

Operational risk, data management, and economic capital

Allan D. Grody

President, Financial InterGroup

Peter J. Hughes

Managing Director, ARC Best Practices

Robert M. Mark

CEO, Black Diamond Risk

Abstract

Managing a business based on risk-adjusted performance measures (RAPM) is now a generally accepted management tool. The Basel II regulatory capital regime for financial institutions has provided an impetus to calculate both regulatory and economic capital for market and credit risks as well as for operational risk. However, as yet there is no generally accepted set of measures for capturing operational risk exposure and establishing a linkage between operational losses and their causes. A particular challenge has been to manage the value of an organization's data assets. The aim

of our paper is to describe methods that are currently being used to measure operational risk and to demonstrate the inadequacies of these approaches. We propose an illustrative methodology for creating a value-bearing measure of operational risk exposure. We also provide examples of measures to minimize the risk of faulty data and improve the value of data utilized to manage risk. We complete our paper with a discussion of ways to mitigate risk and summarize the risk measure inputs discussed in this paper for achieving RAPM objectives.

Operational risk, data management, and economic capital

Measuring operational risk has become a significant challenge for all financial enterprises. A key component of the measurement process is to work through the consequences of reinforced diligence among regulators for enforcing know-your-customer (KYC) rules, anti-money laundering laws, the Sarbanes-Oxley (SOX) legislation, the Markets in Financial Instruments Directive (MiFid), and the Undertakings for Collective Investments in Transferable Securities (UCITS) III directive in European Community countries, and globally, the Basel II Capital Accords, amongst others.

Operational risk is now formally included in both internal as well as external performance and reporting considerations. The concept of operational risk capital and its associated impact on risk-adjusted performance measures has elevated interest in the value of accurate data. Faulty data is both a significant component of operational risk and a significant cause of operational losses.

Accounting for operational risk exposure, and accommodating the operational risk component of risk capital, has proven a formidable challenge and has yet to be structured with anything approaching an accepted model or methodology or even a thoughtful enduring approach. At its most fundamental level, financial institutions have been evolving management information systems over decades. What stands in the way, however, is the lack of any measure of operational risk exposure, the failure to incorporate the importance of data into risk measurement models, and, finally, the lack of any cohesive mechanism to correlate operational risk exposure with historical operational losses.

Economic capital

Economic capital is based on a probabilistic assessment of potential future losses and is therefore a potentially more forward-looking measure of capital adequacy than traditional accounting measures¹. Conceptually, economic capital can be expressed as protection against unexpected future losses and is commonly referred to as the enterprise value-at-risk (VaR) at a specific confidence level over a particular

time horizon. Basel II has given financial institutions and their boards the impetus to further develop VaR models through the inclusion of advanced measurement approaches (AMA) for market and credit risks (financial risk) and operational risk (non-financial risk).

Economic capital is distinct from familiar accounting and regulatory capital measures, and different from new measures of capital adequacy as mandated under Basel II. Expressed as the dollar value of capital necessary to adequately support specific risks assumed, most traditional measures of capital adequacy relate existing capital levels to assets or some form of adjusted assets. Economic capital relates capital to risks, regardless of the existence of assets.

In reality, we want to ensure that each strategic business unit (SBU) incurs a transparent economic capital charge that will allow firms and individual SBUs to use risk/reward analysis to improve and effectively communicate their operational decisions. A significant challenge for practitioners and academic researchers is to provide the models which will enable a financial institution to calculate the economic operational risk capital saved due to such innovations as internal process improvements, information technology enhancements, impact of external payment and settlement time compression, etc.

Operational risks can be divided into those losses that are both expected and unexpected. There will be a normal amount of operational loss that business is willing to absorb as a cost of doing business, such as error corrections, frauds, and so on. These failures are explicitly or implicitly budgeted for in the annual business plan, and are covered by the pricing of the product or service. We assume that a business unit's management is already assessing and pricing expected failures into severe but not catastrophic losses. By contrast, the attention to operational risk assessment is typically focused on unexpected failures, and the amount of economic capital that should be attributed to business units to absorb these losses. Unexpected losses are actual (economic) losses that exceed expected losses and are a measure of the uncertainty inherent

Operational risk, data management, and economic capital

in the loss estimate. It is this possibility to incur unexpected losses that necessitates the holding of capital. However, unexpected failures can themselves be further subdivided.

