Risk Accounting: A Next Generation Risk Management System for Financial Institutions

Allan D. Grody
Peter J. Hughes
Steven Toms

2011 Enterprise Risk Management Symposium
Society of Actuaries
March 14-16, 2011

Abstract

The financial crisis has awoken financial service organizations to the reality that when financial transactions enter their operating environments, they trigger real-time risk exposures that can go well beyond nominal transaction values, capital charges and other measures deemed appropriate for preventing unexpected losses. Traditional risk accounting approaches have caused lagging measures of risk to be recorded in much of managements' traditional performance and risk-reporting systems. Conventional financial and risk management systems are failing management and their boards due to their inability to measure, aggregate and report risk exposures as they accumulate. In reaction to the current financial crisis, the boards of many firms are assigning the additional task of oversight of management's risk policies and guidelines to audit committees. Accountants are also being asked to discuss the enterprise's key risk exposures with management, including those beyond financial reporting-related risks.

The aim of this paper is to consider whether a more comprehensive and timely measurement framework for risk exposure is now needed and to examine one possible approach. The paper introduces a common unit of exposure measurement for a diverse set of business risks and demonstrates how nominal transaction values and relevant quantitative and qualitative risk metrics can be mapped to each transaction and used to calculate a risk adjusted transaction value. The combination of conventional risk measures derived from the capital conventions mandated by the Basel Committee on Banking Supervision and this proposed risk exposure measurement framework provides the basis for the system of risk accounting described in this paper.

Keywords: Risk accounting, Basel, risk management, operational risk, enterprise risk.

Background

Regulators have always fostered an expectation that capital is what sustains banks in periods of stress and prevents them from failing. However, given the recent failures, bailouts and nationalizations of some of the world's leading financial institutions, we should perhaps view regulatory capital as the measure by which banks countdown to failure rather than the system that proactively prevents it.

So what offers a bank the greatest protection against failure if it isn't capital? Quite simply, it is the risk culture embedded in its people and processes. And at the core of any risk culture are 1) the incentives for individual compensation that balance risk and return with short-term self interest and long-term stakeholder goals, and 2) the early warning systems that highlight growing exposures to risk. Here, Basel regulations for operational risk were designated for such things as model risk, fraud, control weaknesses, faulty product structures, process and control risk, inappropriate sales to counterparties, and business practices that lead to faulty incentive compensation schemes. The risks inherent in the myriad of such business-level details went undetected, primarily because its implementation was left to last. Most firms had not implemented meaningful early warning systems for operational risk exposures. Indeed, it was actually pushed back by the industry's leading risk managers with complacency demonstrated by their managements and regulators.

Stakeholders in the financial services industry have a right to expect that the new profession of risk management and the risk managers who practice it would, by their rapid elevation to the executive-level "C suite" in most financial firms, facilitate a risk culture in these enterprises. Thereafter, they would ensure that early warning systems are installed to highlight growing exposures to risk with the final purpose of presenting reliable and meaningful assessments of future losses. But this is what risk managers and conventional risk management systems have evidently not succeeded in doing.

The current financial crisis can be linked to an inability to record and account for risk exposures in a timely manner. Indeed, recent failures of financial institutions provide some measure of the degree to which accumulating risk exposures escaped the exercising of business judgment simply because executive management, investors, auditors and regulators were unaware of their existence on such a scale. The result is risk management systems and, consequently, financial statements that failed to report the life-threatening concentrations of risk exposures that had unknowingly accumulated in so many of our leading financial organizations around the globe.

In recent testimony before the U.S. Congress, Alan Greenspan, former chairman of the Federal Reserve, acknowledged he incorrectly assumed managers of financial firms were aligning their risk appetite to their shareholders' interests. What he did not say, but implied, was that executives had aligned their appetite for risk to their own individual interests and that self-imposed risk and accountability controls failed regulators.

Risk management experts have long been aware of the difficulties attached to the measurement and management of operational risks, particularly where this relates to the translation of operational metrics. All the evolving risk measurement systems and generally accepted accounting conventions have been devoid of the ability to accommodate operational metrics into the risk reporting and aggregation methods used to oversee business performance. These have been presented of late as useful management tools in balanced scorecards, dashboards, six sigma measurements and the like. Such operating metrics have always been open to interpretation by management against the results of the performance and reporting systems of their institutions as they did not have a naturally occurring monetary basis from which they could be extrapolated or transformed into risk valuation measurements of any kind.

This problem was to be confronted at the time operational risk was offered as the third leg of the Basel capital regime, following credit risk and market risk, which described a framework in which discovery of new techniques for measuring such risk would be incented with lower capital charges. However, whether for lack of will, inability to communicate across business silos, or preoccupation with the earlier Basel pronouncements of externally focused market and credit risk, the industry pushed back without really trying. For example, when considering the application of the use test applied to operational risk, one such expert group commented: "[Operational risk] however is very different. The nature of [operational risk] is such that the direct linkage of measurement to management is difficult. This is partly due to the inherent difficulties in assessing the [operational risk] positions that a firm faces and how to measure these, but also because the risk profile of a firm does not change quickly, nor can changes to this profile be identified over a short time frame." [1]

Risk management experts were publicly airing their misgivings before the financial crisis broke. Such an example is the remarks presented in May 2007 by the Advanced Measurement Approach Group formed by leading U.S. banks under the auspices of the Risk Management Association (RMA). In response to the U.S. Joint Regulatory Agencies' proposals for the supervision of operational risk under Basel II, this group was dismissive of banks' ability to discern direct relationships between a change in risk and future losses. In fact, they even dismissed the ability to meet Basel's requirements to produce management reports to signal risk of future losses as not being capable of being met at this point in time or in the near future. They pointed out that, "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." [2]

1. Operational Risk Corporate Governance Expert Group, "The 'Use Test.'" (July 4, 2005): accessed April 9, 2009, http://www.fsa.gov.uk/pubs/international/orsg_use_test.pdf.
2. 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," p. 8 accessed July 18, 2011 at http://www.federalreserve.gov/SECRS/2007/August/20070809/OP-1277/OP-1277_2_1.pdf

Later, this same group, commenting on the same issue, but doing so when the financial crisis was well under way, concluded they struggle with the concept of a unit of measure at the operating level with sufficient granularity to be meaningful to the operational capital calculations, specifically in allowing for the determination of dependencies.[3] They also commented on the common method of performing a risk and control self assessment (RCSA), which, while admittedly having limited use in capital estimation, is also inadequate to the task of affecting management's ability to assess operational risk. They concluded RCSAs should be reinforced in this effort over its use in capital estimation.[4]

Regulators expected that the provisioning of capital for extreme losses would sustain financial enterprises in periods of stress. Did they truly believe these capital rules would prevent financial institutions from failing? To be fair, they did expect to see the coincident evolution of a risk culture within these institutions along with the development of a risk exposure measurement system to capture key operating metrics that could affect its operational risk profile. Taken together, and with regulatory oversight, it was anticipated that the new risk regime would do just that—prevent failures, or at least give an early warning of pending doom.

However, whether by abdication or by push back from the industry, or simply because there was not sufficient time to evolve in a natural way, we stopped the risk management process at capital provisioning. And we certainly failed in risk oversight.

This paper proposes a new approach to risk measurement that, along with capital measurement and more rigorous oversight, will allow banks an ability to manage risk.

3. Risk Management Association, "Unit of Measure and Dependence." (industry position paper, Advanced Measurement Approaches Group, December 2008).
4. Risk Management Association, "Business Environment and Internal Control Factors (BEICFs)." (industry position paper, Advanced Measurement Approaches Group, December 2008).

Failing to Manage Risk

The current financial crisis and recent failures of financial institutions are all examples of exceptional and unmeasured accumulations of risk exposures that escaped the purview of management, investors, auditors and regulators who were unaware of their existence on such a scale. The result was a failure to accommodate appropriate unexpected loss scenarios into their risk calculations, whereby model and liquidity risk are the most prominent of these failures. Further, many of the more recent events are all examples of risks that can be slotted into one or more of the business-level operational risk categories noted in the still unimplemented Basel operational risk framework.[5]

The largest failures of all were caused by model failures, which then cascaded into liquidity failures. In general, the models' creators failed to update them based upon marketplace changes created by the very same products that were enabled by these models. Examples abound; Bear Stearns' collapse was initially caused by holding a mortgage portfolio of subprime debt, improperly rated as relatively risk free when the parameters of the model were no longer valid. The inputs to the models had moved away from the early benchmarks and using past data from an earlier era when subprime debt was not prevalent and mortgage lending criteria were much more stringent.

Countrywide, American Century, Wachovia, Merrill Lynch, Citibank and Bank of America indulged in the miracle of risk modeling of an ever-increasing eroding assemblage of no income, no job or assets (NINJA) mortgages into off balance sheet repackaging vehicles. These investment trusts became the preferred mechanism to escape Basel capital requirements by risk-tranching the cash flows of individual mortgages, and later of other forms of assets. These later-stage securitized products used cash flows from credit card receivables, car loans, whole loans and debt that had previously been brought into existence as a result of securitized and tranched assets. These products evolved into risk adjusted return instruments with names like collaterized loan obligation (CLO), collaterized debt obligation (CDO) and CDO squared.

