction (i.e. quantity and transaction price), and an attempt made to match, identically, the details sent by counterparties and supply chain participants in order to accept and pay for the transaction, significant failures in matching occurs.

There have been many attempts to estimate costs and losses associated with reference data but they have all been based upon surveyed opinions and anecdotal evidence. Recent research estimated that each of the largest financial firms have embedded annual costs on average between $238 million and $1,242 million comprising direct costs, losses and operational risk related capital.[17] Of the total, 35% to 52% represent losses caused by faulty reference data.

[17] *"Operational Risks and Reference Data: Exploring Costs, Capital Requirements and Risk Mitigation"* Allan D. Grody, Fotios C. Harmantzis, Gregory J. Kaple – February, 2007

In a sample survey of 30 international banks conducted by the Basel Committee on Banking it was found that the highest loss event category was "Execution, Delivery and Process Management" a category defined as "Losses from failed transaction processing or process management, from relations with trade counterparties and vendors" that implicitly contains the consequence of faulty product related reference data. This category accounted for approximately 42% of total operational loss events, with a total loss value of €908,000 (34.8% of the total). In this same survey, another event type "Clients, Products & Business Practices" defined as "Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product" represented 27.5% of overall losses, a category that also contains reference data.[18] Unfortunately, in the instructions to those who where asked to participate in the sampling, this loss event category was described as the tail end of a flow chart. If one made it to that end point and had not yet categorized losses in any other category, the remaining losses would be categorized as Execution, Delivery & Process Management. In hindsight this is obviously not a satisfying way to categorize what turns out to be the largest loss event.

In a follow-up survey of 27 US banking institutions conducted in 2004 by the U.S. Federal Reserve and thrift regulatory agencies and reported on in May, 2005, an additional event type and business line category "Other" was added, post facto, which resulted in the largest category of losses.[19] This loss for the event type "Clients, Products & Business Practices", $5,820.5 million, represented 67% of this new "Other" business line category and 80.8% of overall losses.

This data collection exercise was, unfortunately, also flawed. For example, 1) while all respondents submitted data for the Retail Banking business line, only half submitted data for Corporate Finance, 2) respondents reported losses at a mix of different threshold levels, from $0 and above to $10,000 and above, and 3) in aggregating the data, the 'Other" business line, representing the largest total loss amount ($6,122.5 million and 70.8%) had to be created because of an inability to map these losses to any of the eight previously identified business lines. The authors of the data aggregation exercise stated that this suggested the classification of losses affecting more than one business line remains an industry challenge. We suggest that it may also point to the fact that some components of the transactions that underlie these losses are inherently systemic in nature. Given the pervasive nature of reference data in 70% of financial transactions, it also suggests that in future loss data collection exercises a more granular look at the accumulation of loss data related to faulty reference data is warranted, perhaps to be accounted for in a similar manner as one aggregates retail credit loss or check fraud data.

---

[18] QIS2 - Basel Committee on Banking Supervision, The Quantitative Impact Study for Operational Risk: Overview of Individual Loss Data and Lessons Learned, January 2002

[19] U.S. Federal Reserve, The Quantitative Impact Study 4 (QIS4) and the Loss Event Collection Exercise, May, 2005

Redefining Risk Mitigation

A key part of the measurement process is to take mitigation of operational risk into consideration. For example, a firm may be operating in an environment in which the structure and culture, practices and oversight are flawed. Mitigating effects include implementing strong and enforceable back-office controls, including such practices and protocols as strict reconciliation of trade confirmations and a clear segregation of duties between the front, middle, and back offices.

At its heart, the focus of Basel II is on providing capital reduction incentives for those financial enterprises that mitigate their risk. The Basel Committee has stated that banks will be allowed to reduce their capital allocations for operational risk by as much as 20% through the use of risk mitigants, such as insurance. Regulators have stated *"The bank may adjust operational risk exposure results by no more than 20% to reflect the impact of operational risk mitigates"* [20] and *"Currently, the primary risk mitigant used for operational risk is insurance"*.[21] Thus, while the AMA methodology recognizes the risk mitigation impact of insurance in the measures of operational risk, the benefit will be limited to 20% of the total operational capital charge, and this has proven to be a contentious point. Also, insurance coverage by itself does not guarantee a dollar for dollar reduction in capital requirements. Regulators will determine the impact of insurance on capital requirements using a process of both qualitative and quantitative judgment. Regulators will first consider issues concerning the rating of the insurance provider and the terms of the insurance contract. After this, regulators will take into account the treatment of residual risks such as payment uncertainty, payment delays and counterparty risks, which are inherent in using insurance coverage

Of particular interest in risk mitigation offsets is the 30 largest, internationally active financial enterprises headquartered in the US. Currently, approximately 10 of these, large "core" banks, will be required to adopt the Advanced Measurement Approach (AMA) for risk management under the Basel II regime. Further, under rules proposed in 2003 by the SEC's Consolidated Supervised Entities (CSE) regulations, five large US securities firms will also be required to abide by the Basel II regulations. Other securities firms are owned by banks and will thus be supervised by the Federal regulators requirement to adhere to the Basel II framework.[22] The SEC's rules establish regulatory guidelines for a Supervised Investment Bank Holding Company (SIBHC), which includes requirements to establish a group-wide internal risk management control system, record keeping, and periodic reporting system. This will specifically include reporting consolidated computations of allowable capital and risk allowances consistent with the standards published by the Basel Committee on Banking Supervision.[23]

---

[20] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices, Page 9179
[21] Ibid, Page 9180
[22] Securities & Exchange Commission, August 2004
[23] Ibid