As indicated in Figure 1, expected losses are the anticipated average loss over a defined period of time that represent a cost of doing business and are generally expected to be absorbed by operating income. Expected losses are priced into the products' costs and profit margins, as for example in the case of loan losses, where the expected loss is priced into the yield and an appropriate charge included in the reserves provisioned for loan losses. Provisions for credit card losses, payments and securities settlement losses, uncollectible commercial loans, trade counterparty defaults, etc. are estimated as the potential costs of doing business. Catastrophic losses are potential risks of losses that can be protected by either the capital of the enterprise, by insurance, by mutual risk-sharing as in reinsurance, and/or through risk mitigating infrastructure utilities, such as payment networks, settlement systems, and centralized counterparties.

Capital VaR is an estimate of the unexpected losses at a specific confidence interval over a given time frame. There are usually measures of VaR for each of the three enterprise risks – market, credit, and operational². Confidence interval is

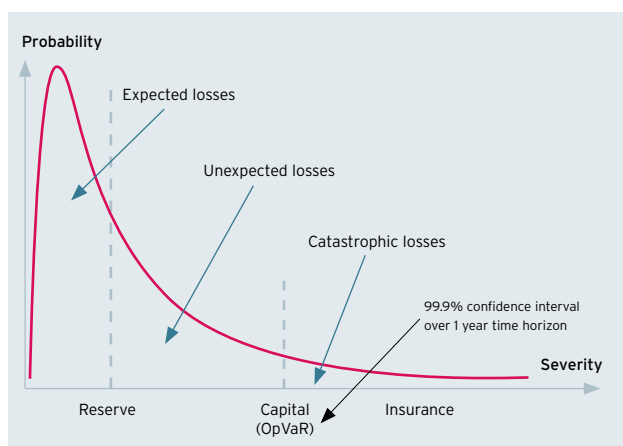


Figure 1 - Calculating economic capital

the level of risk, expressed as a confidence interval during a prescribed time period, at which the enterprise has chosen to operate. The higher the confidence level selected, the lower the probability of insolvency. For example, at a 99.97 percent confidence level the enterprise is accepting a 3 in 10,000 probability of insolvency over a one-year period. Many banks using economic capital models have selected a confidence level of between 99.96 and 99.98 percent, equivalent to the insolvency rate expected for a AA credit rating. Insurance is an expense item usually purchased for protecting both catastrophic and unexpected losses. The enterprise needs to make trade-offs between the uncertainty of capital insolvency and the costs of insurance. Insurance is usually built into the cost of the product with a commensurate effect on its profit margin. Economic capital is typically defined as the difference between some given percentile of a loss distribution and expected losses. It is the common currency for risk adjusted performance sometimes referred to as the unexpected loss measured at a specified confidence interval.

The RAPM model allows an organization to make objective judgments across business units including fee-based services, trading desks, credit and deposit businesses, and fiduciary units. A key decision is the amount of capital to allocate to each business line. In order to manage in this way the organization must be structured into the appropriate business units and within a hierarchy of accountability in the manner that management information systems require.

Implementing transfer pricing schemes, as well as cost accounting and attribution systems, are prerequisites to having a well-defined risk-adjusted performance management. Closely aligned with management's responsibility for performance are the incentive compensation schemes. This too must be in place if performance and incentives on a risk-adjusted basis are to make sense to the organization.

A robust RAPM solution depends on being able to properly accumulate historical data over time, starting with the massive accumulation of historical market prices and credit

² Under the Basel II regime, risk coverage for each type of risk is broadly defined as:

- Market risk - the risk that an enterprise's tradable assets or its interest rate differential (asset-liability gap) loses value due to market price fluctuations.

- Credit risk - the risk of the enterprise not receiving payment for deploying its assets
- Operational risk, the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. (Operational risk includes legal risk, but excludes business strategic and reputational risk).

Operational risk, data management, and economic capital

default histories along with adding the accumulated measures of operational risk. Furthermore, the connections between the identities of issuers of debt and equity, and their identities as counterparties in a trade, or as borrowers, is not done in any meaningful or consistent manner, making it difficult to associate. For example, it is quite difficult to link a potential defaulting obligor (whose market price of its public debt is declining, a market risk) with its subsidiary that has a loan outstanding whose probability of default is increasing (a credit risk). It is, thus, apparent that while market and credit risks are linked, the diversification benefits between these two financial risks are lost in the added operational risk of faulty data.