Indeed, the unmeasured and unreported risk exposures that contributed to the current financial crisis were a cocktail of all the principal categories of risk: credit, market, liquidity and operational. This serves to heighten the awareness of financial institutions and their regulators to the need for the measurement and management of risk exposures in the aggregate rather than on a specific risk category or silo basis as described in an April 2008 paper issued by the Basel Committee on Banking Supervision.[6]

5. J.D. Cummins, C. Lewis, and R. Wei, "The Market Value Impact of Operational Risk Events for U.S. Banks and Insurers," *Journal of Banking & Finance* 30, no. 10 (2006): 2605-34.
6. Basel Committee on Banking Supervision, "Cross-Sectoral Review of Group-wide Identification and Management of Risk Concentrations." (2008).

There is no shortage of evidence that firms recognize these threats and in response have elevated the monitoring of cross-enterprise risk exposures to the board level. For example, the Journal of Accountancy recently reported the results of an Ernst & Young survey[7] that found the boards of many firms are assigning the additional task of risk oversight, despite their already lengthy list of responsibilities, to audit committees. But not only are they being charged with overseeing management's risk policies and guidelines, they are also being asked to discuss the enterprise's key risk exposures with management, including those beyond financial reporting-related risks. In a 2006 survey of Fortune 100 companies[8] conducted by the Conference Board Governance Center and Directors' Institute, McKinsey and KPMG's Audit Committee Institute, it was found that 71 percent place responsibility to report on risk to the board with the chief financial officer. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) "Enterprise Risk Management — Integrated Framework"[9] provides a broader perspective in that it expects the entirety of enterprise risk management to be monitored through ongoing management activities, separate evaluations or both.

Irrespective of how risk monitoring accountabilities are assigned, if they are not underpinned by a consistent and replicable cross-enterprise risk exposure measurement framework that provides for the consolidation and aggregation of risk exposures, the task borders on the futile. Robert Rubin, a Citigroup director and former Treasury secretary, recently told the Wall Street Journal, "The board can't run the risk book of a company. ... The board as a whole is not going to have a granular knowledge of operations."[10]

7. Ernst & Young, "Global Internal Audit Survey." (2008).
8. C. K. Brancato, M. Tonello, and E. Hexter, "The Role of the U.S. Corporate Board of Directors in Enterprise Risk Management." *The Conference Board* (2006).
9. Committee of Sponsoring Organizations of the Treadway Commission (COSO), "Enterprise Risk Management – An Integrated Framework." (2004).
10. Wall Street Journal, "Rubin, Under Fire, Defends His Role at Citi." (November 29, 2008).

Basel II and the Regulatory Agenda

Recently, the Basel Committee on Banking Supervision (BCBS) has progressively extended requirements for quantifying and reporting financial risk.[11] It hopes to improve risk management by establishing operational risk as a separate category and publishing guidance for operational risk management. Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events.[12]

Research to date has considered the importance of operational risk in the financial marketplace, concluding that exposure is significant.[13] Within banking organizations, corporate-level risk has been allocated on a top-down basis. A survey by the BCBS found that, on average, banks had allocated approximately 15 percent of their capital for operational risk on this basis, adjusting for scale factors.[14] An important aspect of operational risk is fraud potential and significant losses have resulted from well publicized incidents.

More recently, the subprime mortgage failures and the unprecedented leverage that had been allowed to accumulate in the financial system have triggered bankruptcies, bailouts and nationalizations of financial institutions on an unprecedented scale. As prominent as the model failures were, the liquidity failures that resulted were even more significant, triggering cascading waves of collateral liquidations to meet margin and collateral calls impacting the correlation of previously uncorrelated assets. Coupled with the lack of credibility of the value of balance sheet assets that were previously being marked to market and now to suspect models, the flight to quality and known risks led to the abandonment of firms now suspected of having failing balance sheets due to marked down assets, newly described as "toxic" assets.

In response to BCBS-inspired regulatory changes and these high profile cases of fraud and failure, a large body of academic literature has accumulated on the various aspects of operational risk modeling.[15] Specifically, a number of studies have examined the problems related to the quantification of operational risk and associated events and processes, for example legal risk, that might defy precise quantification.[16]

---

11. The BCBS is an international forum for cooperation and produces guidelines on banking supervisory matters. http://www.bis.org/bcbs/. See for example: BCBS, "Working Paper of the Regulatory Treatment of Operational Risk," (2001) and BCBS, "Sound Practices for the Management and Supervision of Operational Risk," Basel Committee Publications, No. 96 (2003).
12. BCBS, "Sound Practices for the Management and Supervision of Operational Risk." (Basel Committee Publications, no. 96, 2003, 2).
13. For example, in 2001, operational risk was quantified at 2.5 billion Euros and $6.8 billion in the annual reports of Deutsche Bank and JPMorgan Chase respectively. See P. Fontnouvelle, V. DeJesus-Rueff, J. Jordan, and E. Rosengren, "Using Loss Data to Quantify Operational Risk," (Federal Reserve Bank of Boston Working Paper 2003).
14. Fontnouvelle et al., "Using Loss Data to Quantify Operational Risk," 3.
15. M. Cruz, *Modeling, Measuring and Hedging Operational Risk* (Chichester: Wiley, 2002); M. Cruz, ed., *Operational Risk Modeling and Analysis: Theory and Practice* (London: Risk Waters Group, 2004); and J. King, *Measurement and Modeling Operational Risk* (Wiley, 2001).
16. V. Chavez-Demoulin, P. Embrechts, and J. Neslehova, "Quantitative Models for Operational Risk: Extremes, Dependence and Aggregation," *Journal of Banking & Finance* 30, no. 10 (2006).

Similar problems arise from detected frauds and errors, where infrequent high value occurrences produce an uneven pattern of loss history. Compared to credit and market risk, operational risk has a dramatically different distribution[17] requiring different measurement and modeling approaches, characterized by assumptions about the statistical distribution of the loss history and calling on advanced mathematical techniques and theories.[18] The objective of such techniques is to produce both a consistent measure of risk exposure and robust estimates of value at risk (VaR). Such methods typify what is described in Basel II[19] as an advanced measurement approach (AMA).[20]

However, a consequence of attempts at modeling operational risk has been to create significant differences in terms of risk typologies, metrics and mathematical analysis. According to a recent BCBS report, these differing methods are both impediments to the integration of enterprise risk management and a promise of new modeling and measurement techniques.[21]

17. B. Nocco and R. Stultz, "Enterprise Risk Management: Theory and Practice," *Journal of Applied Corporate Finance* 18, no. 4 (2006): 8-20.
18. For example, V. Chavez-Demoulin et al., "Quantitative Models for Operational Risk: Extremes, Dependence and Aggregation," and L. Allen and T. Bali, "Cyclicality in Catastrophic and Operational Risk Measurements," *Journal of Banking & Finance* 31, no. 4 (2007): 1191-1235.
19. Basel II, agreed in 2004, is a BCBS framework for minimum capital adequacy now being implemented by national supervisory authorities.
20. Under AMA, banks must integrate internal data with relevant external loss data, account for stress scenarios, and model the factors that reflect the business environment and the internal control system.
21. See note 6 above.

Risk Management

Risk management has always been an intuitive management skill that was and is expected of all business managers. Business managers manage their revenues and costs through performance management systems. They manage their risk through observing variances in various operating metrics and combine this with their experience and judgment of those measures' historical correlation with losses and near misses. The problem with this approach is that it lacks the ability to be measured and aggregated in any systematic way. Quantifying operational risk is left to a wide range of relatively subjective analyses performed by: internal and external auditors around the Sarbanes-Oxley Act, COSO reviews and annual financial audits; cost analysis teams performing unit costing, business process re-engineering and six sigma exercises; and risk managers applying scorecards and risk and control self assessments.

It was and still is wrongheaded to believe that a historical, mathematically modeled view of past losses, manifest in capital provisioning, would prevent too much risk from being taken. Financial transactions entered into in real time have the potential of risk exposures cascading far beyond their notional values and certainly far beyond capital provisioned from past loss events.

The industry has not yet found a way to identify operational exposures and put a consistent and comparable value on them. Operational risk, in all its diversity and complexity, is thought not measurable. In the absence of such a direct exposure measurement metric, the industry has looked to loss history as being the only objective source of information on operational risks. So what would be an approach to observing the risk of loss in an operating environment?

Contrary to conventional thinking, operational risk can be measured. Just look at all the diversity in the human condition represented in a FICO score for measuring retail credit or the diversity of corporate cultures distilled into credit rating categories, or the complexity of trading strategies across multiple geographies and products synthesized into a market VaR calculation.

An answer to measuring operational risk is found in the evolution of FICO scores and credit ratings. Credit reporting was born more than 100 years ago, when small retail merchants banded together to trade financial information about their customers. Lenders eventually began to standardize how they made credit decisions by using a point system that scored the different variables on a consumer's credit report. Credit granting took a huge leap forward when statistical models were built that considered numerous variables and combinations of variables around these point systems. Today, credit analysis uses a well-defined set of inputs from the historical set of key risk indicators accumulated from many years of refining intuition into predictors of loss.

