Risk Accounting

The Risk Data Aggregation and Risk Reporting (BCBS 239) Foundation of Enterprise Risk Management (ERM) and Risk Governance

Allan D. Grody, Peter J. Hughes

Allan D. Grody is President of Financial Intergroup Holdings Ltd (New York, NY, US), former adjunct professor of Risk Management Systems at NYU's Stern Graduate School of Business and a founding Editorial Board member of the Journal of Risk Management in Financial Institutions.
agrody@FinancialinterGroup.com

Peter J. Hughes FCA is Managing Director of Financial InterGroup (UK) Ltd, a Visiting Research Fellow at the Leeds University Business School and a member of the Advisory Board of Durham University Business School's Banking, Risk & Intermediation Research Group.
peter.hughes@FinancialInterGroup.com

February 2016

Table of Contents

Figures

Risk Accounting: The Risk Data Aggregation and Risk Reporting (BCBS 239) Foundation of Enterprise Risk Management (ERM) and Risk Governance

Allan D. Grody, Peter J. Hughes

February 2016

Abstract

In the period following the global financial crisis high profile regulatory breaches and other instances of banks' misconduct triggered widespread concern that the culture and standards of conduct in banks had declined to a point of unacceptability. The crisis also brought into sharp focus the inability of banks to completely and accurately report the risks they accept in order to create shareholder value. These events and circumstances culminated in a crisis of trust between banks and their stakeholders that include governments, regulators, investors and customers.

In this same period regulators focused on their primary 'capital-at-risk' regimes administered through the Basel capital accords, reinforcing additional levels of capital as a bank's primary protection against unexpected losses. At the same time Basel introduced 'firm-at-risk' mandates that required improvements in banks' control over risk data and associated technology infrastructure.

The most significant game changing post-crisis regulatory mandate in this regard is the Basel Committee's principles for effective risk data aggregation and risk reporting also known as 'BCBS 239'. This new mandate requires banks: to implement controls over risk data that are as robust as those applicable to accounting data; to create accurate and single authoritative sources of risk data; and to ensure the precision, timeliness, comprehensiveness and adaptability of risk reporting. BCBS 239 effectively sets the parameters for enterprise risk management (ERM) and provides the foundation on which risk governance and risk cultures can positively evolve.

Whereas BCBS 239 expressly states that a common risk metric for all forms of risk is not required, the authors challenge this thinking and argue that it is only through the adoption of a common risk metric that the objectives of BCBS 239 can be reasonably achieved.

Part 1 of this paper explains why bankers – risk managers and accountants in particular – must view the need for the convergence of finance and risk systems within a common control and reporting framework as an imperative. Part 2 describes the 'Risk Accounting' methodology and its introduction of both a common measurement framework for all forms of risk and a common risk metric, the 'Risk Unit' or RU.

Key words*: Risk accounting, Basel II, Basel III, Risk measurement, Risk management, BCBS 239, Risk data aggregation, Operational risk, Enterprise risk, Risk appetite, Risk culture, Governance*

Part 1

Introduction

The successive capital accords issued by the Basel Committee on Banking Supervision (Basel Committee) have had little impact on the ability of banks to prevent losses which raises concerns as to whether the risk calculation methods applied in the calibration of regulatory capital are fit for purpose. This has been the continuing focus of public comment by global regulators, central bankers and industry commentators. These comments suggest that excessively complex and flawed capital adequacy rules resulted in banks being insufficiently capitalized in relation to the true amount of accepted risks that remained unidentified and unreported in banks' audited financial statements.

The regulators' short-term response to these circumstances, primarily through Basel III[1], was to require banks to build deeper and higher quality reserves of capital and liquidity with the aim of increasing their capacity to buffer unexpected losses and weather liquidity crises. Additional regulatory devices were also introduced, such as the leverage ratio, which serves as a backstop to the risk based capital measures, which proved to be unreliable, by providing an extra layer of protection against model risk and measurement error.

The longer-term response of regulators is focused on implementing more robust enterprise risk management (ERM) frameworks and technology infrastructures. The most significant and potentially game changing post-crisis regulatory mandate in this regard is BCBS 239[2].

BCBS 239 requires banks, among other requirements, to implement controls over risk data that are as robust as those applicable to accounting data and to provide assurance that aggregated risk data reflects all accepted risks in an exact manner. This paper proposes that BCBS 239 constitutes the enabler of true ERM systems as a foundation for effective governance and improved risk cultures.

It is apparent from the Basel Committee's December 2015 progress report[3] on the implementation of BCBS 239 that banks are falling short of its requirements. This status was further confirmed by a prominent industry survey conducted by EY in 2014[4]. The progress report and survey are examined later in this paper in the sections 'Risk Data Aggregation' and 'Risk and Culture – An Industry View' respectively.

---

[1] Basel Committee on Banking Supervision (2010), 'Basel III: A global regulatory framework for more resilient banks and banking systems', Bank for International Settlements, available at http://www.bis.org/publ/bcbs189.pdf (accessed 7th February 2016)

[2] Basel Committee on Banking Supervision (2013), 'Principles for effective risk data aggregation and risk reporting', Bank for International Settlements, available at http://www.bis.org/publ/bcbs239.pdf (accessed 7th February 2016)

[3] Basel Committee on Banking Supervision (2015), 'Progress in adopting the principles for effective risk data aggregation and risk reporting', Bank for International Settlements, available at http://www.bis.org/bcbs/publ/d348.pdf (accessed 7th February 2016)

[4] EY (2014), 'Shifting focus: risk culture at the forefront of banking', available at: http://www.ey.com/GL/en/Industries/Financial-Services/Banking---Capital-Markets/ey-shifting-focus-risk-culture-at-the-forefront-of-banking (accessed 7th February 2016)

The industry survey commented that regulatory breaches and misconduct issues that have shocked the industry over the past several years have driven a sharpened focus on the evident deterioration of standards of conduct and risk culture within banks. One particularly alarming statistic from the survey aptly illustrates the dire condition in which banks and their stakeholders find themselves; "…an overwhelming 93% of the global systemically important banks (G-SIBs) surveyed agreed that weak oversight and controls led to the (numerous regulatory and misconduct) failures."

The authors take the view that a primary cause of deterioration in standards of conduct is the absence of a system of risk metrics and controls that reliably communicate accepted risks in a consistent, timely and comprehensive manner. A significant contributing factor to the unreliability of risk metrics is the lack of effective controls over the risk data that supports these metrics.

This simple metaphor is offered to illustrate the point:

> *Car drivers intuitively respect and follow road traffic controls… the signage and road markings that are designed to enhance traffic flow and prevent accidents. They have become a societal norm. If we were to look into the future and imagine that cars are being manufactured that can also fly, it wouldn't require much imagination to envision the chaos that would ensue if today's road traffic controls were not adapted to also function above the ground.*

This metaphor, in effect, describes today's global financial system. Banks are flying above the financial accounting and control systems that were designed for a bygone era when risk concentrations within and between financial firms were innocuous. The purpose of today's accounting systems is to provide validated and proven accounting data used in the preparation of static, point-in-time statements of financial condition published in audited financial statements based, primarily, on the prevailing fair values of assets and liabilities. They were never intended to consider the potential financial consequences of the often massive concentrations of risk that have become a feature of today's banks and the global financial system. If accounting and control systems are not 'risk-adjusted' relative to the exponential growth in risk concentrations, the systems required to report accepted risks, including their monitoring against approved levels of risk appetite will not meet their dual objectives of controlling risk behavior and minimizing unexpected losses.

As was evident from the financial crisis of 2007-2008 massive risks were accepted by banks that remained unreported. If banks and bankers are allowed to operate in a risk control environment safe in the knowledge that the risks they either knowingly or unknowingly accept are likely to escape proper identification, quantification and reporting, negative behaviors will be the inevitable outcome.

This paper argues that a system of effective control over risk data requires new techniques that enable the convergence of risk and accounting data within a common control and reporting framework. The result would be the still awaited true ERM framework enabled by effective risk data aggregation upon which programs of effective and meaningful risk governance can be based. This is the vision of regulators as set out in BCBS 239.

In Parts 1 & 2 of this paper the authors describe new techniques collectively referred to as Risk Accounting. In brief terms, Risk Accounting involves tagging coded risk information onto transactions

upon their posting in accounting systems. Such tagged risk information complements the existing financial and management codes that define the aggregation paths for financial and management reporting. The combined risk and financial information of each transaction is then used in a standardized calculation of risk-weighted transaction values that are accounted for using a new additive risk metric, unique to the Risk Accounting method, the Risk Unit or 'RU'.

With such an additive risk metric a comprehensive ERM system allowing for all risk types to be aggregated is created and tied to the financials of the enterprise as required by BCBS 239.

The authors further demonstrate how risk accounting aligned with management accounting can produce a system of integrated risk and financial reporting by, for example, group, legal entity, organisational unit, product, customer and geography which, in turn, enables the risk appetite setting process to become an integral part of the enterprise's financial planning and budgeting cycle.

The authors believe that over time the outputs from Risk Accounting can be correlated with actual loss history thereby imparting a monetary value to the RU. Hughes et al[5] describe how this valuation of the RU can then be used in: the determination of regulatory capital requirements; the computation of risk adjusted return on capital (RAROC); and in adjusting the betas in the capital asset pricing model (CAPM), thus bridging accounting with economic theory and risk management concepts.

This paper sets out to position Risk Accounting as the next generation accounting and control system for financial enterprises that enables both an effective ERM system and the alignment of accepted risks and financial performance within a common reporting and governance framework.