The discipline of operational risk

After a decade of intense industry-wide consultation and investment, the operational risk component of Basel II is falling well short of what its founding fathers envisaged when, in its first consultation paper in 1999, the Basel Committee challenged the industry to quantify the levels of operational risks and incorporate them into a firm's overall capital adequacy [BIS (1999)].

A fairly reliable indicator of where the industry is positioned relative to Basel II was the industry's response to the regulatory agencies' implementation plans. Such a process is currently underway in the U.S. with regards to the joint agencies' request for comment relative to their proposed Basel II supervisory guidance. Consider this recent comment from the Advanced Measurement Approach Group of the Risk Management Association, which was formed to represent the leading U.S. banks in this area: "Practically speaking, the requirement to produce comprehensive management reports including 'changes in factors signaling an increased risk of future losses' cannot be met at this point in time or in the near future. In many instances, operational risk factors that led to a particular event cannot be uniquely determined retrospectively, let alone detecting a change in factors that signals an increase in future losses"³.

This statement begs the question, what value does a global risk management, capital adequacy, or economic capital

regime have if the banks applying it, by their own admission, are unable 'at this point in time or in the near future' to fulfill a requirement as fundamental as being able to demonstrate the link between changes in risk factors and past and likely future negative outcomes? The answer is that, without this capability, risk management programs, and their risk-adjusted performance measures, have very little value. But it is not difficult to see why this set of circumstances exists. An essential ingredient for any risk management program, namely exposure, is missing. The industry has not yet found a way of identifying a financial institution's total portfolio of operational exposures in live operating environments and intends to put a consistent and comparable value on them. In the absence of such a direct exposure measurement methodology the industry has looked to loss history as being the only objective source of information on operational risks. Consequently, advanced measurement approaches under Basel II rely mainly on loss history to deduce the possible current portfolio of operational risk exposures through the application of actuarial modeling techniques.

It is clear by now that a risk management regime that operates on imperfect operational loss history can benefit from a bottom-up approach that measures operational risk exposure and is able to isolate its root causes. Operational risk exposures fluctuate on a daily basis, often dramatically, as a consequence of changes in transaction volumes, implementations of new technology, failures of existing technology, business reorganizations, staff absences, new products, etc. There are also hidden exposures related to, for example, fraud and control breakdowns. And if loss events do occur, technology and operations personnel invariably diagnose the causes and fix them. The conclusion is that historical loss experience is a useful tool to help focus on current exposure but without the ability to measure it we can not be proactive in risk management nor in risk mitigation.

The proposed U.S. implementation of final regulatory guidelines for Basel II related to operational risk calls for a "consistent and comprehensive capture and assessment of data

³ Federal Reserve, 2007, "Response by the Advanced Measurement Approach Group of the Risk Management Association to the 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," May 24 page 8

Operational risk, data management, and economic capital

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)"⁴.

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"⁵.

Unfortunately, we have not yet achieved a meaningful calibration of operational risk capital nor have we engaged in a 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(s). 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 risk exposure to their frequency and severity measures of operational losses. 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.

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 and credit risks,

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 exposure 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 as yet on the right path to accurately measure operational risk? Well, we simply abrogated the difficult task of measurement to the easier path of a subjective assessment. We have also misunderstood the significance of a pillar of operational processes, data management, and its significant role in operational risk. And finally, we bypassed a crucial step, the bridging of operational performance to the metrics of risk measurement.

The major sources of operational risk

The majority of operational losses are due to transaction processing errors, that is at the highest level, the failure of people, systems, and the data they act upon to operate seamlessly [sometimes referred to as straight-through-processing (STP)]. These losses result from human error, failure to follow existing procedures, or from inadequacies within the procedure when first established, such as wrong codes or identifiers. These losses are also normally considered unintentional and correctable with proper business planning and controls. The next largest source of operational losses is due to employee violations of internal policies for intentional purposes (fraud). Remaining operational losses result from external forces, and systems or technology disruptions⁶.

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 that implicitly contains the

4 Federal Register, 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," 72:39, page 9170, Wednesday, February 28

5 Ibid, page 9173, footnote 13

6 Harmantzis, F. C., 2003, "Risky business," Institute for Operations Research and the Management Sciences, Lionheart Publishing, Inc., Feb

Operational risk, data management, and economic capital

Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	
Transaction capture, execution, and maintenance	Miscommunication Data entry, maintenance, or loading error Missed deadline or responsibility Model/system misoperation Accounting error/entity attribution error Other task misperformance Delivery failure Collateral management failure Reference data maintenance
Monitoring and reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
Customer intake and documentation	Client permissions/disclaimers missing Legal documents missing/incomplete
Customer/client account management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
Trade counterparties	Non-client counterparty misperformance Misc. non-client counterparty disputes
Vendors and suppliers	Outsourcing Vendor disputes

Figure 2 - Basel II event type: execution, delivery, and process management

consequences of faulty data (see Figure 2 for the definition and examples of what constitutes this loss event category)⁷. This category accounted for approximately 42% of total operational loss events, with a total loss value of €908,000 (34.8% of the total).