If we move over to the commercial side of credit ratings, we get a similar history and methodology from the major credit rating agencies. Their methods also refined, over a

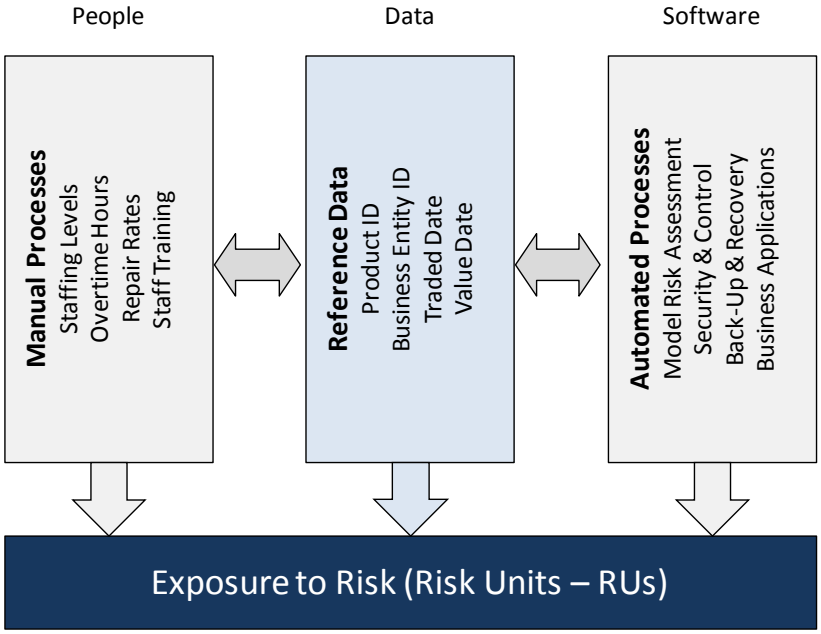
century, associate commercial credit scores into ABC rating systems where, for example, a confidence level between 99.96 and 99.98 percent has been calibrated as equivalent to the insolvency rate expected for a AA credit rating.

We start to solve the problem of determining such a metric for measuring operational risk of loss by returning to the roots of the operational risk capital charge, this being the measure of the potential for losses derived from processing transactions, for truly that is what financial institutions, in the main, do. We then make the observation that all operational processes in a financial institution are driven by transactions interacting with human, automated and data-dependent activities. Thereafter we dissect each of these pillars into a finite number of subcomponents of standardized activities that reflect key risk indicators that are known intuitively by business managers to cause losses (see Figure 1).

This is a critical observation in that each of these "pillars" of activities represents actionable elements in a transactional process. This is important if risk measurement systems are to be able to support management decisions to mitigate risk before they become losses and capital charges.

We perform this analysis by using the enterprise's personnel and documentation in a structured process that allows for the understanding of the exposures inherent in the operating environment in which the business exists and translating this knowledge into risk weights. We then use these values for the calculation of a forward-looking measure of risk exposure, a scaled inherent risk value and a risk-mitigating best-practice control value. A set of standardized risk metrics is then calculated representing inherent risk, risk mitigation effectiveness and residual risk.

Figure 1
Examples of Mapping Causes of Losses to Risk-mitigating Activities



These risk metrics, applied at the transaction level, can then be aggregated to provide departmental, divisional, subsidiary and groupwide views, and views by categories such as product, geography, business unit and risk type.

This method of calculating risk exposure provides a view of residual risk that is dynamically updated when changes in causal factors occur. In this way, the potential for statistical correlation of measurements of exposure to risk and loss history is created and, over time, will cause the risk metrics generated through this new method to become inherently predictive. This is quite different from, but complementary to, the backward-looking capital calculations that financial institutions rely upon today to gauge the largest unexpected loss that may occur within a given confidence level and time horizon.

More importantly, it is built from the ground up, allowing for the intellectual property of operating management to be imbedded in the very fabric of the risk measurement system. Institutionalizing such knowledge into the operational risk activity creates credibility and actionability—most critical components in enabling a risk culture to evolve and continual risk mitigation to be its outcome. Without a measure of risk exposure, and a dynamic mechanism for seeing it build up, we cannot take preventive actions.

The purpose of the product-based approach to risk weighting transactions in the risk accounting method described in this paper and outlined in Figure 2 is to assign ex ante values to risky processes that can subsequently be correlated with loss history events and, in turn, economic capital as they evolve.

Figure 2
Risk Accounting Overview

Information feedback loops can be developed to provide management with near real-time risk exposure and risk management data. In complementary fashion, such an approach will help build more robust, comparable and, therefore, consistent estimates of VaR. Prior work[22] has demonstrated that a common measurement framework, connecting operational metrics to risk metrics, will assist the development of better systems to account for all the dimensions of risk, including those captured in expected losses (capital reserves), unexpected losses captured in capital charges, and those yet to be captured by measurement of exposures to potential losses. This later dimension of a prospective measure of "loss potential" is best captured by the proposed introduction of a new unit of measurement for risk exposures and a methodology to map operating metrics to it, in a proposed system of risk accounting, the subject of this paper.

22. For example, A. Grody and P. Hughes, "Financial Services in Crisis: Operational Risk Management to the Rescue," *Journal of Risk Management in Financial Institutions* 2, no. 1 (2008): 47-56. See also Appendix 2.

Current State of Risk Management

Today, best practices for the mapping of an organization's granular knowledge of its operating environment to the risk management systems is done, in the main, through a continual (typically annual or quarterly) people-intense risk assessment process. Questionnaires are used by risk managers to facilitate meetings with operating management and the management group at the top of each of the business silos. Questions and discussions are focused on the status of key risks and controls and the range of expected losses, estimating their magnitude and frequency within the timeframes required for input to the capital models of the firm, including the largest expected loss usually at the 99.9 percent confidence level (a 1-in-1,000 year occurrence). Past losses are viewed in context, projects that are in place to manage risk are assessed, and new targets for further risk mitigation are planned.

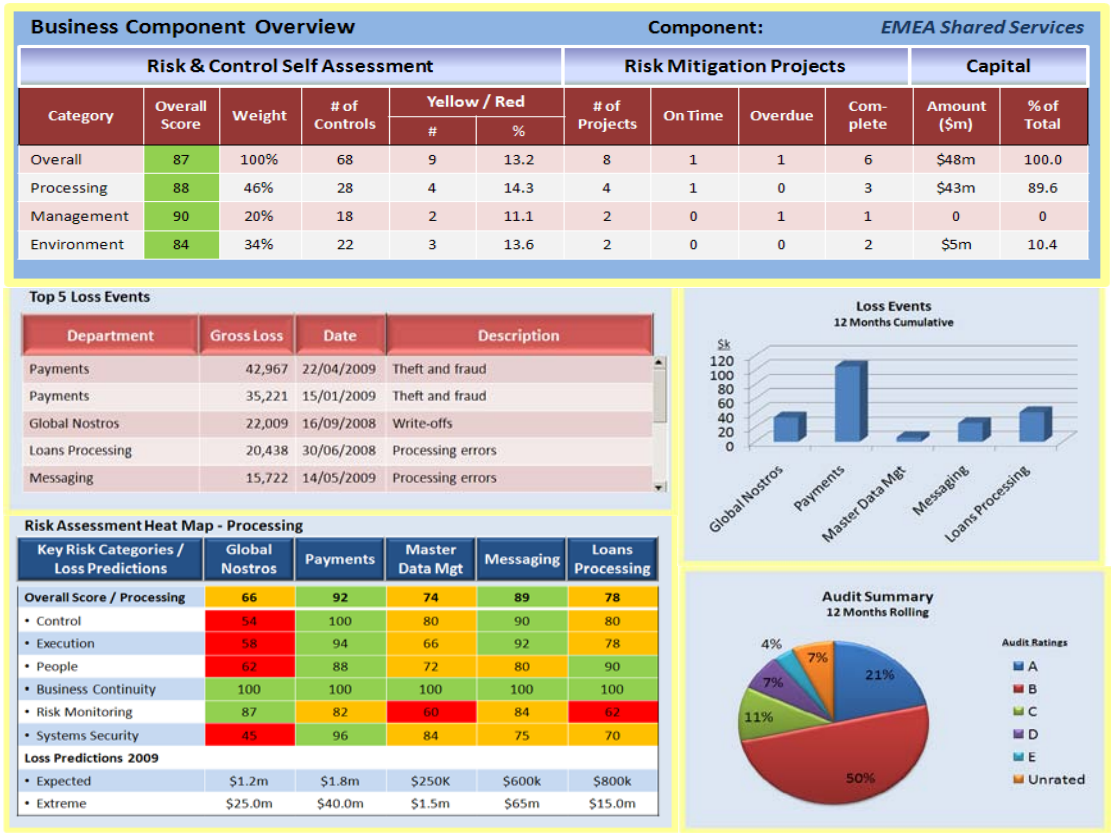
All of these discussions and projections of future losses (really "guesstimates") are summarized and subjected to a number of iterative review sessions until the capital number for operational risk for the firm is agreed and each business silo is comfortable with its own allocation of the top-of-the-house number.

The reporting of all these review sessions, loss projections and risk mitigation projects are formalized in an RCSA system characterized by the reporting of items such as counts of loss events, dates of audits and audit ratings, historical losses per activity of a particular business silo, capital assigned to each department and a color-coded scheme indicating progress in risk mitigation projects. An example of such a report is shown in Figure 3. The senior management and board are presented with a filtered view of all of these reports, highlighting the few key projects and high priority risks determined quite subjectively by the risk management officer after input from the key risk management staff and a review of the RCSA reports.