Accounting Standards and Risk

The opinions of independent public accounting firms included in published financial statements typically follow these lines:

> *In our opinion, the (financial statements) present fairly, in all material respects, the financial position, the results of the operations and the cash flows of (company) and its subsidiaries for (dates) in conformity with International Financial Reporting Standards as issued by the International Accounting Standards Board. Also in our opinion, (company) maintained, in all material respects, effective internal control over financial reporting as of (date), based on criteria established in Internal Control – Integrated Framework (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

International Financial Reporting Standards (IFRS) and Generally Accepted Accounting Standards (GAAP) are framed to produce a static point-in-time statement of financial condition based, primarily, on the fair values of assets and liabilities that prevail at the time of reporting. IFRS, GAAP and the opinions expressed by public accountants are not intended to consider the financial consequences of

[5] Fernandes, KJ. and Grody, AD. and Hughes, PJ. and Phillips, O and Toms, JS (2013) 'Risk Accounting: An Accounting Based Approach to Measuring Enterprise Risk and Risk Appetite', pp. 28-33, available at SSRN: http://ssrn.com/abstract=2165034 (accessed 7th February 2016)

accepted risks should macroeconomic and other operating conditions change. In other words, they do not give assurance that a firm's risk position is, or is not endangering its financial position.

Thus, accounting has been more concerned with valuation than the prediction of the probability and severity of future losses that are likely to occur as market and macroeconomic conditions change. This limits the usefulness of audited financial statements as there is limited assurance that they incorporate the profit and loss and balance sheet implications of accumulating risks.

In recent years the accounting profession has attempted to address this situation by introducing accounting practices that recognize, in accounting terms, the loss potential inherent in financial products. For example, in the 1980s banks began to incorporate fair market valuations into their accounting through marking (valuing) their trading positions to market values ('mark-to-market') and, more recently, marking such positions to financial models ('mark-to-model').

Whereas banks are required to disclose the methods they apply in the quantification of risk and how this relates to capital reserves, the diversity of modeling approaches adopted and their inherent complexity limits regulators' and investors' insight into how much risk a bank has accepted absolutely and the amount of risk accepted by one bank in comparison with others.

Effective bank regulation also suffers from the absence of standardized data and reporting formats. Such standardization would facilitate an automated means to routinely provide regulators with information relating to banks' accumulating risk exposures derived from a common risk quantification and reporting framework.

As banks increase in size and complexity, their inability to reliably and consistently quantify and report accumulating exposures to risk constitutes a significant problem for regulators and investors. Modern financial institutions now reflect the consequences of massive increases in concentrations of risk resulting from: the heightened complexity of financial instruments; the creation of more sophisticated forms of risk intermediation and trading schemes; greater operating density and centralization through rapidly advancing automation and data management capabilities; and business consolidation through successive mergers and acquisitions. Large scale increases in concentrations of risk mean that changes in the risk profile of a financial institution can occur rapidly and dramatically with material loss implications.

However, such changes in risk profile do not necessarily trigger accounting events and there continues to be no adequate accounting solution as far as the new contagion of systemic risk is concerned. Funding gaps, credit risk concentrations and correlations, excessive trading positions, a severe recession, poor data, flawed financial models, the bypassing or overriding of internal controls... these are all examples of conditions or events that materially affect the risk position of an enterprise but do not necessarily translate into accounting events.

The evidence of the financial crisis is that life-threatening exposures to risk, that defied identification and quantification, were accumulating in financial institutions of all sizes. Lo[6] aptly summarized the situation:

> *"Before we can hope to reduce the risks of financial crisis, we must be able to define and measure those (systemic) risks explicitly. Therefore, a pre-requisite for effective financial regulatory reform is to develop dedicated infrastructure for defining, measuring, monitoring and investigating systemic risk on a standardized, on-going and regular basis".*

This represents both a risk quantification challenge and an accounting challenge. They are inextricably linked.

The Changed Risk Landscape

The risk landscape in banks and the global financial system as a whole has undergone dramatic change in little more than a generation: massive advances in technology created an operating dependency on globally interconnected electronic data and information networks; escalating business consolidations through successive mergers and acquisitions created the mega-bank and 'integration' risk; and increases in risk intermediation products such as the 'derivative', the 'synthetic' and the 'structured' product created 'complexity' risk.

Substantial concentrations of risk are now a permanent feature of banks whose operating environments are invariably comprised of highly complex risk management ecosystems within similarly complex information technology infrastructures. In these circumstances it is questionable whether audited financial statements prepared in conformity with IFRS or GAAP can adequately communicate a firm's financial position in a complete and comprehensive manner. This situation is due, in part, to accounting standards not considering the financial implications of the risks firms must accept in order to create shareholder value. This limits the value of audited financial statements for banks' stakeholders generally, and boards of directors and C-suite executives in particular who, in light of the changes in risk landscape described above, have become increasingly concerned with accumulating risks and their potential to trigger material unexpected losses.

In the recent past there have been numerous examples of corporate disasters and financial crises involving unexpected losses on a scale that severely impacted or even wiped out a firm's capital. It is not unrealistic, therefore, to suggest that unexpected losses caused by the lack of effective identification, quantification and reporting of accepted risks are potentially more devastating to a bank than accounting errors or financial reporting misstatements or deficiencies in internal controls that are the focus of independent public accountants' opinions included in published financial statements.

The lack of due consideration of accepted risks in accounting standards causes disclosures of financial position to be inherently favorable. Firms' management theoretically ameliorate the moral hazard

[6] Lo, AW. (2009), The Feasibility of Systemic Risk Measurement: Written Testimony for the House Financial Services Committee Hearing on Systemic Risk Regulation, available at SSRN: http://ssrn.com/abstract=1497682 (accessed 7th February 2016)

inherent in overly favorable reporting of financial condition by including voluminous narrative disclosures in annual reports on the status of a firm's risk management. However, the denseness and boilerplate formats that are a feature of such narrative disclosures mask the true level of accepted risks thereby increasing, rather than reducing moral hazard.

The Regulators' Position

It is often said that accountants are concerned with 'what is' and risk managers with 'what if'. Since the first capital accord 'Basel I'[7], the banks' global regulatory standards setting body, the Basel Committee, has focused on the 'what if' when determining the amount of regulatory capital banks should hold to buffer unexpected losses that may occur in extreme but plausible operating conditions. We can conclude from this that banks' audited financial statements have limited value for regulators as accounting standards generally assume normal, not extreme operating conditions.

Basel I introduced the concept of Risk Weighted Assets (RWAs) that were used in place of the fair values reported in accordance with IFRS and GAAP to calculate a bank's minimum regulatory capital requirement. The calculation mandated in Basel I involved applying fixed percentages to five predetermined categories of risk assets. This method received increasing criticism from across the industry due to its inherent lack of risk sensitivity.

This limitation was addressed in the second capital accord 'Basel II'[8] that also recognized the risk consequences of increases in market-priced assets in banks' balance sheets that occurred as a consequence of burgeoning trading book activities. Basel II permitted and even encouraged banks to apply advanced mathematics in the form of stochastic models in their calculation of RWAs. This allowed the larger, more sophisticated banks to use their inherently complex and non-standardized internal risk models to determine their regulatory capital requirement.

It is self-evident that, during the period leading up to the financial crisis, massive exposures to risk had accumulated in banks and in the global financial system. The stochastic techniques promoted in Basel II that were meant to identify and quantify such risks were found wanting. Similarly, published financial statements failed boards, CEOs, investors and other stakeholders due to accounting standards that were never intended to consider the likely financial consequences of accumulating risk concentrations. Published financial statements, with their inherently favorable accounting, provided the basis on which banks misguidedly approved dividends, discretionary bonuses and share buy-backs only to become, months later, the object of government bailouts, forced acquisitions and even liquidations.

[7] Basel Committee on Banking Supervision (1988), 'International convergence of capital measurement and capital standards', Bank for International Settlements, available at http://www.bis.org/publ/bcbs04a.pdf (accessed 7th February 2016)

[8] Basel Committee on Banking Supervision (2006), 'International convergence of capital measurement and capital standards', Bank for International Settlements, available at http://www.bis.org/publ/bcbs128.pdf, (accessed 7th February 2016)

Independent Assurance Services

In its discussion paper the Institute of Chartered Accountants in England and Wales (ICAEW)[9] responded to a request from the UK's Prudential Regulation Authority (PRA) to consider how assurance on bank capital ratios and risk-weighted assets might support confidence in these important measures. The paper reported on the results of discussions between the ICAEW, PRA, Financial Reporting Council (FRC), large accountancy firms and other relevant parties. It explained the importance of the confidence that banks and their stakeholders must have in the controls, processes and governance surrounding the production of capital ratios and related information and concluded that external assurance from auditors on these matters could contribute to achieving such confidence.

While the ICAEW refers to capital ratios and RWAs in general terms the discussion paper appears to place greater emphasis on credit risk as the primary focus of proposed assurance reports. This is evident through specific references to the internal ratings-based (IRB) approaches, which relates exclusively to credit risk, and the repeated use of the term "risk, credit and financial reporting systems". This focus on credit risk could potentially mask the true complexity of providing assurance as the management of credit risk is more straightforward than the other principal risk types. Whereas details of credit exposures can be obtained from accounting records, equivalent details relative to the other risk types are not so readily available. Further, lending has always been a core activity of banks whereas the emergence of material exposures to the other risk types is more recent.

The combination of a readily available and deeper history of credit information provides risk managers with a comprehensive and relatively reliable source of historic data that can be used in the quantitative modeling of credit risks. Indeed, some organizations have a century or more of such data points. The additional complexities connected with providing independent assurance on capital ratios and RWAs in relation to risk types that do not have the informational advantages of credit risk are not specifically addressed by the ICAEW in its discussion paper.

For example, in the case of market risk Basel II promoted the application of Value-at-Risk (VaR) methodologies to provide a common measurement framework for trading book exposures. The credit crisis of 2007/8 attracted regulatory focus on the suitability of VaR as a basis for determining capital adequacy leading to the Basel Committee declaring them inappropriate and even misleading for enterprise-wide risk considerations. In a consultative paper the Basel Committee[10] commented:

> *"Weaknesses include: its (VaR's) inability to adequately capture credit risk; its inability to capture market liquidity risk; the provision of incentives for banks to take on tail risk; and, in some circumstances, the inadequate capture of basis risk."*

[9] Institute of Chartered Accountants in England & Wales (2015), 'Reporting on regulatory capital: choices for assurance', available at http://www.icaew.com/~/media/corporate/files/technical/financial%20services/financial%20planning%20and%20advice/reporting%20on%20regulatory%20capital%20choice%20for%20assurance%20report.ashx (accessed 7th February 2016)

[10] Basel Committee on Banking Supervision (2012), 'Fundamental review of the trading book', Bank for International Settlements, available at http://www.bis.org/publ/bcbs219.pdf (accessed 7th February 2016)

New techniques, such as Expected Shortfall have been proposed that are still under review.