Another event type 'clients, products, and business practices,' represented 27.5% of overall losses, a category (Figure 3) that also contains faulty data categories such as model errors, exceeding client exposure limits, and suitability/disclosure issues (KYC, money laundering). Unfortunately in the instructions to those who were asked to participate in the sampling, this loss event category was described as the end tail of a flow chart that 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 and process management.' In hindsight this is obviously not a satisfying way to categorize what turns out to be the largest loss event category.

In a follow-up survey of 27 U.S. 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 losses⁸. The loss for the event type 'clients, products, and business practices,' (U.S.\$5,820.5 million) represented 67% of this new 'other' business line category and 80.8% of overall losses. Like 'execution, delivery, and process management' (in this study it comprised 9.9% of overall loss value), if those filling out the data sheet made it to this end point and had not yet categorized losses in any other category it would be categorized in this event type.

This data collection exercise was, unfortunately, also flawed, for a number of reasons. Firstly, while all respondents submitted data for the retail banking business line, only half submitted data for corporate finance. Secondly, respondents reported losses at a mix of different threshold levels, from U.S.\$0 and above to U.S.\$10,000 and above. Finally, in aggregating the data, the 'other' business line, representing the largest total loss amount (U.S.\$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 that 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 exercises a more granular look at the accumulation of loss data related to faulty data is warranted, perhaps to be accounted for in a similar manner as one aggregates retail credit loss or check fraud data.

Looking within the general structure of Basel's broad categorizations (Figure 4) it would appear that the 'payment and settlement' business line, now categorized under banking and, thus, suggesting monetary settlements exclusively,

7 QIS2 - Basel Committee on Banking Supervision, 2002, "The quantitative impact study for operational risk: overview of individual loss data and lessons learned," January

8 U.S. Federal Reserve, 2005, "The quantitative impact study 4 (QIS4) and the loss event collection exercise," May

Operational risk, data management, and economic capital

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	
Suitability, disclosure, and fiduciary	Fiduciary breaches/guideline violations Suitability/disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender liability
Improper business or market practices	Antitrust Improper trade/market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
Product flaws	Product defects (unauthorized, etc.) Model errors
Selection, sponsorship and exposure	Failure to investigate client per guidelines Exceeding client exposure limits
Advisory activities	Disputes over performance of advisory activities

Figure 3 - Basel II event type: clients, products, and business practices

should be reviewed with a view to it being included as a loss event type as well, under the asset management, trading and sales and/or corporate finance business lines, to assure that the loss data collection exercise captures physical asset or contract settlements in addition to such money settlements as foreign exchange, fed wire, swift/chips payments, and credit/debit cards. Physical asset and contract settlements include futures, equities, derivatives, sovereign debt, corporate, municipal and provisional debt, etc, where there is not only a cash payment and settlement, but additionally the 'clearance and settlement' of the non-cash portion.

Other sources of operational risk loss data are the databases of SAS Institute's OpRisk Global Service, Fitch's Algo OpData database, and the more recent Operational Risk Data eXchange Association (ORX) database. SAS carries loss data on events exceeding U.S.\$100,000 and Fitch's Algo OpData has data on events exceeding U.S.\$1 million, and both have classified their datasets by Basel business line and event type. A large percentage of their losses (nearly 40%) are in the

retail banking line of business. Each has data culled from the trade press, news reports, press releases, the SEC, and other regulatory and public sources. In contrast, ORX, a consortium of financial institutions, populates its database directly from inputs of its contributing members and at a loss threshold of €20,000. The ORX consortium was founded in 2002 by 12 member banks and has since grown its membership to 36 banks in 13 countries. Each loss is characterized according to the following primary attributes: reference ID number and related event Ref ID (member generated), business line, event category, country, date of occurrence, date of discovery, date of recognition, credit-related, gross loss amount, and direct and indirect recovery amount. ORX also requires the submission of gross income per business line and is working on developing categorizations for product and process. They are also considering plans to expand the scaling of data to include expenses and assets. Most interestingly they are also considering producing a categorization for cause.