In this RCSA approach, neither senior management nor the board has the ability to observe operational-level risk metrics in any granular manner, or in the aggregate, or be able to drill down to the details of the operational risk status or issues being presented. If one were to undertake such a task, it would require a review of each of the reports at the departmental level to interpret them, which requires granular knowledge of the activities of each of the business units. This, in turn, would require interaction with departmental personnel in combination with internal audit, risk management and, perhaps, the business process re-engineering team, to assess the interpretations being presented. In fact, this process does occur, typically on a retrospective basis when a significant loss occurs.

Our proposed method of risk accounting is offered as a substitute for this backward-looking approach, providing a prospective method to observe risk exposures at both an aggregate and granular level, with the ability to drill down to the root causes of any observed increase in risk exposures. Actions can then be taken to both examine the effects of risk mitigation projects under way and to initiate new projects before exposures turn into losses.

Figure 3
Sample Risk and Control Self Assessment Report



Business Component Overview — Component: *EMEA Shared Services*

Risk & Control Self Assessment						Risk Mitigation Projects				Capital	
Category	Overall Score	Weight	# of Controls	Yellow / Red #	Yellow / Red %	# of Projects	On Time	Overdue	Com-plete	Amount ($m)	% of Total
Overall	87	100%	68	9	13.2	8	1	1	6	$48m	100.0
Processing	88	46%	28	4	14.3	4	1	0	3	$43m	89.6
Management	90	20%	18	2	11.1	2	0	1	1	0	0
Environment	84	34%	22	3	13.6	2	0	0	2	$5m	10.4

Top 5 Loss Events

Department	Gross Loss	Date	Description
Payments	42,967	22/04/2009	Theft and fraud
Payments	35,221	15/01/2009	Theft and fraud
Global Nostros	22,009	16/09/2008	Write-offs
Loans Processing	20,438	30/06/2008	Processing errors
Messaging	15,722	14/05/2009	Processing errors

Risk Assessment Heat Map - Processing

Key Risk Categories / Loss Predictions	Global Nostros	Payments	Master Data Mgt	Messaging	Loans Processing
Overall Score / Processing	66	92	74	89	78
• Control	54	100	80	90	80
• Execution	58	94	66	92	78
• People	62	88	72	80	90
• Business Continuity	100	100	100	100	100
• Risk Monitoring	87	82	60	84	62
• Systems Security	45	96	84	75	70
Loss Predictions 2009					
• Expected	$1.2m	$1.8m	$250K	$600k	$800k
• Extreme	$25.0m	$40.0m	$1.5m	$65m	$15.0m

The proposed method of risk accounting is directed at transactions to which risk weightings and scaled values are assigned. By engaging with the business line managers across the entire enterprise, both the historical and current knowledge of the operating metrics used at the business level are interpreted into the risk metrics of the proposed risk accounting system. A method to achieve this has already been published and piloted in a number of institutions. [23]

In developing the risk accounting system, an organization deploys its risk management team in each operating department to interact with operating personnel. Together, they develop risk scores that represent the department's exposure to risk and the risk mitigation effectiveness of each of the business processes that comprise their operating environment. Risk scores and/or risk weightings are determined for each business process based on three sets of standardized tables and templates that relate to risk drivers present in all business processes; they are exposure, value and risk mitigation. The resulting risk scores and weightings are applied in a scorecard where operational metrics are computed, consolidated and aggregated.

23. P. Hughes, "Operational Risk: The Direct Measurement of Exposure and Risk in Bank Operations." *Journal of Risk Management in Financial Institutions* 1, no. 1 (2007): 25-43.

Summary of Risk Accounting

Following testimony given before the U.S. House Oversight Committee in November 2008, Massachusetts Institute of Technology professor Andrew Lo commented in an interview with the Wall Street Journal, "The very fact that so many smart and experienced corporate leaders were all led astray suggests that the crisis can't be blamed on the mistakes of a few greedy CEOs. In my view, there's something fundamentally wrong with current corporate-governance structures and the language of corporate management. We just don't have the proper lexicon to have a meaningful discussion about the kinds of risks that typical corporations face today, and we need to create a new field of 'risk accounting' to address this gap in GAAP [generally accepted accounting principals]."[24]

Financial institutions need to find a way of accounting and reporting consolidated and aggregated cross-enterprise risk exposures as they accumulate. The challenge they face is analogous to the one they faced a generation or more ago as businesses evolved from legal entity-based profit centers within sovereign states into globalized lines of business. At that time, financial controllers had to learn how to tag transactions with business unit, unit cost, market segment, product and customer codes to drive cross-enterprise management performance analysis and reporting.

The new challenge is to learn how to tag those same transactions with risk-weighted exposure measures and risk-weighted financial values to produce a risk exposure metric that is additive and to do it within a framework that can actually track the value of risk mitigation efforts and drive cross-enterprise risk analysis and reporting.

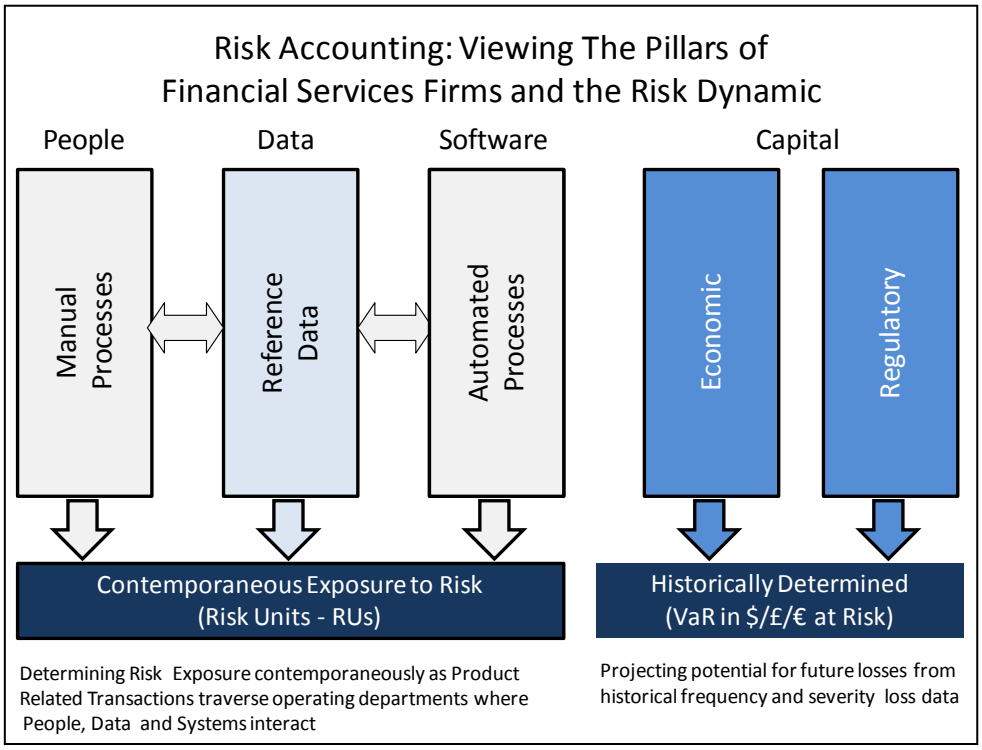
Recognizing that risk exposures are first triggered upon transactions entering the operating environment, it follows that risk exposure measurement for risk accounting and reporting purposes must be transaction based and occur at a financial institution's transaction gateway at precisely the same points that financial (general ledger) and management accounting interfaces are positioned. It is upon these basic premises that the approach to risk accounting described in this paper is constructed.

Risk accounting represents an extension of financial reporting to embrace a new risk metric, exposure to risk. It links changes in reporting of traditional VaR measures to changes in business activity and the reporting of operational and performance metrics in order to make them more effective, timely and more meaningful to stakeholders as in this formulation of the enterprise's overall risk where the sum of the diversified effects of operational, market, credit and liquidity risk capital (VaR)—a measure of the potential for the magnitude of future losses—is combined with a current and dynamically changing measure of risk exposure denominated in a new unit of measure, the risk unit (RU).

24. Wall Street Journal, "Understanding Our Blind Spots: Financial Crisis Underscores Need to Transform our View of Risk." (May 23, 2009): R2.

The RU is a mechanism to translate all manner of diversified internal processes described under the general term operational (business) activities into a common risk measurement framework, in much the same way as all manner of externally focused market and credit risks have been mapped into a common risk measurement framework, VaR, using stochastic calculus (see Figure 4). While separate and distinct in terms of managements' and regulators' use (capital is future looking, exposure is immediate and actionable), VaR and RUs are complementary measures and may be correlated. Even so, RUs measure aspects not captured by VaR and may provide a better substitute for measuring the elements that are. If true, enterprise risk can be better captured by RUs.