As previously commented, independent accountants' opinions on audited financial statements are not intended to consider the likely economic consequences of accepted risks should macroeconomic and other operating conditions change (see 'Accounting Standards and Risk' above). This omission can be substantially resolved through an assurance report on capital ratios and risk-weighted assets (RWAs). However, the authors believe that such independent assurance will be of limited value given the diversity and inherent complexity of internal models used by banks to calculate risk, notwithstanding the Basel Committee's publicly stated concerns as to the reliability of banks' internal models. Further, independent assurance reports typically focus on: mathematical and procedural accuracy; the appropriateness of inputs given the models' parameters; and whether outputs are consistent with generally accepted and documented standards. Less focus is placed on whether the models' outcomes are reflective of the accepted risks.

The authors argue that banks must first develop systems that systematically account for and report accepted risks following accounting-like disciplines which, in the main, is what BCBS 239 sets out to achieve. It follows that assurance reporting such as that proposed by the ICAEW should be aligned to the implementation of BCBS 239.

The implementation of independent reporting on risk measures, capital ratios or controls prior to achieving compliance with BCBS 239 will invariably lead to inconsistent assurance reporting. Accordingly, the identification and status of improvements necessary to achieve compliance with BCBS 239 should be a feature of early phases of assurance reporting on capital information and that such improvements should be in relation to a set of broadly accepted principles and standards applied to the control, quantification and reporting of risk. The authors believe that independent assurance providers should be instrumental in promoting such principles and standards and they offer Risk Accounting as one possible framework on which these may be constructed.

Current Approaches to Capital Calculations

The VaR standard for capital adequacy at the enterprise level was embedded in Basel II and was initially viewed and widely adopted as a best practice method of blending diverse trading exposures within a common metric to enable more effective oversight of these activities. However, when applied in the determination of minimum capital requirements at the enterprise level it reveals a number of limitations. In its original conceptualization, VaR was not intended to represent a 'maximum loss figure'. Indeed, VaR may be exceeded, potentially on continuous days, a feature that causes it to be inherently flawed when used in the determination of minimum capital requirements. This shortcoming was accepted by regulators as discussed in the section 'Independent Assurance Services' above. The authors question whether regulatory aims can be successfully achieved by building upon an evidently flawed and overly complex capital adequacy regime in an incremental way.

This view found endorsement from Haldane and Madouras[11] who questioned the role that risk models, such as VaR, play in modern regulation. Haldane commented:

[11] Haldane, A. and Madouras, V. (2012), 'The dog and the Frisbee', the Bank of England, available at http://www.bis.org/review/r120905a.pdf (accessed 7th February 2016)

> *"The quest for risk-sensitivity in the Basel framework, while sensible in principle, has generated problems in practice. It has spawned startling degrees of complexity and an over-reliance on probably unreliable models... With thousands of parameters calibrated from short samples, these models are unlikely to be robust for many decades, perhaps centuries to come. It is close to impossible to tell whether results from them are prudent".*

In a 2013 discussion paper[12] the Basel Committee observed that:

> *"...banks are likely to employ a large number (possibly hundreds) of models to determine their consolidated capital requirements which are, in turn, based on a very large number of inputs estimated using complex quantitative techniques".*

Haldane further cautioned that due to escalating complexity:

> *"…the Tower of Basel is at risk of over-fitting – and over-balancing. It may be time to rethink its architecture".*

The conclusion was that simpler, more judgment-based approaches to regulation should be considered.

Operational Risk

The Basel Committee[13] wrote:

> *"Reflecting the different nature of operational risk, for the purposes of this paper, management of operational risk is taken to mean the 'identification, assessment, monitoring and control / mitigation' of risk. This definition contrasts with the one used by the Committee in previous risk management papers of the 'identification, measurement, monitoring and control' of risk".*

Note the reference to operational risk as being 'different' and the transformation of the word 'measurement' into 'assessment'. The inference is that an exposure to operational risk can only be assessed… it can't be measured. This position from the global regulatory standards setter effectively removed the obligation from banks to seek quantitative methods of managing this particular risk type which continues to be the situation today.

In the absence of a generally accepted method of explicitly quantifying exposures to operational risk banks have universally adopted assessment based risk management techniques such as Key Risk Indicators (KRIs) and Risk & Control Self-Assessment (RCSA). The most common metric financial firms use to report the existence and likely impact of operational risks is through a system of three colours:

---

[12] Basel Committee on Banking Supervision (2013), 'The regulatory framework: balancing risk sensitivity, simplicity and comparability', available at http://www.bis.org/publ/bcbs258.pdf (accessed 7th February 2016)

[13] Basel Committee on Banking Supervision (2003), 'Sound practices for the management and supervision of operational risk', Bank for International Settlements, available at https://www.bis.org/publ/bcbs96.pdf (accessed 7th February 2016)

red, amber and green. Whereas assessment based metrics can provide a vital source of risk intelligence at the operating unit level, they are inherently subjective and are not aggregatable or comparable along the vertical and horizontal dimensions of an enterprise.

In 2004 the Basel Committee published its second capital accord 'Basel II' which included, for the first time, the requirement for banks to set aside protective capital for operational risks. In paragraph 665 it states:

> *"…a bank's internal measurement system (Advanced Measurement Approach – AMA) must reasonably estimate unexpected losses based on the combined use of internal and relevant external loss data, scenario analysis and bank-specific business environment and internal control factors (BEICFs)".*

Noteworthy is the lack of reference to a bank's quantified operational risk exposures as an input to the internal measurement system; instead, banks are directed to use a proxy in the form of assessment data derived from scenario analyses and BEICFs.

This imposes limitations on the usefulness of outputs from the advanced approaches as described by Currie[14] who comments:

> *"In operational risk modelling the portfolio of risks is not available with any reasonable degree of certainty by any direct means… (this) explains the weakness in proposed approaches to measuring operational risk that rely mainly on loss experience to infer a loss distribution. In essence, these quantification approaches effectively try to imply the 'portfolio' of possible operational risk loss events from historic loss events. Imagine taking this approach to credit risk modelling that is, 'deducing' the loan portfolio from historic defaults".*

Operational risk exposure fluctuates on a daily basis, often dramatically, as a consequence of changes in transaction volumes, implementations of new technology, failures of existing technology, business reorganisations, staff absences, new products… the list is almost endless. There are also hidden exposures related to, for example, fraud and control breakdowns. In the case of fraud, it can take several years before they are detected and their scale understood, and many more years of intense investigation before the true amount of loss can be determined and recorded in financial statements and loss event databases. Similarly, when control breakdowns occur it is impossible to know what their financial impact is until detailed investigations are undertaken. This is understandable given that a control breakdown invariably results in accounting records and documentation being unreliable.

The combination of fluctuations in daily operational risk exposures and the hidden exposures that are present in most financial transaction processing environments makes it questionable whether, in the absence of real-time or near real-time direct measurements of exposure to risk, a meaningful statistical conclusion on the size and distribution of current operational exposures can be made. In

[14] Currie, C. (2005), ' A Test of the Strategic Effect of Basel II Operational Risk Requirements on Banks', University of Technology, Sydney Working Paper No. 143, available at SSRN: http://ssrn.com/abstract=831304 (accessed 7th February 2016)

these circumstances, the creation of such a direct exposure measurement framework, such as that proposed in the Risk Accounting method, becomes an imperative.

Some years following the publication of Basel II the Basel Committee[15] publicly voiced its own concerns with the limitations of the AMA through its observation that the:

> *"…range of practice continues to be broad, with a diversity of modeling approaches being adopted by AMA banks... (this) clearly affects the AMA methodology of individual banks and, ultimately, the amount of capital resulting from the application of the AMA… While flexibility allows modeling to reflect individual bank risk profiles, it also raises the possibility that banks with similar risk profiles could hold different levels of capital under the AMA if they rely on substantially different modeling approaches and assumptions".*

More recently, the Basel Committee has advised its intention to remove the AMA from the regulatory framework. In an interview reported by Risk.Net[16] the General Secretary of the Basel Committee, Bill Coen, was quoted:

> *"There are always two sides of a debate. But when it comes to the advanced measurement approaches for operational risk, the views largely converge in the same direction - that the AMA has not worked as intended… When we consult by the end of the year on a revised standardized approach, I expect we will also propose removing the advanced modelled approach from the regulatory framework."*

Banks have not yet achieved a meaningful calibration of operational risk capital nor has there been a comprehensive debate on how to measure operational risk. Specifically, a primary reason for failing to arrive at a reasonably useful measure is that the fundamental nature of the measurement unit (or units) applied to operational risk has not been defined. For all practical purposes, the measurement of operational risk has been deferred 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 model for calculating the minimum capital requirement in accordance with the Basel soundness standard, that is, 99.9% confidence interval over a one year horizon.

The mapping of loss events into business lines and event types is a well-established procedure in most, if not all internationally active financial institutions that have been approved for the adoption of the AMA. Nevertheless, missing from the typical mapping are the causal events at a sufficient level of

[15] Basel Committee on Banking Supervision (2011), 'Operational risk – supervisory guidelines for the advanced measurement approaches', Bank for International Settlements, available at http://www.bis.org/publ/bcbs196.pdf (accessed 7th February 2016)

[16] Risk.Net magazine (2015), 'Basel Committee to consult on scrapping op risk modeling', available at http://www.risk.net/operational-risk-and-regulation/news/2429034/basel-committee-to-consult-on-scrapping-op-risk-modelling (accessed 7th February 2016)

granularity that resulted in the losses. This failure makes it more difficult to observe risk exposure and perform risk mitigation.

A first step to calculating a risk based operational capital charge is to understand the causal events and quantifying the exposure to risk inherent in the operations associated with those events. This can only be achieved in a meaningful way if a common risk exposure measurement framework is applied that produces meaningful, relevant, consistent and comparable results. In the rush to satisfy the regulators' well intentioned interest in calculating operational risk capital, banks have failed to develop such a framework.