Measuring operational risk

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 underlying cause⁹. For example, people risk would include cases where people 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 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. In 2003, in a consultative paper, it reversed itself and redefined the management of operational risk to mean the assessment of risk not its measurement¹⁰.

9 Crouhy, M., D. Galai, and R. Mark., 2005, Essentials of risk management, McGraw Hill

Operational risk, data management, and economic capital

Corporate finance	Municipal/government finance	Mergers and acquisitions, underwriting, privatizations, securitization, research, debt (government, high yield), equity, syndications, IPO, secondary private placements
	Merchant banking	
	Corporate finance	
	Advisory services	
Trading and sales	Sales	Fixed income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage
	Market making	
	Proprietary positions	
	Treasury	
Retail banking	Retail banking	Retail lending and deposits, banking services, trust and estates
	Private banking	Private lending and deposits, banking services, trust and estates, investment advice
	Card services	Merchant/commercial/corporate cards, private labels and retail
Commercial banking	Commercial banking	Project finance, real estate, export finance, trade finance, factoring, leasing, lending, guarantees, bills of exchange
Payment and settlement	External clients	Payments and collections, funds transfer, clearing and settlement
Agency services	Custody	Escrow, depository receipts, securities lending (customers) corporate actions
	Corporate agency	Issuer and paying agents
	Corporate trust	
Asset management	Discretionary fund management	Pooled, segregated, retail, institutional, closed, open, private equity
	Non-discretionary fund management	Pooled, segregated, retail, institutional, closed, open
Retail brokerage	Retail brokerage	Execution and full service

Figure 4 - Basel II mapping of business lines

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 can be highly predictive of the actual losses. In the absence of a consistent and comparable risk measurement method, risk managers do 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 monitored¹¹. Reliance is placed almost exclusively on qualitative performance management mechanisms, such as risk and control self assessments (RCSA), key performance indicators (KPI), key risk indicators (KRI), and other control and business process management methods¹².

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.

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 do not 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

10 Basel Committee on Banking Supervision, 2003, "Sound practices for the management and supervision of operational risk," February

11 The Financial Services Roundtable, BITS, 2005, "Reconciliation of regulatory overlap for the management and supervision of operational risk in U.S. financial institutions: improving compliance efficiencies by minimizing redundancy,"

Operational Risk Management Working Group, May 20, Page 18

12 Wahler, B., 2005, "Process managing operational risk. Developing a concept for adapting process management to the needs of operational risk in the Basel II-framework," working paper, Johns Hopkins University

Operational risk, data management, and economic capital

Basel II's suggested framework. For example, the regulators allow for and define scenario analysis¹³ 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, increasing 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.

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 transac-

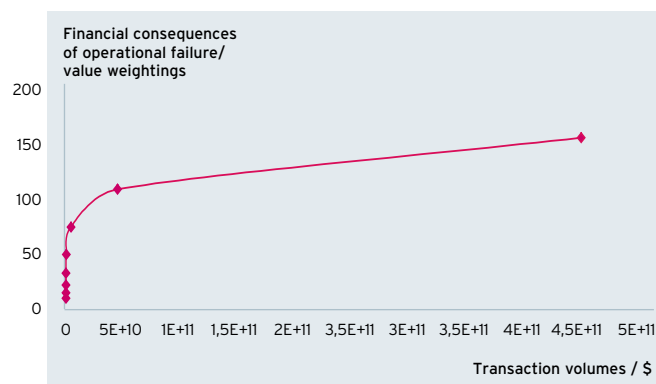


Figure 5 - Scaling operational risk measurement
Operational value curve: first 8 bands

tion 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 volume¹⁴. This concept is reflected in the graph displayed in Figure 5 and discussed in a paper published by the Federal Reserve Bank¹⁵.

The graph in Figure 5 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 in 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.