Figure 4
A New Paradigm for Risk Measurement



It is also possible for VaR and RUs to be correlated over time by assigning a monetary value to the RUs using a scaling factor associated with the financial dimension of the enterprise. For example, in a top-of-the-house view of enterprise risk using the standard correlation formula:

$$\text{Correlation Coefficient } \mathbf{R} = \frac{n\sum \mathit{VaR}\ \mathbf{X}\mathit{RU} - \sum \mathit{VaR}\ \mathbf{X} \sum \mathit{RU}}{\sqrt{[n(\sum \mathbf{VaR}^2 - (\sum \mathbf{VaR})^2] \ \mathrm{X}\ [n\sum \mathit{RU}^2 - (\sum (\mathit{RU})^2]}}$$

The introduction of a risk exposure metric, the risk unit, is necessitated by business managers' need to report in quantitative terms how the risks they manage are impacted by operational factors, i.e., high transaction counts, nonreconciled position values, failure counts and values of undelivered securities, overtime hours, absenteeism rates, systems downtime, number of unauthorized systems accesses, number of password changes per employee, number of internal nonclient accounts opened and a myriad of other business-level metrics. The Risk Management Association[25] has documented nearly 2,000 such key risk indicators (KRIs) for financial organizations.

These KRIs supplement the accounting records and are a major part of the performance evaluation framework available to management and the board. Some of them find their way into the annual report as commentary and footnotes, and some are used by security analysts and external auditors to further assess the performance prospects of the organization.

Some of these operating metrics become de facto industry best-practice benchmarks upon which firms gauge their performance in addition to the GAAP performance results published in the audited financial statements. They are, however, unavailable in aggregated form for executive management in a manner that equates changes in these operating factors to real-time or near real-time measures of risk exposures and, in turn, to operational loss predictions and capital requirements, which is the desired result of the method of risk accounting proposed in this paper.

25. Risk Management Association (RMA). http://www.rmahq.org/RMA/.

The Proposed Method of Risk Accounting

The method of operational risk measurement upon which the method of risk accounting has been derived has been described in prior papers[26] and in a pending patent as well as demonstrated through its diverse application in the financial services industry. Its application to the business processes that comprise financial operating environments presents comprehensive quantitative and qualitative management information concerning the risks of a financial enterprise in RUs. In this way, the risks inherent in financial operating environments can be represented by three standardized, interrelated and additive risk metrics:

> **Inherent risk** is a representation of the risk-weighted size of a financial operating environment expressed in RUs.
>
> **Risk mitigation index (RMI)** is a dynamic measure on a scale of 1 to 100 of the effectiveness of the risk management systems and controls that mitigate risk where 100 represents best practice.
>
> **Residual risk** is expressed in RUs and is the inherent risk less the risk mitigation effects of risk management systems and controls as represented by the RMI.

The RMI can be immediately adjusted when changes in the underlying causal factors occur, thereby causing residual risk to be a dynamic measure of a financial enterprise's exposure to risk. In this way, the potential for statistical correlation of measurements of exposure to risk and loss history is created, which, over time, will cause the risk metrics generated through the method described in this paper to become inherently predictive.

The application of the method in financial institutions to date has been focused primarily on transaction processing, which financial firms typically refer to as operations. Its primary aim has been to provide operations managers and their stakeholders with quantitative risk-based management information to complement the qualitative management information relating to the status of risks and controls that exists in the form of audit reports, KRIs and RCSAs.

This paper considers whether the method of operational risk measurement developed for transaction processing environments can be extended to represent an enterprise-level quantitative and qualitative risk management system. The solution described in this paper proposes a method of identifying and codifying risk information that is appended to transactions to drive cross-enterprise risk reporting. Such a solution is analogous to the work undertaken by financial controllers over a generation ago when they learnt how to codify management information (customer, product, market segment, cost center, unit cost, etc.) and append it to transactions to drive cross-enterprise management accounting and reporting. Hence, the method proposed in this paper is characterized as a next generation risk accounting and reporting system.

---

26. See note 23 above.

The method constitutes a consistent and replicable means of converting notional transaction values into risk-weighted transaction values denominated in RUs representing inherent and residual risks. Thereafter, cross-enterprise risk reporting follows the well established management accounting and reporting lines and principles.

It is important to note that the application of the method as a next generation risk accounting system is an area of ongoing research. Whereas certain tables and templates described below and their related risk weightings have been proven through more than a decade of application in diverse financial operating environments and subject to ongoing domain expert validation, there are others that exist conceptually and have not yet been subjected to field testing and expert validation. As researchers, we intend to undertake such tests and simulations in the near future.

The Method in Overview

The method operates on three underlying premises. First, inherent risk is triggered upon transactions being accepted into an operating environment for processing and that the degree of such risk is a function of a transaction's notional value and the particular types of risk inherent in the product to which the transaction relates. Second, a primary aim of an operating environment is to mitigate the risks inherent in the products and related transactions accepted for processing. Third, the rate at which operational risk exposure is created decelerates relative to the rate at which transaction volumes increase (mainly due to further automation).

The method presented in overview in Figure 2 presupposes that the risk characteristics of product types, the daily values associated with them and the risk mitigation effectiveness of operating environments can be represented through scores and risk-weightings derived from the tables and templates described in this paper and converted into standardized quantitative risk metrics expressed as inherent and residual RUs.

Calculation of Inherent Risk

Inherent risk is the cumulative value in RUs of the individual risk weightings of each product type multiplied by a value weighting. The product's risk weightings are derived from a product risk table. An extract from this table relating to market risk is shown in Figure 5.

Figure 5
Product Risk Table

Product Risk Table:	Market Risk	
Risk Criteria	**Description**	**Weighting**
Availability and reliability of market prices	Active market prices	2
	Inactive but observable market prices	5
	Unobservable prices that need judgment	8
	No prices but economic or other assumptions (demographic, holistic etc.) are required	10
Period the product has been actively traded in the business	More than 3 years	2
	Between 1 year and 3 years	4
	Between 4 months and 1 year	6
	Between 1 month and 3 months	8
	Less than 1 month	10
If the product is model dependent for pricing or valuation purposes, the extent to which the model is used across the industry	Vetted through independent audit process and in general use	2
	Used by many trading institutions	4
	Used by some reputable trading institutions	6
	Used by few trading institutions	8
	No other known users	10
The manner in which the product is traded	Electronic	2
	Hybrid (electronic + floor / voice-based)	4
	Floor / voice-based	6
	Over-The-Counter (OTC)	10
	Other	10

Note: *The above table is an extract of some of the criteria used to determine inherent market risks*

The value weighting is obtained by accumulating daily transaction notional values relative to each product accounted for in the general ledger using the following criteria:

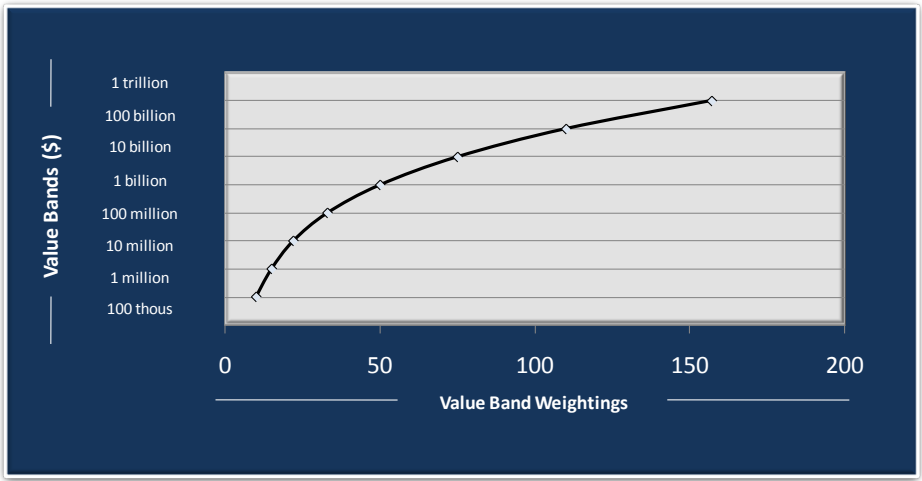
- **Transaction-based products**: Daily transaction count multiplied by average transaction value
- **Trading-based products:** Daily aggregate buys, sells and hedges
- **Portfolio-based products:** Daily change in portfolio value

The resulting values are then processed through the value table shown in Figure 6 to obtain a value band weighting.

The value table presents a logarithmic expression of the relationship between transaction values and risk. In general, operational sophistication and the effectiveness of risk mitigation increase as transaction volumes increase primarily due to enhanced automation. 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 increases in the transaction volume and values accepted for processing.

Figure 6
Value Table



The inherent risk by product is calculated in RUs on a daily basis. An example of an inherent risk calculation relative to collateralized debt obligations (CDOs) is shown in Figure 7.

Figure 7
Sample Calculation of Inherent Risk

Product: Collateralized Debt Obligations (CDOs)			
Daily Calculation	**Risk Weighting**	**Value Band Weighting**	**Inherent Risk (Risk Units)**
Processing Risk	18	75	1,350
Market Risk*	18	75	1,350
Credit Risk	12	75	900
Liquidity (Funding) Risk	8	75	600
Interest Rate (Non-Trading) Risk	-	75	-
Cumulative Risk-Weighting	**56**	**75**	**4,200**

* Includes market liquidity risk

Transaction Volume on dd/mm/yyyy	$1,233m
Value Band Weighting	75

Note: *The above scores and weightings are fictitious and are presented for illustration purposes only*

The risk weighting of 18 applied to market risk for a CDO is shown in Figure 8 and is derived from the product risk table shown in Figure 5.