As long as banks use non-additive assessment metrics to manage and report exposures to operational risk they will not be able to comply with the risk data aggregation requirements of BCBS 239. Neither will they be able to implement meaningful, quantifiable risk appetite frameworks. This in turn puts the creation of effective ERM systems and governance frameworks beyond their reach thereby limiting their ability to positively impact risk culture.

Resolving this conundrum can be accomplished through the production of standardized and real-time or near real-time direct measurements of exposure to enterprise risks, including operational risk. The authors offer a possible solution 'Risk Accounting' as a method of achieving the direct measurement of exposures to operational risk.

Risk Data Aggregation

In 2013 the Basel Committee issued BCBS 239 that requires global systemically important banks (GSIBs) to be in compliance with the 11 principles set out in the paper by January 2016.

In December 2015 the Basel Committee published the results of a survey on progress toward BCBS 239 objectives which concluded that banks still fall short of full compliance and additional work must be done to meet the intent of the principles. The report included a comparison of progress made since the previous report issued in December 2014 and reported that, based on banks' self-assessments of their progress, 14 of the total 30 G-SIBs will not fully comply with at least one of the 11 principles by the deadline; expected completion dates for full compliance with all 11 principles ranged from sometime in 2016 to as far out as 2018.

The principal areas of concern relate to principle 2 (data architecture and IT infrastructure) that has the lowest average compliance rating indicating that this was a critical area in need of improvement. Banks referenced the complexity of large-scale, ongoing, multi-year IT infrastructure projects and other data-related projects, as the primary cause of delays relative to the deadline.

The Basel Committee also noted that principle 3 (accuracy/integrity) and principle 6 (risk data aggregation adaptability) had some of the lowest reported compliance ratings. In the 2014 self-assessments, 8 G-SIBs noted that they would not be compliant at the implementation deadline, twice the number of banks that indicated this in 2013. Moreover, in 2014, half the banks rated themselves as materially non-compliant. This is most notable in the areas of unifying and rationalising the dictionaries and taxonomies of their risk data repositories as well as establishing clear risk data ownership and responsibilities over the attendant quality controls.

The authors consider the above status reported by the banks via their self-assessments and summarized by the Basel Committee in its progress report as overly favourable in regard to compliance for two primary reasons:

First, there is an element of incongruity between the projected full compliance with the 11 principles by all 30 G-SIBs by 2018 and the survey of these same G-SIBs conducted by EY that reported "...an overwhelming 93% of GSIBs agree that weak oversight and controls led to the (numerous regulatory and misconduct) failures" (see 'Risk Culture – An Industry View' below). A precondition of meaningful risk data aggregation is the implementation of effective risk data controls and governance which, in turn, requires the adoption of standardized identification systems and a common risk measurement framework. These aspects are discussed in more detail in the 'Introduction' to this paper and in Part 2.

Second is the absence of a method of quantifying exposures to operational risk that constitute a major component of the risk profile of any financial institution. Banks cannot claim to have satisfied the risk data aggregation requirements of BCBS 239 if they have not devised a method of dynamically and explicitly quantifying their operational risks. This is discussed in the section 'Operational Risk' above.

In an article Grody and Hughes[17] explained how the Risk Accounting method and system, the object of this paper, can provide greater certainty of achieving compliance with BCBS 239. They state this is achievable through the adaptation of existing accounting and control frameworks that rely on proven and trusted sources of accounting data and the creation of a standardized unit of risk quantification, the 'RU'. In their article they concluded:

> *"Banks, over time, will need to invest in upgrading their IT and data architectures where there are ongoing dependencies on legacy systems, but these are business investment decisions that should follow business priorities. The successful implementation of BCBS 239 is too critical to be dependent on prior reconfigurations of IT and data architectures that may take many years to achieve. Banks and regulators must quickly resolve the downside risks associated with banks' present inability to completely and accurately, in timely fashion, report the risks they accept in the creation of shareholder value. Risk Accounting can potentially provide a viable solution at a fraction of the time and cost of reconfiguring entire IT and data infrastructures by adapting the control and reporting frameworks that already exist in accounting and general ledger systems".*

Risk and Culture – An Industry View

From a 2014 risk management survey conducted by EY it was evident that banks still have much work to do if their risk control systems are to achieve the required degree of effectiveness. In their report, EY commented that:

[17] Grody, AD. and Hughes. PJ. (2014), 'BCBS 239: is spending $8 billion on IT the answer?', GARP Magazine, available at https://www.garp.org/#!/risk_intelligence_detail/a1Z40000002vHzkEAE (accessed 7th February 2016)

> *"This sharpened focus (on risk culture) is the result of numerous regulatory breaches and misconduct issues, such as LIBOR and product missellings, that have shocked the industry over the past several years. These problems have shaken boards' certainty about prevailing enterprise risk culture. An overwhelming 93% of GSIBs agree that weak oversight and controls led to the failures."*

The Group of Thirty (G30)[18], a private sector thought leadership group, reported on a comprehensive survey conducted through hundreds of interviews with global bank executives, audit executives, board members, and regulators. It discusses at many points in the paper the need for proper metrics for conduct and risk culture and refers to a balanced scorecard as the means to measure such risk.

The G30 report defines the need for cultural indexes and performance metrics that have so far proved elusive. The report states:

> *"The Banks are searching for metrics to assist in monitoring and understanding cultural progress over time, and while a broad range of metrics has been adopted, most banks are still experimenting and have neither found a definitive set of indicators nor concluded what those metrics should be."*

In a cited bank case study described in the report it was stated that:

> *"The bank recognizes the importance of ongoing measurement, and continues to work on metrics and management tools as it seeks to develop an 'alert mechanism' that can warn when an individual is straying from the values and behaviors defined, and identify the areas in the bank where its values and code of conduct are not effectively implemented."*

In these circumstances, the feasibility of designing and implementing effective assurance programs to promote confidence in banks' calculations of regulatory capital and capital ratios is questionable given the already widespread acceptance of the immaturity and frailty of risk controls, the absence of the proper metrics to monitor conduct and culture risk, and the unreliability of aggregated risk reporting.

Risk Accounting and Control

The lack of confidence in banks' ability to accurately report risk information, such as capital ratios and risk-weighted assets (RWAs), can be attributed to the emergence of a highly complex risk management ecosystem and an absence of an appropriately dimensioned risk accounting and control system. As discussed in the section 'Independent Assurance Services' above, whereas assurance programs may provide partial or limited assurance in the short term, banks must seek longer term solutions. It would appear that the design and adoption of a framework of effective accounting and control to govern and oversee accepted risks is an imperative.

[18] The Group of 30 (2015), 'Banking conduct and culture: a call for sustained and comprehensive reform', available at http://group30.org/images/uploads/publications/G30_BankingConductandCulture.pdf (accessed 7th February 2016)

Precedents for such a framework already exist; they can be found in the financial accounting and control systems of banks that comprise:

- the general ledger as the single source of aggregated financial information that provides the foundation on which firms' financial statements are prepared;
- systems of internal control that provide assurance that transactions accepted for processing are properly authorized and are processed in a complete, accurate and timely manner thereby ensuring that official accounting books and records are reliable;
- the verification of accounting information through the reconciliation of general ledger balances with associated sub-ledgers and product systems;
- the proofing and substantiation of the composition of individual ledger balances by reference to documentary evidence and, where applicable, through physical inventory taking; and
- the validation of the resulting data through independent (internal and external) trusted auditing functions.

Part 2 of this paper will describe how the above framework applied to accounting data, which has evolved over generations, can now be adapted for risk data.

Capital-at-Risk vs. Firm-at-Risk

Requiring banks to enhance the quality and quantity of their capital and liquidity reserves is one method of ensuring a more robust and secure financial system but it is only a part of the solution.

Regulators' short-term response to the global financial crisis was to require banks to hold more capital with the aim of increasing their capacity to buffer unexpected losses. They also introduced mechanisms to counter model risk and measurement error in capital adequacy calculations through devices such as the leverage ratio. Their longer-term response addresses the root of the problem by placing emphasis on the creation of more robust risk management frameworks and technology infrastructures. Five such frameworks are worthy of particular mention:

Basel Committee on Banking Supervision (BCBS):

1. Principles for effective risk data aggregation and risk reporting (BCBS 239)
2. Regulatory framework for balancing risk sensitivity, simplicity and comparability (BCBS 258)

Financial Stability Board (FSB):

3. Principles for an effective risk appetite framework[19]
4. Guidance on supervisory interaction with financial institutions on risk culture[20]

[19] Financial Stability Board (2013), 'Principles for an effective risk appetite framework', available at http://www.fsb.org/wp-content/uploads/r_130717.pdf?page_moved=1 (accessed 7th February 2016)

[20] Financial Stability Board, 'Guidance on supervisory interaction with financial institutions on risk culture', available at http://www.fsb.org/wp-content/uploads/140407.pdf (accessed 7th February 2016)

5. A global legal entity identifier for financial markets[21]

The above five initiatives are interdependent: an effective risk appetite framework is dependent on a bank's ability to aggregate risk data... the ability to aggregate data is dependent on defining participants in transactions consistently through common identification standards... the development of a positive risk culture is dependent on the implementation of an effective risk appetite framework... and none of this will be possible if we do not achieve a greater degree of simplicity and comparability in the regulatory framework.

More specifically: the long missing standard identification scheme for financial market participants and the products they trade, own and process, now taken up by the FSB, will permit data aggregation across business silos for enterprise-wide risk and across financial institutions for systemic risk analysis; the call in BCBS 239 to reconcile risk data with accounting data will provide a single authoritative source of risk data; regulators' aspirations for greater simplicity in risk measures will provide incentives to build risk systems so that risk can be mitigated at the operating level, rather than an exclusive focus on managing the depletion of capital; and finally, it will all lead to quantifying risk appetite and providing objective measures of risk culture to sit side-by-side with Boards' and regulators' judgments. This will enable Boards to refocus management's priority on observing and proactively managing and mitigating risk exposures before they become losses.