These value bands that are assigned to the curve shown in Figure 6 are designed to demonstrate the linkage between the financial consequences of operational failure (converted

¹³ Board of Governors of the Federal Reserve System, 2006, "Basel II Capital Accord, notice of proposed rulemaking (NPR) and supporting board documents," Board memorandum, March 22

¹⁴ ARC technical paper, April, 2007 <http://www.ARC1.co.uk>

¹⁵ de Fontnouvelle, P., V. DeJesus-Rueff, J. Jordan, and E. Rosengren, 2003, "Capital and risk: new evidence on implications of large operational losses," Federal Reserve Bank of Boston, September

Operational risk, data management, and economic capital

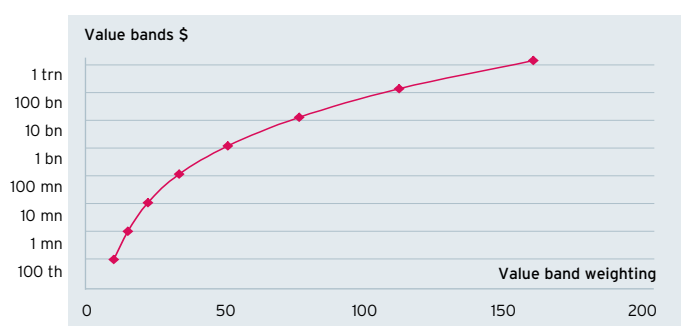


Figure 6 - Value bands

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.

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 allocating a standardized risk weighting to each allows for a direct correlation with operational risk measurements, tying operational risk to the financial and operating performance of the bank.

Operational exposures can be expressed in each organizational unit in terms of potential transactional failure through the faulty interaction of people, process, data, and systems. The intersection of these interactions will result in a set of values derived from benchmarked scoring templates associated with risk factors (KRIs), which, in turn, can be mapped to the value bands described previously. The resulting 'risk units' calibrated from associating risk factors with process volumes and value bands can then be benchmarked with other processes, and with other organizational units similarly calibrated. Thereafter, other 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, identified with causes in loss databases, will become a predictive measure of loss events and hence a mechanism for the actions needed to first manage and then mitigate operational risk.

Data management at the core of operational processes

Determination of the 'risk units' that are the consequence of transactional failure and faulty reference data requires a method of directly measuring exposures to operational risks in live operating environments. One such method described in this paper is currently being benchmarked, calibrated, and piloted at major international financial institutions¹⁶. The approach involves: defining the core component of exposure (an operational process, a business critical reference data element, a mission critical software application, etc.); agreeing a common measurement framework to value each exposure; risk-weighting the exposures via benchmarked, best-of-breed qualitative scoring templates; using statistical techniques to correlate the exposure measurements with actual loss experience; and continually adjusting the exposure measurement methodology and fine-tuning the risk model to enhance its predictive sensitivity and accuracy¹⁷. Such techniques have been explored in another section of this paper for another risk category, credit risk, which, we remind the reader, we can now see why it can serve as a metaphor for the just described process of measuring operational risk.

Transactional and, more specifically, reference data are broad terms understood by operating management, information technology professionals, and risk managers alike. Unfortunately each group understands it differently. To the information professional reference data is "any kind of data used solely to categorize other data found in a data base or solely for relating data in a data base to information beyond the boundaries of an enterprise."¹⁸ To the risk manager it is "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"¹⁹. To operating management reference data is information that

16 Thoresen, T., 2007, "The marvel of metrics," Inside Reference Data, 2:8

17 Hughes, P., 2007, "Operational risk: the direct measurement of exposure and risk in bank operations," Journal of Risk Management in Financial Institutions, 1:1

18 Chisholm, M., 2000, "Managing reference data in enterprise databases: binding corporate data to the wider world," The Morgan Kaufmann Series in Data Management Systems, Aug, 3

19 Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices, Page 9100

Operational risk, data management, and economic capital

enables financial transactions to be identified and processed and financial information to be internally and externally reported. It is no wonder that risk management, operating management, and information technology professionals are not focused on observing, let alone resolving, one of the most significant operational risks, that of faulty, operationally defined, reference data.

For example, reference data represents the data elements comprising: financial products and their changing specifications, such as 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 that should be identical in each organization is not. It is sourced independently by each financial organization, is costly to acquire and maintain, is duplicative across the industry, and comprises 70% of the data content of financial transactions²⁰. A reference data repository contains business

critical and non-critical data elements. Critical data elements, if faulty, have the potential to cause negative outcomes in the form of losses, sanctions, or penalties due to transaction or trade failures and incomplete or inaccurate reporting processes.

The size of the exposure to such potential negative outcomes, the 'exposure to risk,' is measured in risk units and is the risk-weighted size of data elements based on their business criticality (criticality weighting) and usage in bank operations (value band weighting) adjusted by a data quality index (DQI), which is a measure of the effectiveness of risk mitigation in data maintenance processes. The DQI is on a scale between zero (wholly ineffective or nonexistent risk mitigation) and 100 (best practice risk mitigation), and is calculated as a result of mapping the current state of risk mitigation to scoring templates containing a complete range of best practice benchmark data and criteria.