Figure 8
Sample Market Risk Weighting of a CDO

Product: Collateralized Debt Obligation (CDO)		
Risk Type: Market Risk		
Risk Criteria	**Applicable Description**	**Weighting**
Availability and reliability of market prices	Unobservable prices that need judgment	8
Period the product has been actively traded in the business	Between 4 months and 1 year	6
If the product is model dependent for pricing or valuation purposes, the extent to which the model is used across the industry	Vetted through independent audit process and in general use	2
The manner in which the product is traded	Electronic	2
	Total Weighting	**18**

The Operating Environment

The operating environment for which an RMI is to be calculated is defined. Typically, this is the total enterprise or a business division thereof, for example, an investment bank or investment banking division. Such an operating environment incorporates the business components required to achieve business self-sufficiency and includes sales and marketing, operations, information technology, treasury, risk management, finance, internal audit, etc.

The risk measurement method recognizes that business components can be deconstructed into business processes and that each business process is comprised of manual and automated activities interacting with data to achieve one or more operating objectives. Thus, the risk mitigation effectiveness of an operating environment is related to two attributes. First, its ability to ensure that the transactions it accepts for processing are properly approved and processed in a complete, accurate, timely and secure manner (processing risks). Second, risks are quantified to an acceptable degree of precision and are properly reported and applied in, for example, product pricing, economic capital calculations and allocations, and for determining capital adequacy (quantification risks).

It follows, therefore, that an RMI is required relative to:

1. Processing risks: each business process, reference data source and business information system, and

2. Quantification risks: each major risk category including credit risk, market risk, operational risk, liquidity risk and interest rate (nontrading) risk.

To this end, the method provides for the calculation of an RMI at the business process level in a way that the associated inherent and residual risks in RUs can be consolidated and aggregated through to the enterprise level and at multiple intermediate levels including by organizational unit, product, risk type and geography.

A sample operating environment relating to an investment bank and its respective business components is shown in Figure 9 (this is a fictitious entity created for illustration purposes only).

The business components subject to an RMI calculation are highlighted in green or yellow. Consistent with the explanations given above, these are the components that are either processing risk-related (green) or quantification risk-related (yellow). The green components constitute elements of the end-to-end processing path that transactions follow from their origination through to ledger posting and reporting and the yellow components represent elements of the risk quantification and reporting processes.

All other business components relate to infrastructure management, administration or business development and, consequently, are not subject to an RMI calculation as the related business activities do not have a direct risk mitigation or quantification effect on the transactions accepted for processing.

Figure 9
Sample Business Components of an Investment Bank

Pre Trade Operations & Services		
Research	**Client Services**	**Sales & Marketing**
Research Production & Distribution	Client Relationship Management	Sales & Marketing
	Client Information Services	Product Sales
	Advisory Services	Product & Service Pricing
		Deal Structuring
Product Development	**Trading & Brokerage Services**	**Treasury**
Product & Service Development	Order Management	Funding
Issuance & Securitization	Pre-Trade Validation	Cash Management
	Quote Management	Depot Management
	Trade Execution & Capture	

Post Trade Operations & Services		
Trade Support	**Operations**	**Proofing & Control**
Trade Confirmation & Matching	Trade Settlement	Trading Account Reconciliations
Position Control & Amendments	Corporate Event Processing	G/L Proofs & Substantiation
Transaction Reporting	Custody Services	
Credit Limit Monitoring	Payments	
Trading Limit Monitoring	Nostro Reconcilement	
	Billing / Collections	
	Physical Commodities Management	
	Collateral & Margin Management	

Market Data Analytics	Data Management	IB Systems
Analytic Services	**Reference Data Services**	**Applications Support**
Valuation & Pricing	Client & Counterparty Data	Integrated Trading System
Scenario Management	Market Data	Funds Transfer System
Curves Management	Products & Instruments Data	Global Nostros System
Risk Quantification	Corporate Events Data	Global Ledger System
Loss Data		Funding & Liquidity System

Assurance Services		
Financial Control	**Risk Management**	**Compliance**
Financial Planning	Counterparty Credit Risk Management	Trade Monitoring
Management Reporting	Portfolio Risk Analysis	Employee Monitoring
Regulatory & External Reporting	Risk Model Back Testing	Post Transaction Review
Expense Management & Reporting	Operational Risk Management	Regulatory Information Services
Accounting Advisory Services	Capital Optimization & Limit Allocation	
Resource Allocations & Control		

Infrastructure Management		
Human Resources	**Legal & Contract Services**	**Performance Management**
Performance Management	Legal Services	Operational Efficiency Management
Recruitment & Workforce Management	Trade Contract Management	Client Profitability Management
Learning & Development	**Support Infrastructure**	Service Level Agreements
Benefits Management	Internal & External Communications	Market Share Analysis
	Internal Audit	Profitability Analysis
	Facilities Management	
	Procurement	
	Program & Change Management	

The Product Summary

A sample product summary is shown in Figure 10 relative to a CDO (all data is fictitious and is presented for illustration purposes only). The business components trade confirmation and matching, data risk and market risk are supported by detailed scorecards and related calculations presented in figures 11, 12 and 13 respectively.

Figure 10
Sample Product Summary

Collateralized Debt Obligations (CDOs)

Date: DD/MM/YYYY

Product Summary	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)		
	Risk Metrics				
Processing Risk					
Transaction Processing Risk					
Product & Service Pricing	1,350	63.5	493	IB Front Office	Decentralized
Deal Structuring	1,350	55.2	605	IB Front Office	Decentralized
Order Management	1,350	68.2	429	IB Front Office	Decentralized
Pre-Trade Validation	1,350	62.3	509	IB Front Office	Decentralized
Quote Management	1,350	73.4	359	IB Front Office	Decentralized
Trade Execution & Capture	1,350	44.9	744	IB Front Office	Decentralized
Cash Management	1,350	52.3	644	Operations	Centralized
Trade Confirmation & Matching*	1,350	60.0	540	Operations	Centralized
Position Control & Amendments	1,350	60.2	537	Operations	Centralized
Transaction Reporting	1,350	63.2	497	Operations	Centralized
Credit Limit Monitoring	1,350	45.0	743	Operations	Centralized
Trading Limit Monitoring	1,350	62.4	508	Operations	Centralized
Trade Settlements	1,350	63.4	494	Operations	Centralized
Nostro Reconcilement	1,350	72.8	367	Operations	Centralized
Trading Account Reconciliations	1,350	66.7	450	Operations	Centralized
G/L Proofs & Substantiation	1,350	73.3	360	Operations	Centralized
Management Reporting	1,350	64.2	483	Finance	Centralized
Regulatory & External Reporting	1,350	64.2	483	Finance	Centralized
Control Totals	24,300	62.0	9,245		
Transaction Processing Risk	1,350	62.0	514		
Data Risk*					
Client & Counterparty	1,350	79.2	281		
Market Data	1,350	52.9	636		
Products & Instruments	1,350	68.2	429		
Corporate Events	1,350	43.3	765		
Control Totals	5,400	60.9	2,111		
Data Risk	1,350	60.9	528		
Business Information Systems Risk					
Integrated Trading System	1,350	78.9	285		
Funds Transfer System	1,350	65.4	467		
Global Nostros System	1,350	65.0	473		
Global Ledger System	1,350	82.3	239		
Funding & Liquidity System	1,350	69.4	413		
Control Totals	6,750	72.2	1,877		
Business Information Systems Risk	1,350	72.2	375		
Control Totals	36,450	63.7	13,233		
Total Processing Risk Metrics	1,350	63.7	490		
Quantification Risk					
Credit Risk	900	65.3	312		
Market Risk*	1,350	43.9	758		
Liquidity Risk	600	55.0	270		
Interest Rate (Non-Trading) Risk	-	-	-	Trading product - IRRBB is N/A	
Total Quantification Risk Metrics	2,850	53.0	1,340		
Product Operational Risk	4,200	56.4	1,830		

* Sample scorecards relating to these components are shown in Figures 11, 12 & 13

The product summary is developed by identifying the business components on the product's end-to-end transaction processing cycle's critical path and the reference data sources and business information systems they interact with. The business components that process the product's transactions (transaction processing risk) are deconstructed to identify the individual processes, as illustrated in Figure 11, at which level the RMI and inherent and residual risks in RUs are calculated.

The sample product summary in Figure 10 shows the total exposure to operational risks generated by CDOs on a particular day. The total inherent risk is 4,200 RUs, residual risk is 1,830 RUs and the RMI is 56.4. The calculation of the inherent risk for each component is shown in Figure 7.

The amount of inherent risk applied to each business component and risk category within processing risks is the same (1,350 RUs). The repetition of the inherent risk recognizes that each component handles the respective product-related transactions as an organizationally segregated operations unit and, consequently, independently exposes the full amount of inherent risk.

The business components listed under transaction processing risk in Figure 10 show the relevant organizational unit—IB front office, operations and finance—with an indication whether processing is centralized or decentralized. The inherent and residual risks presented in the product summary are additive and, consequently, the totality of products handled by each centralized or decentralized component can be consolidated and aggregated and the RMI recalculated. In this way, inherent and residual risks can be summed for all the products handled by each centralized or decentralized business component to produce total risk metrics by business component or hierarchically from the product (lowest) through to the total enterprise (highest) level.