These five mandates are highlighted as they provide the cornerstone for a future 'firm-at risk' enterprise risk management (ERM) framework. Their implementation by industry members will be a proactive response to the financial crisis and its aftermath, not a reactive one where more capital is simply used to count down to failure.

The Risk Accounting Method and System

Regulators and other stakeholders still await the emergence of true ERM systems in banks. The Basel Committee has taken the first step by setting the parameters for such systems in BCBS 239. In Part 2 of this paper 'Risk Accounting' will be described that offers a common measurement framework for all forms of risk and a common risk metric, the 'Risk Unit' or RU.

To date banks have viewed BCBS 239 as, primarily, a data quality challenge. This is, without question, a major challenge for most banks and, over time, banks will need to invest in upgrading their IT and data architectures particularly where there are ongoing dependencies on legacy systems. While these are business investment decisions that should follow business priorities the successful implementation of BCBS 239 is too critical to be dependent on the reengineering of bank-wide IT and data architectures which may take many years and at great cost to achieve.

Notwithstanding the need to reengineer their IT and data infrastructures, banks must quickly resolve the downside risks associated with their present inability to identify, quantify and report the risks they accept in a complete, accurate, consistent and timely manner. The authors argue that Risk Accounting can potentially provide a viable solution at a fraction of the time and cost of reconfiguring entire IT

[21] Financial Stability Board (2012), 'A global legal entity identifier for financial markets', available at http://www.fsb.org/wp-content/uploads/r_120608.pdf (accessed 7th February 2016)

and data infrastructures by adapting the control and reporting frameworks that already exist in accounting and general ledger systems. However, this is dependent on banks' and regulators' acceptance that it is indeed possible to define and implement a common risk metric that can be applied to all forms of risk. This constitutes both a risk management and an accounting challenge for banks.

Part 2

Risk Accounting – An Overview

Note: The Risk Accounting method does not use the term 'Operational Risk' as it is too generic and imprecise. In preference, the term 'Processing Risk' is used; exposure to processing risk exists in all business components that are engaged in the capture, processing, control, accounting and reporting of transactions.

Introduction

Hughes et al[22] describe Risk Accounting as an extension of management accounting. Risk Accounting comprises a new risk quantification technique, described in the paragraphs that follow, now replicated in software that produces explicit, dynamic and aggregatable measurements of an enterprise's exposure to risk by primary risk type: processing, credit, market, liquidity, interest rate and conduct. Risk Accounting's calculations of exposure to risk supplement the backward leaning stochastic techniques adopted under Basel II to determine minimum capital requirements and the risk management techniques developed by financial firms for the day-to-day management of risk at the more granular operating level.

The Monovalent Concept

The current state of accounting systems in the provision of risk oversight and governance is succinctly summarized in, of all places, a Wikipedia entry[23]':

> *"As of now, no specialized comprehensive accounting system for the purpose of representing risk, organization wide, in comparable terms has evolved."*

In Part 1 of this paper the authors explained the need for financial firms to adapt extant financial accounting and control systems to encompass accepted risks. The urgency and scale of the challenge demands the combined endeavor of both accountants and risk professionals; for far too long they have been working independently of each other with respect to the design of integrated finance and risk control frameworks, hence the lack of progress.

Returning to the 'Managerial Risk Accounting' entry in Wikipedia there is another revealing passage:

> *"Existing accounting systems are primarily 'monovalent'. That is, a single accounting value is attributed to a specific object or purpose. In contrast, risk and uncertainty are formally characterized by a whole range of possible values connected to an object."*

---

[22] Fernandes, KJ. and Grody, AD. and Hughes, PJ. and Phillips, O and Toms, JS (2013) 'Risk Accounting: An Accounting Based Approach to Measuring Enterprise Risk and Risk Appetite', available at SSRN: http://ssrn.com/abstract=2165034 (accessed 7th February 2016)

[23] Wikipedia, 'Managerial risk accounting', available at https://en.wikipedia.org/wiki/Managerial_risk_accounting (accessed 7th February 2016)

As is the case for risk, there is more than one value that can be assigned to a transaction for accounting purposes such as historic cost, fair value and net present value. Accountants learned a long time ago that financial accounting and control systems must be constructed around a common metric embodying a single and universally accepted accounting value assigned to each transaction. This is the 'monovalent' accounting system referred to above and defined in accounting standards such as IFRS and GAAP.

Only through a monovalent system is it possible to: embed controls in financial operating infrastructures (reconciliations, substantiations etc.); effectively aggregate accounting data; achieve direct comparability of outputs from accounting systems; create single authoritative sources of accounting data; and create firm-wide operating limits (the financial equivalent of 'risk limits') and budgets (the financial equivalent of 'risk appetite').

This monovalent concept must now be applied to 'risk adjusting' these same accounting transactions to embody a single and universal risk-adjusted value denominated in a common risk metric for all forms of risk. This should be the focus of regulators' and academics' ongoing research; to design and test the viability of a common risk metric for all forms of risk that can be applied in a system of risk accounting and control.

The Risk Unit (RU)

Accounting involves the posting of all transactions upon their approval in accounting systems. As already described above, transactions are tagged with codes upon acceptance to ensure that accounting data follows predefined aggregation paths. From these codes tagged onto transactions, accounting data can be aggregated to provide financial performance and profitability reports by, for example, business line, organizational unit, customer, product, legal entity and location. Transaction values in conformity with accounting standards such as IFRS and GAAP are also assigned to each transaction that include historic cost, notional values, net present values and mark-to-market values.

The tagging of transactions with identification codes and standardized values has enabled effective systems of control over data aggregation and reporting to evolve. When a different cut of accounting data is required, for example, to construct product profitability, aggregated transaction values function as population controls to ensure that the data used to compile the report is complete and accurate. Almost by instinct, accountants embed control totals based on transaction values throughout their reporting processes to ensure they are complete and accurate. Accounting data can be verified by tying it back to its single authoritative source - the general ledger - and, in turn, to its sub-ledgers and product processing systems.

The hypothesis for Risk Accounting is that transactions tagged with information that can be used in a standardized, monovalent calculation of each transaction's exposure to risk enables the same control systems, trusted data sources and aggregation paths that already exist for accounting data to be applied to risk data. This resolves a number of BCBS 239 requirements relating to the accuracy and single authoritative sources of risk data and the precision, timeliness, comprehensiveness and adaptability of risk reporting.

A universal measurement system needs a common, standardized unit of measurement and natural currency is not a good standard unit of risk measurement for the following reasons:

1. There are many currencies and their values relative to each other are constantly changing
2. The quantification of exposures to risk in monetary terms usually involves the application of stochastic techniques that are difficult to standardize, are invariably complex and inherently backward looking
3. Exposures to non-financial risks, e.g. operational risk, cannot be validly expressed in monetary terms

To address these issues a common, additive and standardized unit of risk exposure is used in Risk Accounting called the 'Risk Unit' or 'RU'. Through the application of RUs, financial firms can validly aggregate risk data to report the risks they accept absolutely and in comparison to others.

When first applied, as with any risk measurement system, the calculation of RUs in Risk Accounting will rely on subjective inputs but these will become progressively more objective and, consequently, more precise over time. Given the RU is an additive metric, that is, it combines quantitative and qualitative properties, the statistical correlation of actual operating losses with associated residual risks in RUs is enabled which, as shown in Figure 1, will identify refinements that will need to be made to the exposure measurement system in Risk Accounting. Such statistical techniques are not available for the exclusively assessment based and inherently subjective risk management techniques widely in use today, such as Risk & Control Self-Assessment (RCSA) and Key Risk Indicators (KRIs) discussed in Part 1 of this paper in the section 'Operational Risk', that are reported using an assessment-based metric such as 'RAG' (red/amber/green).

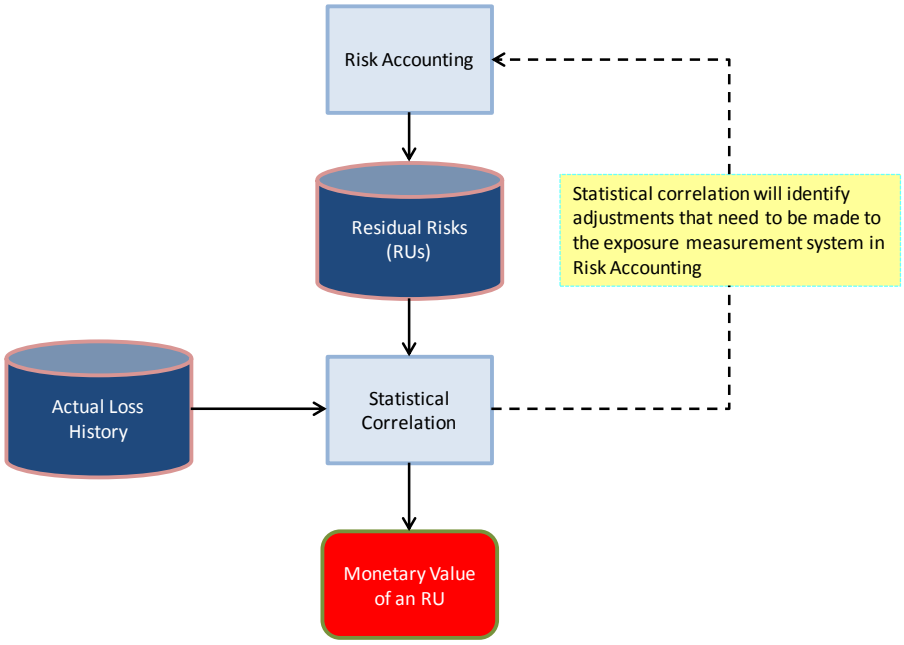

Figure 1 – Deriving a Monetary Value for an RU

RCSA and KRI techniques require subjective inputs at high impact level, for example, choosing which KRIs to correlate with which product or process risk or choosing the magnitude of potential losses at a departmental level for a 1 in 1,000 year event (the Basel soundness standard - 99.9% confidence

level). Risk Accounting also requires subjective inputs but at the more granular process level relative to a particular product or activity, thus mitigating the impact that any one flawed subjective input can potentially have on the overall result.