While faulty data has been a persistent impediment to systemic risk mitigation across the global capital and investment markets²¹, its consequences are not yet fully appreciated in fulfilling the new requirements of identifying causal factors in operational loss events. Risk managers should now be focusing on the importance of data as they ponder the underlying dynamics of operational loss events.

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

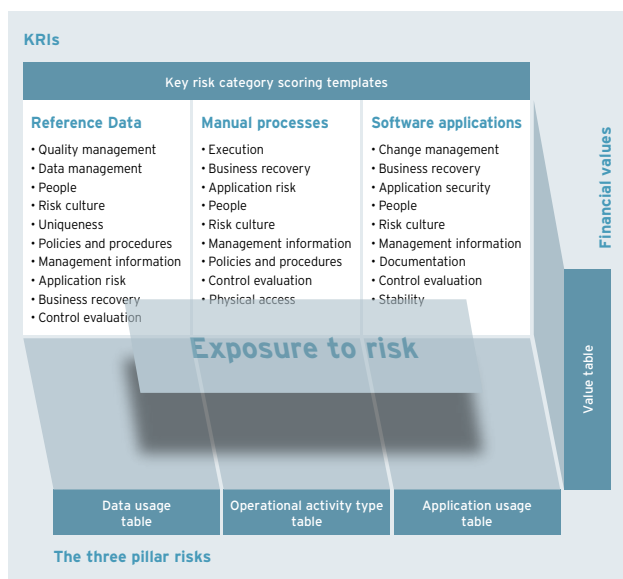


Figure 7 - Calculation of exposure to risk in risk units

20 Grody, A. D., F. Harmantzis, and J. G. Kaple, 2006, "Operational risk and reference data: exploring costs, capital requirements and risk mitigation," Journal of Operational Risk, 1:3

21 Group of Thirty, 2006, "Global clearance and settlement," Final monitoring report, May

Operational risk, data management, and economic capital

which contains causal relationships that drive these operational loss events.

Here we observe a normalized measure of operational risk exposure (the risk unit) and tie it to both the operating processes and to the financials of a financial institution. Secondly, we aggregate the operational metrics associated with operational processes around three key pillars of KRIs and KPIs, those associated with manual process and business software applications, and the interaction of these two with transactional and reference data (Figure 7). The broad range of outcomes, STP (as the benchmark) = 0 risk, and the level of failure of those interactions measured in risk units, gives us the ability to rank order the outcomes in management dashboards (see Figure 8), and assess relative risk through both a set of quality indices and benchmarks.

Thereafter, the risk measures are correlated with loss history, as was demonstrated over time in the development of credit risk measures, and the usual measures of operational

	Control evaluation	People	Execution	Business recovery	Risk culture/ management	Management oversight	Application security	Physical access	Policies and procedures	Ops quality index	Risk	Exposure
Category weightings	10	10	10	8	6	6	4	4	2		Risk units (Thousands)	
Department A												
Process 1	25	50	45	15	50	75	75	100	50	47.8	86	165
Process 2	80	100	50	0	30	50	40	100	20	56.3	48	110
Process 3	25	50	45	15	50	75	75	100	50	47.8	57	110
Process 4	0	30	25	5	40	10	70	100	0	26.2	111	150
Dept. OQI	29.3	54.7	40.4	9.1	43.1	51.6	66.4	100.0	29.8	43.5	302	535
Department B												
Process 1	70	70	50	100	100	100	70	100	100	79.7	18	90
Process 2	70	70	50	100	100	100	70	100	100	79.7	20	100
Process 3	70	60	85	80	60	85	75	100	80	75.3	54	220
Dept. OQI	70.0	64.6	68.8	89.3	78.5	92.0	72.7	100.0	89.3	77.3	93	410
Division OQI	47.0	59.0	52.7	43.9	58.5	69.1	69.1	100.0	55.6	58.2	395	945

Figure 8 - A sample scorecard of operational quality indexes (OQI) and risk values

risk VaR are calculated from the historical accumulation of loss frequency and severity. Finally, this allows us to complete our thinking about the calculation of economic capital in the context of being able to include operational risk as the third component (along with market and credit risk) of risk-adjusted returns, as previously discussed.