The Scorecards

The sample scorecards presented in figures 11, 12 and 13 show the calculation of RMIs and inherent and residual risks in RUs relative to transaction processing, reference data sources and market risk respectively. Typically, risk metrics for transaction processing-related business components are calculated at the more granular process level and others are calculated at the business component level. This recognizes that transaction handling processes are designed to process and control transactions that are value-bearing, whereas processes that maintain reference data sources, business information systems and risk quantification are generally not value-bearing. Consequently, transaction processing components have a greater need for more granular risk assessment, analysis and management information. However, inasmuch that non-transaction processing components are also comprised of manual and automated processes interacting with data, it is an optional possibility to calculate risk metrics at the process level.

The sample scorecard shown in Figure 11 relates to the business component trade confirmation and matching and illustrates the calculation of risk metrics relating to CDOs on a particular day.

The process risk weightings shown in the scorecard are derived from an activity table that is a catalogue of pre-identified processing activities to which a fixed risk weighting has been assigned. This risk weighting represents the relative immediacy and likelihood of financial loss in the event of process failure. For example, a process that involves the release of funds has a higher risk weighting (higher loss immediacy) than a process that involves the matching of trade confirmations (lower loss immediacy).

Such processing objectives or activities are collectively referred to as activity types and include the following (this is not an exhaustive list):

- Prepare, capture and control transactions
- Process transactions
- Transaction (deal) confirmation
- Release value items
- Prepare and issue reports
- Independent verification and validation
- Determine and control cash positions

Current versions of the method use a catalogue comprised of 34 activity types and associated risk weightings. The actual activities of each process are mapped to the activity types in the catalogue and where there is a match, the applicable activities and risk weightings are extracted and applied in the respective scorecard. The inherent risk on a given day (1,350 RUs in Figure 11) is distributed to individual processes in proportion to their total activity risk weightings.

Best Practice Scoring Templates

The risk mitigation effectiveness of each process is then determined and scored by reference to best practice scoring templates (figures 14 and 15), which can be one of two types:

Type 1. Benchmark Data

Type 1 scoring templates include execution and people. In these templates, benchmark data are presented that delineate scores in fixed intervals between zero and 100. Appropriately graduated benchmarks and/or status descriptions are assigned to each score interval. Scores are determined for each Type 1 template by identifying the benchmark and/or status description that best matches the current status or condition of the element being scored.

Type 2. Best Practice Statements

Type 2 scoring templates include business recovery, model management and data quality management. In these templates, best practice statements are presented and a value between zero and 100 (deductible points) is assigned to each statement representing its relative risk mitigation impact. Each template is assigned a starting score of 100 and for each best practice statement that does not apply to the current status or condition, the respective deductible points assigned to that statement are deducted from the starting score. The lowest possible score is zero.

Figure 14 shows a detailed model management scoring template that is aligned to qualitative standards issued by the Basel Committee on Banking Supervision[27] and relates to the market risk quantification scorecard shown in Figure 13. A further six summarized examples of best practice scoring templates relating to transaction processing and reference data sources are shown in Figure 15 whereby the respective deductible points in Type 2 templates relative to each best practice statement are shown in brackets.

The scoring templates are structured such that there is only one score, within a reasonable tolerance, applicable to the status or condition of the process or component being scored. This has the effect of characterizing the RMI as a true measurement metric as opposed to an assessment metric thereby reducing subjectivity in the measurement process.

Where there is more than one subcategory within a primary category in a Type 1 template, a lower score displaces a higher score. This occurs because the condition that gave rise to the higher score is invariably impacted negatively by the condition represented by the lower score. For example, in the primary category execution, a straight-through-processing

27. Basel Committee on Banking Supervision, "Amendment to the Capital Accord to Incorporate Market Risks." (2005): 36-37.

(STP) rate of 100 percent is of limited value if the underlying business information system is highly unstable, characterized by 12 or more failures in a year.

Figure 14
Best Practice Scoring Template: Model Management

Model Management	
Relates to the management of the product's models used for risk pricing, valuation, value-at-risk (VaR) calculations and capital adequacy	
Best Practice Score = 100 Points	
Best Practice Statements	**Deductible Points**
Responsibility for the management of the product's model is assigned to an independent risk control unit	100
The product's position is valued at least daily by marking-to-market at readily available close-out prices that are sourced independently in a process under the direct management and control of the independent risk control unit[1]	100
The independent risk control unit conducts a regular back-testing program of the product's model[2]	80
The independent risk control unit conducts the initial and on-going validation of the internal model[3]	80
The independent risk control unit produces and analyzes daily reports produced by the product's model including an evaluation of the relationship between measures of risk exposure and trading limits	70
The product's model is subject to a routine and rigorous program of stress testing[4]	60
Risk factors incorporated into the product's pricing model are also incorporated into the product's value-at-risk (VaR) model	50
An independent review of the model is carried out regularly (at least once a year) by the bank's own internal audit function[5]	40
Daily reports prepared by the independent risk control unit are reviewed by senior management[6]	30
The product's trading and exposure limits are related to the model in a manner that is consistent over time and that is well-understood by both traders and senior management	25

Guidance Notes:

1. *If there are no readily available "active" market prices for the product, the statement is not applicable so no points are deductible.*
2. *Back-testing at a minimum must include a comparison of the risk measure generated by the model against actual daily changes in portfolio value over longer periods of time as well as hypothetical changes based on static positions.*
3. *Validation at a minimum must include ensuring that any assumptions made within the internal model are appropriate and do not underestimate risk.*
4. *Guidelines for stress testing are set out in the Basel Committee on Banking Supervision's November 2005 "Amendment to the Capital Accord to Incorporate Market Risks" Part B.5.*
5. *Internal audit's review must be conducted by suitably qualified individuals and at a minimum must include the verification of: the consistency, timeliness and reliability of data sources used to run internal models and the independence of such data sources; the accuracy and appropriateness of volatility and correlation assumptions; the accuracy of valuation and risk transformation calculations; and the verification of the model's accuracy through frequent back-testing.*
6. *Senior management means individuals with sufficient seniority and authority that they can enforce both reductions of positions taken by individual traders and reductions in the bank's overall risk exposure.*

In stress conditions, it is assumed the degree of reliance placed on each risk category in the prevention of operational failure is different. The method recognizes this differentiation by assigning category weightings to each of the primary risk categories. The category weightings relative to each of the risk categories in transaction processing, reference data sources and market risk quantification are shown in figures 11, 12 and 13.

It can be noted that the category weightings are not necessarily consistent from scorecard to scorecard. For example, control evaluation has a category weighting of 10 for transaction processing and 3 for reference data sources. This is consistent with the above

discussion that transaction processing cycles are designed for value-bearing processes and, consequently, internal controls have greater risk mitigation significance than processes designed to maintain reference data that are not value-bearing.

Figure 15
Sample Best Practice Scoring Templates (Summarized)

Execution:
Levels of automation vs. manual workarounds; levels of repair rates; and the stability of core application(s).

Level of automation or STP rate:
- 100% score 100 (Best Practice)
- 75% score 75
- 50% score 50
- 25% score 25
- 0% score zero

Average percentage of input rejection / repair:
- 0% score 100 (Best Practice)
- 5% score 75
- 10% score 50
- 25% score 25
- 50% score zero

Number of core system failures in year:
- None score 100 (Best Practice)
- 1 score 75
- 2 score 50
- 4 score 25
- > 12 score zero

People:
Stress, accountability, experience, depth of cover and availability of staff

Average levels of overtime hours per person per month over last 3 months:
- 20 or less score 100 (Best Practice)
- 30 score 75
- 40 score 50
- 60 score 25
- 80 or more score zero

Percentage of temporary and new staff to total existing staff:
- 0% score 100 (Best Practice)
- 20% score 75
- 40% score 50
- 60% score 25
- 80% or more score zero

Percentage of activities / controls that can be performed by alternate staff:
- 100% score 100 (Best Practice)
- 90% score 75
- 75% score 50
- 50% score 25
- 25% or less score zero

Data Quality Management:
Faulty data is identified, researched and eliminated in an acceptable timeframe

Best Practice score 100

Deduct following scores from Best Practice score if statement does not apply:
- Business Critical Data Elements validated to at least one independent source or imported through an approved source (100)
- Expert resources positioned and empowered to enhance data through appropriate research (100)
- Independent quality assurance applied to expert data enhancements (75)
- Audit trail available for data validation provenance (50)
- Defined and monitored process to escalate recurring issues (25)
- Defined and monitored process to provide feedback to supplier source of recurring issues (25)
- Automated controls within core application (25)
- Data formatting standards exist for each of the defined data elements (10)

Business Recovery:
Continuation of operations at an alternative site in a timeframe that is acceptable

Best Practice score 100

Deduct following scores from Best Practice score if statement does not apply:
- Recovery or reactivation at alternative site in acceptable timeframe (100)
- Formal business recovery plan (100)
- End-to-end disaster simulation (75)
- Plan complete and comprehensive (30)
- Supervisory review of plan (20)
- Key employees fully briefed (15)
- Key employees active participation in disaster simulation (10)
- Business recovery specialist review of plan (10)
- Key employees' contact details current (5)
- Notification test performed (5)
- Key employees ready access to offsite copy of plan (5)