The adoption of a non-financial metric in universal accounting and reporting systems will challenge the sensibilities of many. However, an abstract unit of measure that becomes a monetized equivalent over time as an increasingly robust set of data points evolves is a fundamental principle of risk management. This is found in the Fair Isaac Corporation's 'FICO scores' for retail credit measurement which is the best-known and most widely used retail credit scoring methodology in the US. The same concepts are applied in credit ratings by credit agencies such as Fitch, Moody's and S&P for determining institutional default probability. Such measurement techniques are already established best practices and can similarly be deployed for the newly created 'RU' as a tool for both enterprise risk management and risk appetite measurement.

The predictability of a FICO score in determining the probability of loss in a credit card or mortgage portfolio and the credit rating migration of a reference entity in determining the probability of default of a credit default swap parallels the change in residual risk measured in RUs. Over time, as RUs are tabulated and aggregated, their intrinsic value in benchmarking both within and across firms will also become statistically correlated with actual monetary loss histories and Risk Accounting's performance measures. Thus, as demonstrated in Figure 1, the RU will obtain monetary and predictive attributes as is the case with FICO scores, credit ratings, scaled indices, rankings, temperature scales and other correlated measurement systems.

Three Core Metrics

Risk Accounting involves the tagging of transactions with risk information that is used in a calculation of each transaction's exposure to risk. Three core metrics are produced that are tagged onto each transaction and for each risk type triggered:

Inherent Risk
Expressed in RUs, the risk-weighted size of a transaction that represents its maximum possible loss

Risk Mitigation Index (RMI)
A dynamic measure on a scale of 1 to 100, where 100 is consensus agreed best practice, that represents, in percentage terms, the portion of inherent risk (expressed in RUs) that is mitigated through the effective management and control of the firm's operating environment

Residual Risk
Expressed in RUs, the portion of a transaction's inherent risk (also expressed in RUs) not covered by effective risk mitigation - represented by the RMI – that represents its probability of loss

The concept of inherent and residual risks is widely used in risk management. COSO[24] defines inherent risk as the risk to an entity in the absence of any actions management might take to alter either the risk's likelihood or impact; residual risk is the risk remaining after management's response to the risk. However, COSO applies this concept in a risk assessment rather than a risk measurement context. McKinsey & Co[25] comments that rarely is the residual risk measured and reported in a systematic manner that gives executives a clear picture of where the 'hot spots' are and, as a result, major risks might go unaddressed. It is precisely such systematic measurement of risk, including residual risk, that Risk Accounting is designed to produce.

It can be argued that a reasonable estimate of 'maximum possible loss' can only be achieved through the application of complex quantitative modeling techniques. This is undoubtedly the case when using stochastic techniques to determine the likely probability and severity of future events by statistically associating multiple datasets, for example, loss history with current exposures.

In principle, accounting involves the identification, coding and recording in accounting systems of the properties of the entire population of transactions accepted by an enterprise. The authors argue that the identification of all the risks triggered by all recorded transactions and applying heuristic techniques to risk-weight those transactions according to the observed risk characteristics of products is a valid approach to determining 'inherent risk'. PwC[26] observes that 'inherent risk' and 'maximum possible loss' are synonymous.

The heuristics that underpin the probability component of the RU are not intended to displace the probability estimates derived from the stochastic methods used by risk managers. Rather, both estimation techniques complement each other. The RU consistently applied in the quantification of all key risk types can, unlike multiple stochastic models, be validly aggregated across the vertical and horizontal dimensions of the enterprise.

A detailed description of the method of calculating the three core metrics is provided in the section 'The Risk Accounting Method' below which includes a sample scorecard in Figure 15 that provides an example of the practical application of the calculations.

The tagging of transactions with information to control data aggregation and management reporting is not new. In the recent past, internationally active business enterprises migrated from legal entity

---

[24] Deloitte & Touche (2012), 'Risk assessment in practice', COSO, available at http://www.coso.org/documents/COSOAnncsOnlineSurvy2GainInpt4Updt2IntrnlCntrlIntgratdFrmwrk%20-%20for%20merge_files/COSO-ERM%20Risk%20Assessment%20inPractice%20Thought%20Paper%20OCtober%202012.pdf (accessed 7th February 2016)

[25] McKinsey & Co (2014), 'Retail banking insights: Creating a robust risk-and-control framework in mortgage lending and servicing', available at http://www.mckinsey.com/~/media/McKinsey/dotcom/client_service/Financial%20Services/Latest%20thinking/Consumer%20and%20small%20business%20banking/Risk_and_control_framework_in_mortgage_lending_and_servicing.ashx (accessed 7th February 2016)

[26] PwC (2012), 'Governance of risk', PricewaterhouseCoopers, available at https://www.pwc.co.za/en/assets/pdf/governance-of-risk.pdf (accessed 7th February 2016). PwC in their paper comments: "The risk exposure before control or maximum possible loss should be evaluated to determine the extent that existing mitigation/control is managing the risk; this is often referred to as inherent risk."

based business organizations to global lines of business. To meet the demand for new performance reporting requirements that emerged as a consequence of such organizational changes, accountants devised management accounting solutions. These solutions involved tagging transactions with management coding that prescribed the aggregation paths for accounting data. This, in turn, enabled the reporting of profitability by various categories such as business line, product, customer and location.

There are two fundamental requirements for effective data aggregation:

- First is standardised identification systems[27], that is, the systems of coding that are used to identify data. If data is to be aggregated that is spread across multiple systems in multiple locations each item of data needs to be tagged with standardised identification codes so computers know which hierarchical aggregation paths the data should follow. Accounting systems already comprise standardised coding to enable aggregation by, for example, general ledger account, legal entity, business line, organizational unit, product, customer and location.
- Second is a standardised risk exposure quantification method. Data cannot be validly aggregated if the quantitative values assigned to them are the product of different measurement methods. For example, miles and kilometres are measurement systems applied to the same object... distance. It is self-evident that the aggregation of miles and kilometres will not produce a meaningful result.

Many different methods are typically used by financial firms and their regulators to identify, quantify and report exposure to risk. A sample of these methods is provided below:

Basel Advanced Approaches:
- Credit - Internal Ratings Based
- Market - Internal Model Method
- Operational – Advanced Measurement Approach

Basel Standardized Approaches:
- Credit – External Ratings Based
- Market – Mixed
- Operational – Gross Income Based

Bank Internal:
- Credit – Credit Analysis / Risk Rating / Credit Scoring
- Market – The 'Greeks'
- Operational – 'RAG' (Red/Amber/Green) Assessments – RCSA / KRIs

***Note**: A number of the above Basel advanced and standardized approaches are under revision by the Basel Committee.*

Each one of the above methods produces outputs that could be termed 'risk data'. They are all vital for ensuring that risks are properly managed at the granular level; but they cannot be validly

[27] Grody, AD. and Hughes, PJ. (2015), 'Risk, Data and the Barcodes of Finance', available at SSRN: http://ssrn.com/abstract=2544356 (accessed 7th February 2016). In their research working paper Grody & Hughes describe and analyze the current state of the design and implementation of global identification standards and systems.

aggregated by simply adding them together because the methods used to produce the outputs are different.

There is a particular issue with the bank internal methods shown above because they are assessment and not measurement based. For example, in the case of operational risk banks typically use 'RAG' assessments where exposures to risk are identified and the likely impact of operational failure is assessed by using a system of 3 colours: 'Red/Amber/Green'. Stating the obvious, colours cannot be consolidated and aggregated and yet colour coded assessments is the technique that is universally used by financial firms to manage their operational risks through tools such as risk and control self-assessment (RCSA) and key risk indicators (KRIs).

The Risk Accounting Method

The Calculation of Inherent Risk

Risk Accounting calculates the amount of inherent risk in RUs based on two factors: (1) Value Band Weightings (VBWs) and, (2) Exposure Uncertainty Factors (EUFs). An overview is provided in Figure 2.

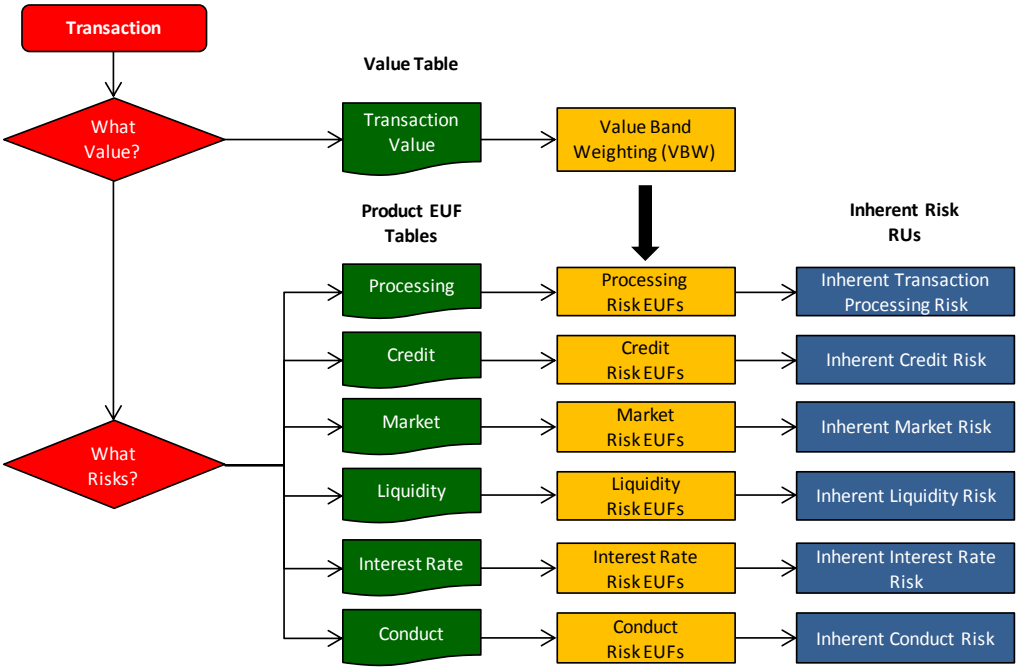

Figure 2 – Calculation of Inherent Risk in RUs

Transaction values are aggregated by product using proven and trusted accounting values as determined by accounting standards such as IFRS and GAAP and the bank's standard chart of accounts (SCA). The result is general ledger account balances and account movements aligned to products. Product totals are mapped to the Value Table, which is described in more detail in the section 'Value Table' below, and the applicable Value Band Weightings are extracted.