It should be noted that since the early 1970's, the SEC has subjected broker/dealers to capital charges for such operational risks as aged failed to delivers, short securities differences, suspense account items (essentially securities transactions that cannot be completed for various reasons), and reconciliation differences (unfavorable bank account, correspondent account, clearing corporation and securities depository reconciliation differences).[24] Other categories of capital charges include aged corporate actions receivable and aged transfers not confirmed. The value of these deductions from net capital is significant. For example, the Banc of America Securities reported aged fails-to-deliver in the first quarter of 2005 of $177 million.[25] Further, participants of a clearing organization must allocate capital to support the guarantees and risk management practices of these industry-wide risk mitigating entities. For example DTCC and its clearing and settlement subsidiaries, NSCC, FICC and GSCC collectively held $10.6 billion of such participants' funds at year end 2004.[26]

Coincidentally, each of these 15 institutions individually spend the most on reference data, duplicating each others costs for no strategic advantage. Collectively they bear the largest risk of faulty data through their representation as traders, investment managers, prime brokers, paying agents, trustees, fiduciaries, and custodians in the majority of the trades conducted in the global capital/investment markets.[27] Initially, another group of approximately 15 US based financial institutions, along with U.S. based foreign owned financial institutions regulated under their parents' home country regulatory regimes, are expected to voluntarily adopt the Basel regime owing to the incentive for reducing overall capital requirements through risk mitigation.

Intriguingly, Federal regulators have reported that *"The industry has raised the possibility that some securities products may be developed to provide risk mitigation benefits"*.[28] This suggests to us that there will ultimately be an operational risk transfer market that will follow the same path as the capital market innovations surrounding risk transfers associated with market risk (interest rate swaps, equity options, futures, et al) and credit risk (credit default swaps). However, this is dependent on the devising a generally accepted operational risk measure that can be applied across all business lines and event types within each financial institution as well as across the industry.

Focusing on the potential for an operational risk mitigant other than insurance, the Federal regulators have stated "*In evaluating an operational risk mitigant other than insurance, [AGENCY] will consider whether the operational risk mitigant covers potential operational losses in a manner equivalent to holding regulatory capital."* [29] While not specifically making any reference to outsourcing, but certainly embracing it in

---

[24] Presentation by Michael A. Macchiaroli, Associate Director of the Division of Market Regulation, U.S. Securities and Exchange Commission at the Boston Federal Reserve's conference on Implementing an AMA for Operational Risk, May 20, 2005

[25] Banc of America Securities LLC, Focus Report, Form X-17A-5 for period 1/1/05 – 3/31/05

[26] DTCC, Annual Report, 2004

[27] Grody, A., Solving the Reference Data Problem in Financial Services – Are We on the Right Path?, Journal of Operational Risk, Dec., 2006, Vol. 1, No. 3, Fall, 2006 , Pages 63-69

[28] Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices, Page 9180

[29] Ibid, Page 9184

concept, this "risk mitigant other than insurance" can certainly be construed as an "outsourced" Clearing Corporation in the U.S. (Under the National Market Clearing and Settlement regulations governing capital and investment markets). A clearing corporation's risk mitigating and captive insurance structures should make it available for capital relief under the stated Basel II risk mitigant criteria.[30] Such an entity, the Global Joint Venture Matching Service, now known as Omgeo, was approved by the SEC as an exempt clearing corporation to mitigate post-trade risk in the matching and settlement of institutional securities.[31] A similar exemption could be obtained for an entity formed to match and "clear" a set of standardized reference data. If such an entity of outsourced repository of quality data is formed in collaboration with large financial institutions(say similar in governance to most other such industry-wide risk mitigating infrastructure entities) then it would be a useful vehicle to minimize operational risk for all who subscribe to this data, and available for distribution to all initial and subsequent downstream participants.

By any standard, the costs and operational risk consequences of faulty reference data are severe. Failed transactions and reporting processes are either manually reprocessed and/or reported into spreadsheets where they can be controlled, investigated, repaired and then reprocessed. Additional verifications and reconciliations are introduced to control the multiple data sources that have to be created in manual workarounds and spreadsheets outside their respective automated information processing systems. In this way these systems also lose their facility for straight-through-processing. SWIFT has estimated that these repairs cost the industry $12 billion annually.[32] Solving this long standing industry problem would be a just reward for the financial institutions who embrace this operational risk mitigation solution within the framework of Basel II.

---

[30] http://www.sec.gov/divisions/marketreg/mrclearing.shtml

[31] SEC, Global Joint Venture Matching Services - US, LLC; Order Granting Exemption from Registration as a Clearing Agency April 17, 2001 http://www.sec.gov/rules/sro/34-44188.htm

[32] SWIFT – Results of STP Reviews Reported on in 2002

The Authors

Allan D. Grody is the President of Financial InterGroup (agrody@stern.nyu.edu), a financial services advisory and development company. He was founding partner of Cooper's & Lybrand's (now PriceWaterhouseCoopers) Financial Services Consulting Practice and founding professor of NYU's Graduate Risk Management Systems course. He writes and speaks extensively on key issues affecting the financial services industry and is a member of the Editorial Board of the Journal of Risk Management in Financial Institutions

Robert M. Mark, Ph.D. is the CEO of Black Diamond (bobmark@blackdiamondrisk.com), which provides corporate governance, risk-management consulting, risk software tools and transaction services. He was a CRO and Corporate Treasurer at several large financial institutions He serves on several boards, is the Vice Chair of the Professional Risk Managers' International Association's (PRMIA) , the co author of two prominent books on risk management and is a member of the Editorial Board of the Journal of Risk Management in Financial Institutions