The Calculations

The best practice scoring templates shown in figures 14 and 15 are scored whereby each score represents the actual status relative to best practices. Scores are updated upon changes or dynamically through automated interfaces (e.g., people scores via the human resources system). Scores are then blended with two other weightings:

1. The category weightings on a scale of 1 to 10 shown in figures 11, 12 and 13, which are calibrated according to the relative risk mitigation impact of each risk category, and

2. The inherent risk representing risk-weighted business processes or components.

From these inputs, risk metrics are calculated using the formulas below where W = weightings, S = scores, VT = value table (Figure 6), PRT = product risk table (Figure 5) and BPST = best practice scoring templates (figures 14 and 15):

- Inherent risk RUs (InhRU) $= PRT^{W} \times VT^{W}$

- Risk mitigation index (RMI) $= \dfrac{\Sigma\,(BPST^{S} \times BPST^{W} \times InhRU)}{\Sigma\,(100 \times BPST^{W} \times InhRU)} \times 100$

- Residual risk RUs (ResRU) $= \dfrac{(100 - RMI)}{100} \times InhRU$

Conclusion

The method described in outline in this paper addresses the recent academic literature and the regulatory agenda in bank risk reporting. It achieves this by offering, in conjunction with current top-down practices, a bottom-up transactional method that offers tractable managerial information in conjunction with established methods and an extension of current financial reporting through additions to the underlying accounting system.

If techniques can be applied for the better management of risk factors, as herein described in our view of a risk accounting method and system, their disclosure and audit should add value from the perspective of the stakeholder community. Investors potentially face a "market for lemons" problem,[28] in which they have difficulty discerning effective management processes from the ineffective. Such problems might be compounded insofar as specialist and technical disclosures have no information content for outside investors.[29] There is thus a quality signaling rationale for disclosures that effectively convey the truth of superior processes to non-specialist investors.[30] At the same time, the process and the information generated by the risk accounting method outlined in this paper can both be subject to audit and external scrutiny, and correlated to actual loss experience over time, adding to their consistency and credibility.

To the extent that our method of risk accounting is successful, there is reassurance for regulators and a "better markets" solution that, in the face of the current financial meltdown, is surely needed.

These authors humbly suggest that new directions are possible, and that this proposed method, perhaps in its minimalist contribution, would simply stimulate others toward further research into these new directions.

28. G.A. Akerlof, "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics* 84, no. 3 (1970): 488-500.
29. S. Brown et al., "Mandatory Disclosure and Operational Risk: Evidence from Hedge Fund Registration," *Journal of Finance*, forthcoming (2008). Note: Register with Oxford Journals to obtain a user name and password at no charge.
30. S. Toms, "Firm Resources, Quality Signals and the Determinants of Corporate Environmental Reputation: Some UK Evidence." *British Accounting Review* 34 (2002): 257-82.

Figure 11
Sample Transaction Processing Business Component Scorecard and Calculations

Component: Trade Confirmation & Matching

DD/MM/YYYY — Inherent Risk 1,350 Risk Units

Activity Descriptions & Weightings	Activity Weighting	Inherent Risk (Risk Units)	Risk Categories & Weightings	Control Evaluation	People	Execution	Business Recovery	Risk Culture / Management	Management Oversight	Logical Access Management	Physical Access	Policies & Procedures	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Inherent Risk (Risk Units)	Actual Score Aggregate	Best Practice Aggregate
				10	10	10	8	6	6	4	4	2					
Team A																	
Control and distribute value bearing instructions	4																
General Administration	1																
	5	250	Process 1	25	50	45	15	50	75	75	100	50	250	47.8	130	717,500	1,500,000
Prepare, capture and control transactions	4																
General Administration	1																
	5	250	Process 2	80	100	50	0	30	50	40	100	20	250	56.3	109	845,000	1,500,000
Issue and match deal confirmations	6																
Prepare and issue internal reports	2																
	8	400	Process 3	25	50	45	15	50	75	75	100	50	400	47.8	209	1,148,000	2,400,000
Team A - Inherent Risk		**900**	**Team A - RMI**	**40.3**	**63.9**	**46.4**	**10.8**	**44.4**	**68.1**	**65.3**	**100.0**	**41.7**	**900**	**50.2**	**448**	**2,710,500**	**5,400,000**
Team B																	
Independent verification / validation	4																
	4	200	Process 1	70	70	50	100	100	100	70	100	100	200	79.7	41	956,000	1,200,000
Resolution of client initiated queries	3																
Process transactions	2																
	5	250	Process 2	70	70	50	100	100	100	70	100	100	250	79.7	51	1,195,000	1,500,000
Team B - Inherent Risk		**450**	**Team B - RMI**	**70.0**	**70.0**	**50.0**	**100.0**	**100.0**	**100.0**	**70.0**	**100.0**	**100.0**	**450**	**79.7**	**92**	**2,151,000**	**2,700,000**
Total	27	1,350	**Component - RMI**	**50.2**	**65.9**	**47.6**	**40.6**	**63.0**	**78.7**	**66.9**	**100.0**	**61.1**	**1,350**	**60.0**	**540**	**4,861,500**	**8,100,000**
			Score Aggregate	362,500	575,000	417,500	78,000	240,000	367,500	235,000	360,000	75,000					
			Best Practice Aggregate	900,000	900,000	900,000	720,000	540,000	540,000	360,000	360,000	180,000					
			Score Aggregate	315,000	315,000	225,000	360,000	270,000	270,000	126,000	180,000	90,000					
			Best Practice Aggregate	450,000	450,000	450,000	360,000	270,000	270,000	180,000	180,000	90,000					
			Score Aggregate	677,500	890,000	642,500	438,000	510,000	637,500	361,000	540,000	165,000					
			Best Practice Aggregate	1,350,000	1,350,000	1,350,000	1,080,000	810,000	810,000	540,000	540,000	270,000					

Figure 12
Sample Reference Data Source Business Component Scorecard and Calculation

Component:	Reference Data Services															
DD/MM/YYYY			Inherent Risk	1,350	Risk Units											
Risk Categories & Weightings	Quality Management	Data Management	People	Risk Culture	Uniqueness	Vendor Data Services	Policies & Procedures	Management Information	Logical Access Management	Business Recovery	Control Evaluation	Inherent Risk	Risk Mitigation Index (RMI)	Residual Risk	Actual Score Aggregate	Best Practice Aggregate
	10	10	5	5	4	4	4	4	4	3	3					
Client & Counterparty Data	75	85	80	80	85	75	70	75	80	85	80	1,350	79.2	281	5,987,250	7,560,000
Market Data	45	50	65	50	50	65	75	45	45	55	50	1,350	52.9	636	3,996,000	7,560,000
Products & Instruments Data	65	65	60	70	75	75	80	65	60	75	75	1,350	68.2	429	5,157,000	7,560,000
Corporate Events Data	35	30	35	45	55	45	55	50	60	55	50	1,350	43.3	765	3,273,750	7,560,000
Risk Mitigation Index (RMI)	**55.0**	**57.5**	**60.0**	**61.3**	**66.3**	**65.0**	**70.0**	**58.8**	**61.3**	**67.5**	**63.8**	**1,350**	**60.9**	**528**	**18,414,000**	**30,240,000**
Score Aggregate	2,970,000	3,105,000	1,620,000	1,653,750	1,431,000	1,404,000	1,512,000	1,269,000	1,323,000	1,093,500	1,032,750					
Best Practice Aggregate	5,400,000	5,400,000	2,700,000	2,700,000	2,160,000	2,160,000	2,160,000	2,160,000	2,160,000	1,620,000	1,620,000					

Figure 13
Sample Market Risk Quantification Business Component Scorecard and Calculation

Component: Market Risk

Risk Categories & Weightings	Model Management	People	Execution	Policies & Procedures	Control Evaluation	Logical Access Management	Business Recovery	Management Oversight	Inherent Risk	Risk Mitigation Index (RMI)	Residual Risk	Actual Score Aggregate	Best Practice Aggregate
	10	10	4	2	2	2	2	2					
Collateralized Debt Obligations (CDOs)	0	40	80	80	85	75	70	75	**1,350**	**43.8**	**758**	2,011,500	4,590,000
Product 2	75	50	65	50	50	65	75	45	**875**	**61.2**	**340**	1,820,000	2,975,000
Product 3	40	65	60	70	75	75	80	65	**950**	**59.4**	**386**	1,919,000	3,230,000
Product 4	0	30	35	45	55	45	55	50	**1,105**	**27.6**	**800**	1,038,700	3,757,000
Risk Mitigation Index (RMI)	**24.2**	**45.0**	**60.9**	**62.6**	**67.9**	**65.2**	**69.4**	**60.2**	**4,280**	**46.7**	**2,283**	6,789,200	14,552,000
Score Aggregate	1,036,250	1,926,500	1,042,200	535,950	581,050	558,200	593,800	515,250					
Best Practice Aggregate	4,280,000	4,280,000	1,712,000	856,000	856,000	856,000	856,000	856,000					