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 financial institutions will be allowed to reduce their capital allocations for operational risk by as much as 20% through the use of risk mitigates, such as insurance²². Currently, the primary risk mitigates used for operational risk is insurance²³. 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 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 and delays, and counterparty risks, which are inherent in using insurance coverage.

Of particular interest in risk mitigation offsets is found in the 30 largest, internationally active financial enterprises headquartered in the U.S. Currently, approximately 10 of these, large core banks, will be required to adopt the AMA for risk management under the Basel II regime. Furthermore, under

Operational risk, data management, and economic capital

rules proposed in 2003 by the SEC's Consolidated Supervised Entities (CSE) regulations, five large U.S. 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 framework²⁴. 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 Supervision²⁵.

It should be noted that since the early 1970s, 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)²⁶. 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 U.S.\$177 million²⁷. Furthermore, 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 U.S.\$10.6 billion of such participants' funds at year end 2004²⁸.

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 markets²⁹. Initially, another group of approximately 15 U.S.-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"³⁰. 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 (interest rate swaps, equity options, futures, etc.) and credit risks (credit default swaps). However, this is dependent on the devising of 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 mitigates other than insurance, the Federal regulators have stated that they will consider whether they cover potential operational losses in a manner equivalent to holding regulatory capital³¹. While not specifically making any reference to outsourcing, but certainly embracing it in concept, this "risk mitigates 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 mitigates criteria³². 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 securities³³.

24 Securities and Exchange Commission, August 2004

25 Ibid

26 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

27 Banc of America Securities LLC, Focus report, Form X-17A-5 for period 1/1/05 - 3/31/05

28 DTCC, Annual Report, 2004

29 Grody, A., 2006, "Solving the reference data problem in financial services - are we on the right path?" *Journal of Operational Risk*, 1:3, 63-69

30 Federal Register/Vol. 72, No. 39/Wednesday, February 28, 2007/Notices, page 9180

31 Ibid, page 9184

32 <http://www.sec.gov/divisions/marketreg/mrclearing.shtml>

33 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>

Operational risk, data management, and economic capital

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 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 U.S.\$12 billion annually³⁴. 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.

Closing comments

The creation of a superior integrated risk framework extends beyond satisfying regulatory requirements (i.e., Basel II). It requires an ongoing commitment from the corporate and business functions to not only build such a framework but to sustain it through a corporate culture which embraces best practice risk management. Today, significant energy is being expended on the capturing and modeling of loss history for market, credit, and operational risk, with the latter still least developed or understood. This paper has attempted to propose a framework for developing such operational risk measures, placing it in an operational risk framework that values the operational process of people and systems interacting with data as the core of operational risk expo-

sure and operational losses. Therefore, we have argued that before enterprise-wide risk management (ERM) can proceed, enterprise data management (EDM) must be understood and mastered. With such an understanding, as suggested in the measurement approaches proposed in this paper, we can fulfill the vision of managing financial institutions within RAPM. Thus, this last uncharted field of risk, first measuring risk exposure and then relating operational risk directly to economic risk capital to cover unexpected losses, will be conquered.

With all of the above in place the final goal, that of risk mitigation, is in sight. Here the causes of risk, as described through the aggregation of the market, credit, and operational risk measures, linked to the loss history database and valued under RAPM, will highlight areas of unnecessarily high risk exposure. Finally, whether through mitigating credit risk through lowering credit limits, offsetting market risk through deploying hedging instruments, eliminating trading counterparty risk through organizing central counterparties, lowering systemic risk through moving to T+1 settlement, or eliminating process risk through either more effective automation, improving data quality, and/or reengineering work processes, the risk profile of each financial institution can be lowered to the benefit of all.

Finally, recognize that through collaboration, mutualized risk mitigation undertakings can benefit the entire global financial industry³⁵. Here, the regulators hope to unleash the creative power of each financial institution, and the financial industry at large, to create the risk culture both internally (the RAPM goal) and externally. Externally, a risk management culture is necessary to safeguard these interconnected enterprises as their transactions electronically traverse a global communication grid at the core of the world's economic activity. In that grid, the goal is to complete transactions seamlessly and in real-time. This requires that each company identify its reference data identically, a lofty goal yet unaccomplished and, as we demonstrated in this paper, at the root of much operational risk throughout the global financial industry³⁶.

34 SWIFT - Results of STP Reviews Reported on in 2002

35 Butterfield, W., 2007, "Collaborating on reference data: is now the time?" Tower Group, Oct

36 Group of Thirty, 2006, "Global clearing and settlement committee final monitoring report," May