The risk characteristics of the product to which the transaction relates are then mapped to Product EUF Tables, which are described in more detail in the section 'Product Exposure Uncertainty Factor

(EUF) Tables' below, and the applicable EUFs are identified, accumulated and assigned to the transaction.

The inherent risk in RUs is the product of multiplying the applicable VBW with the cumulative EUFs.

The Value Table

A basic assumption in Risk Accounting is that there is a positive correlation between exposure to transaction processing risk and the total value of transactions accepted for processing. In other words, if transaction processing is faulty the likely amount of unexpected loss will be a direct consequence of the transaction values accepted for processing. It follows that they should be a factor in the calculation of inherent processing risk. Transaction values are incorporated into the calculation through the Value Table shown in Figure 3 that comprises value bands and associated risk-weights referred to as Value Band Weightings (VBWs).

Band	Value Bands (US$)			Value Band Weighting (VBW)	Change in Risk
1	Zero	to	62,500	**2.0**	
2	62,500	to	125,000	**2.6**	11.20
3	125,000	to	250,000	**3.4**	7.35
4	250,000	to	500,000	**4.3**	4.80
5	500,000	to	1,000,000	**5.5**	3.11
6	1,000,000	to	2,000,000	**7.1**	2.01
7	2,000,000	to	4,000,000	**8.9**	1.29
8	4,000,000	to	8,000,000	**11.3**	0.83
9	8,000,000	to	16,000,000	**14.1**	0.53
10	16,000,000	to	32,000,000	**17.6**	0.33
11	32,000,000	to	64,000,000	**21.9**	0.21
12	64,000,000	to	128,000,000	**27.0**	0.13
13	128,000,000	to	256,000,000	**33.1**	0.08
14	256,000,000	to	512,000,000	**40.4**	0.05
15	512,000,000	to	1,024,000,000	**49.1**	0.03
16	1,024,000,000	to	2,048,000,000	**59.3**	0.02
17	2,048,000,000	to	4,096,000,000	**71.2**	0.01
18	4,096,000,000	to	8,192,000,000	**85.0**	0.01
19	8,192,000,000	to	16,384,000,000	**101.0**	0.00
20	16,384,000,000	to	32,768,000,000	**119.3**	0.00
21	32,768,000,000	to	65,536,000,000	**140.1**	0.00
22	65,536,000,000	to	131,072,000,000	**163.6**	0.00

Figure 3 – The Value Table – Value Band Weightings

It can be observed from Figure 3 that the value band ranges increase at a faster rate than the value band weightings. This depicts the relationship that exists between transaction values and risk, that is, that the marginal increase in risk reduces as transaction (processing) values increase. This is due to the natural increase in operational sophistication that occurs when transaction throughput increases due, primarily, to enhanced automation.

The Change in Risk shown in Figure 4 is a calculation of the relative marginal increase in risk that occurs from band-to-band. The resulting logarithmic curve depicts the decelerating change in risk as transaction processing values increase: the change in risk starts steeply at Bands 1 to 2 (a change factor of 11.2) and is negligible from Band 13 (a change factor of 0.08 and declining). Applications of the method in live operating environments over more than a decade reveal that operating sophistication (highly automated operating environments) typically materialise when daily transaction throughput by product grouping is greater than $100 million.

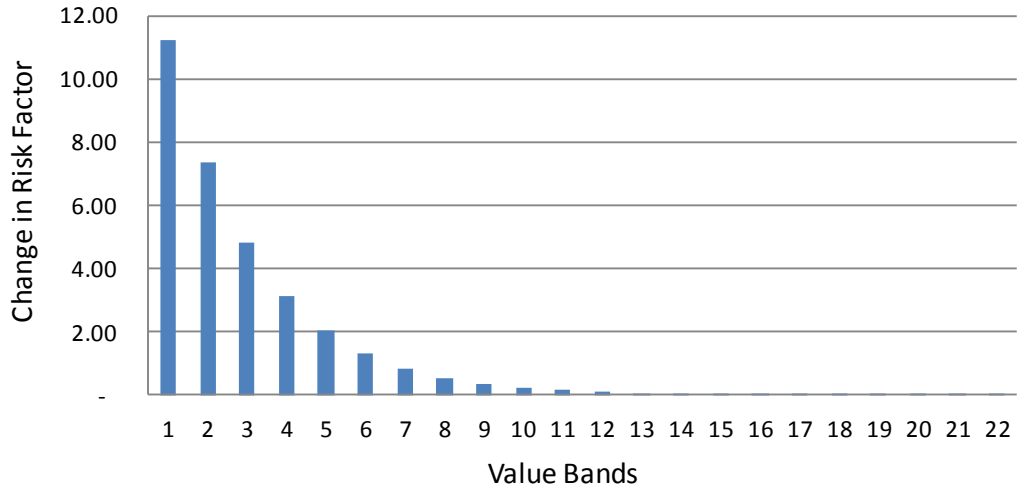

Figure 4 – The Value Table: Change in Risk

As discussed above, the values applied to the Value Table are derived from official accounting records and can represent either daily account movements (new business) or account balances (risk position). The applicable Value Band Weighting is obtained from the Value Table by applying the values in accordance with the criteria set out in Figure 5.

	Transaction Based Products *	Credit Products	Traded Products
Daily New Exposures *(General Ledger account movements)*	Total volume (total number of transactions multiplied by average transaction value)	The amount of new inherent credit risk exposures created on a particular day which can be either: • New loans disbursed including rollovers and extensions • Credit cards and overdrafts – **increase** in total balances	The amount of new trading related inherent market risk exposure created on a daily basis determined by calculating the **aggregate** notional values of the trades (buys, sells and related hedges) relative to a particular trading position that are executed during a given trading day.
Risk Position *(General Ledger account balances)*	Not Applicable	The amount of credit risk exposure inherent in outstanding balances at a given point in time, e.g. balance sheet date	The amount of market risk exposure inherent in trading positions determined by calculating the **aggregate** market values, however derived, of the balance of the trading position at a given point in time, e.g. balance sheet date.

Figure 5 – The Value Table Application Criteria

Transaction Based Products are purely operational and only trigger processing risk. They include, for example, payment orders, safekeeping, lock box and escrow services.

The amount of 'Daily New Exposures' relative to credit risk is determined by reference to the total amount of loans disbursed, guarantees approved, etc. by product. Where credit risk is not the result of a loan disbursement, e.g. casual overdrafts, credit card outstandings, etc., the net day-to-day increase in total outstandings of the respective portfolio is considered to be the new daily credit exposures.

For market risk 'Daily New Exposures' is the aggregate trades (buys and sells) and related hedges relative to each trading position on the principal amounts. Abnormally high trading volume is an indicator of risk and such activities should be reflected in management reports albeit adjusted by the applicable Exposure Uncertainty Factor (EUF) discussed in the next section. Aggregate values are also applied to the products and related hedges that comprise a market risk 'Risk Position' as a high EUF is an indication of a probability that these products and hedges may not be validly combined and netted in a single trading position (basis risk).

In the case of market risk and counterparty credit risk with respect to derivatives, risk accounting considers that the notional values are representative of transaction size as they provide the basis on which future cash flows, mark-to-market and mark-to-model calculations, collateral deposits and related gains and losses are determined. When calculating the exposure in RUs inherent in 'Risk Positions' for both credit and market risk, Risk Accounting uses the fair values or market values in accordance with accounting standards as these more accurately reflect the outstanding amounts.

Product Exposure Uncertainty Factor (EUF) Tables

Risk Accounting considers that unexpected loss and exposure uncertainty are positively correlated. The amount of risk inherent in a transaction accepted for processing relates to its potential to cause unexpected losses which can be prevented through a firm's effective monitoring and management of the associated risks, which is precisely what Risk Accounting is designed to facilitate.

An unexpected loss occurs in circumstances where a firm's management believes its risk management processes are effective but, in reality, they are not due to failures either in their design or application. It follows that an unexpected loss cannot result from a firm intentionally taking on a risk for a projected return if the decision to accept such risk is a consequence of the application of effective risk management processes represented by a high Risk Mitigation Index (RMI) and within approved risk appetite parameters.

Uncertainty is synonymous with risk. Where there is high exposure uncertainty there is also a high probability of unexpected loss. The following are the key risk types with illustrative discussions of EUFs:

Processing Risk: If a transaction is accepted for processing and, either due to the related product's inherent complexity or operational systems inefficiency, it requires interaction with a relatively large number of operational processes in multiple departments the probability for processing failure will be elevated. Processing failure creates exposure uncertainty as accounting records become unreliable; it will not be known with certainty what a bank owes to others and what others owe to the bank. In

these circumstances the product will be assigned a high Processing EUF. Conversely, a product that has a high straight-through-processing (STP) rate will have a low Processing EUF.

Credit Risk: A mortgage loan will be assigned a high Credit EUF because, upon default, there will be uncertainties concerning the time, effort and cost of foreclosing on a mortgage asset and the liquidation value that will be realized whereas an unsecured loan will have a low EUF as the precise amount of exposure upon default will be immediately known. It is assumed that banks will limit their exposures to credit products with low Credit EUFs in line with risk appetite considerations.

Market Risk: A trading position comprised of complex OTC derivatives will have a high Market EUF because a decision to cease trading and exit the risk position could require many months or even years to liquidate the portfolio with the attendant uncertainties as to the liquidation price that will ultimately be realized.

Liquidity Risk: If an investment or credit product is represented by an asset that requires stable sources of funding in the form of reserves of high quality, highly liquid assets it will be assigned a high Liquidity EUF.

Interest Rate Risk: Asset and liability products that are highly sensitive to changes in interest rates will be assigned a high Interest Rate EUF. Products with high Interest Rate EUFs will typically have relatively long maturities and fixed rather than floating rates of interest.

Conduct Risk: Investment products or products that are the result of bundling multiple products such as insurance linked to a loan or a swap linked to a loan... or products that have designated sales incentive schemes will have a high Conduct EUF due to the elevated possibility of misselling and the occurrence of unexpected losses due to litigation or governmental or regulatory penalties.

Following the above rationale the key risk types and their definitions used in Risk Accounting are the following:

Processing	...transactions accepted for processing are properly approved and processing is complete, accurate and timely
Credit	...in the event of an assumed default, a liquidation price for underlying collateral can be realised in a reasonable timeframe and without incurring exceptional losses
Market	...in the event of an assumed unwinding of a risk position, a liquidation price can be realised in a reasonable timeframe and without incurring exceptional losses
Liquidity	...stable sources of funding are available to fund immediate and foreseeable operating needs
Interest Rate	...in the event of unpredicted interest rate movements, interest rate sensitive assets and liabilities can be extinguished, replaced, extended or renewed in a reasonable timeframe and without incurring exceptional losses
Conduct	...positive customer outcomes are achieved and customers are treated fairly

A sample Credit EUF Table is shown in Figure 6. Credit workout and loan recovery experts have assigned an Exposure Uncertainty Factor (EUF) on a scale of zero to 20 to credit products based on their assessment of the relative difficulty they anticipate in liquidating collateral and the collateral's value retention properties. For example, an unsecured commercial loan has an EUF of '2' because, on an assumed default, the exposure and loss potential of an unsecured loan is immediately known. A loan secured on residential property has an EUF of 16 because the process of foreclosing on a defaulted residential property loan and disposing of the property within a reasonable timeframe is complex with a relatively high degree of uncertainty as to the amount of loss that might ultimately be written-off.

Credit Type	Form of Security / Type of Instrument	EUF
Commercial	Casual Overdraft	2
Commercial	Credit Card	2
Commercial	Unsecured	2
Commercial	Cash	4
Commercial	Cash Like Instruments (Margins, Liquid AAA Collateral)	5
Commercial	Repurchase Agreements (Repos)	5
Commercial	Trade Receivables	8
Commercial	Instruments Subject to Mark-to-Market	8
Commercial	Autos	8
Commercial	Inventory	12
Commercial	Equipment	12
Commercial	Investments Subject to Mark to Model	12
Commercial	Personal Guarantee	14
Commercial	Project Financing	16
Commercial	Commercial Real Estate	18
Counterparty	Forward Foreign Exchange	4
Counterparty	Interest Rate Swaps	8
Counterparty	Cross Currency Swaps	8
Counterparty	Security Based Swaps	8
Counterparty	Options	8
Counterparty	Credit Default Swap	14
Counterparty	Collateralized Debt Obligations and Asset Backed Securities	18
Retail	Casual Overdraft	2
Retail	Credit Card	2
Retail	Unsecured	2
Retail	Autos	8
Retail	Personal Guarantee	14
Retail	Residential Property	16

Figure 6 – A Sample Credit EUF Table

There are similar EUF Tables for each risk type: Processing, Credit, Market, Liquidity, Interest Rate and Conduct.

Processing Risk in More Detail

An operating environment can be deconstructed into the simple model shown in Figure 7 represented by three key operational pillars: people, data, and core applications. If the operational interaction of the three operational pillars - manual processes and automated processes with data - is flawless there is no exposure

to processing risk and a theoretical risk-free operating environment is the result. Thus, the unattainable but hypothetical benchmark for a risk-free operating environment can be represented as 100 per cent straight-through-processing (STP) with totally reliable and secure core applications and flawless data.

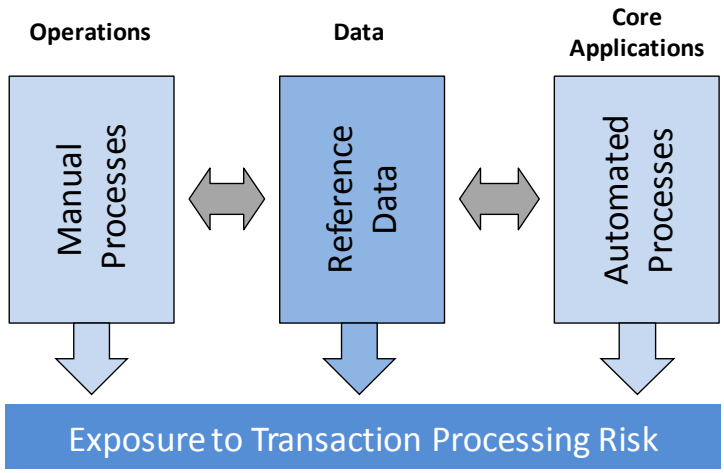

Figure 7 – The Three Pillars of an Operating Environment

This same benchmark also represents a transaction processing environment that is operating at or close to optimal efficiency. Consequently, the correlation between risk mitigation effectiveness and operating efficiency is either '1' or close to '1'.

It follows that exposure to processing risk and the loss of operating efficiency, are the consequence of the failed and/or insecure interaction of manual processes and automated processes with data relative to the processing of transactions and the internal management of financial risks. The risk metrics produced by Risk Accounting are aligned to this dynamic.

Individuals directly concerned with managing processing risk, primarily operations management, will benefit from Risk Accounting as the three core metrics not only provide a framework for proactively and dynamically mitigating processing risk but also enhancing operating efficiency due to the positive correlation of these elements.

In order to be effective, core metrics must be available at an appropriate level of granularity. In the case of operations management this is deemed to be at the operational 'process' level. To accommodate this, the inherent risk in RUs calculated at the business component level is reallocated to operational processes in proportion to the inherent risk of the operational activities that are executed within each process. This is facilitated by the Operational Activity Catalogue shown in Figure 8 that includes a sample of operational activities concerned with the capture, verification, processing, control, accounting and reporting of transactions.

The Operations Activity Catalogue has been compiled through more than a decade of implementing the operations component of the Risk Accounting method in financial institutions. The activities and associated activity weightings have been defined by subject matter experts and subject to continuous refinement through their active application, analysis and evaluation of the associated outputs.

Activity Type	Activity Description and Examples	Activity Weighting
Handling & Distribution	• Control and distribute incoming / outgoing value bearing instructions, e.g. SWIFT messages, Telexes, E-mail, Verbal	9
	• Control and distribute incoming / outgoing non-value bearing instructions and documents	1
Client Services	• Investigation and resolution of client initiated queries	3
Cash Management	• Determine and control cash positions - To support internal and external funding decisions - Advise / agree cash positions with clients - Cash projections and predictions	5
Custodian Services	• Non physical custodian services - Corporate actions	8
	• Non physical custodian services - Proxy voting	2
Control	• Independent verification and validation	4
Documentation Preparation	• Prepare and distribute external documentation (excluding legal and credit risk) - Client agreements - Other legal documentation (suppliers, outsourcing)	4

Figure 8 – Operational Activity Catalogue (Sample)

Once the amount of inherent risk expressed in RUs has been determined for each process, Process Owners complete the scorecard shown in Figure 15 relative to the processes conducted under their responsibility. These inputs provide the basis of the calculation of the RMI discussed in the next section.

Calculation of the Risk Mitigation Index (RMI) and Residual Risk

To understand the RMI one must first understand Component Business Model design which Dodani[28] explains in the following terms:

> *"The main components of an enterprise architecture describe the structure and behaviour of the enterprise's assets (its processes, information and people) through well-defined business and IT architectures that are aligned with the enterprise's goals and strategies"*
>
> *"IBM's Component Business Model designs the business as a set of cohesive and loosely-coupled components that can be combined as a network to support the underlying business activities and that can be shared across the enterprise (and) combine similar activities resulting in increased flexibility and efficiencies"*
>
> *"...the business component allows a natural transition to a services view and can be elaborated by modelling the underlying business processes"*

[28] Dodani (2008), "The Architecture of Business", *Journal of Object Technology,* vol. 7, no. 4, pp 43-50

Risk Accounting is aligned to Component Business Models whereby the business components that comprise a firm's operating environment are identified and assigned to one of the following categories:

- Transaction Processing
- Risk Management
- Core Applications Management
- Data Management

Transaction processing can be characterised as a transaction's journey through a bank's operating environment. This journey is also referred to as the 'end-to-end' processing cycle that starts with a transaction's origination and ends at its registration in accounting systems. Each product has its own predefined end-to-end processing cycle that involves a combination of the Business Components shown in Figure 9. For each product the business components that comprise its end-to-end processing cycle are identified and the result is referred to as the 'Product Processing Profile'.

Transaction Processing		
1. Product & Service Pricing	10. Position Control & Amendments	19. Billing / Collections
2. Deal Structuring	11. Transaction Reporting	20. Physical Commodities Mgt
3. Order Management	12. Credit Limit Monitoring	21. Collateral & Margin Mgt
4. Pre-Trade Validation	13. Trading Limit Monitoring	22. Trading Account Reconciliations
5. Quote Management	14. Trade Settlement	23. G/L Proofs & Substantiation
6. Trade Execution & Capture	15. Corporate Event Processing	24. Management Reporting
7. Cash Management	16. Custody Services	25. Regulatory & External Reporting
8. Depot Management	17. Payments	
9. Trade Confirmation & Matching	18. Nostro Reconcilement	

Risk Management	Core Applications Management	Data Management
1. Treasury	1. Integrated Trading System	1. Client & Counterparty Data
2. Valuation & Pricing	2. Funds Transfer System	2. Market Data
3. Scenario Management	3. Global Nostros System	3. Products & Instruments Data
4. Curves Management	4. Global Ledger System	4. Corporate Events Data
5. Risk Quantification	5. Funding & Liquidity System	
6. Loss Data		
7. Risk Model Back Testing		
8. Operational Risk Management		
9. Capital Optimization & Limits		
10. Counterparty Credit Risk Mgt		
11. Portfolio Risk Analysis		
12. Stress Testing		

Figure 9 – A Sample Summary of Business Components by Category

A Risk Mitigation Index or RMI is calculated for each business component. Additionally, for transaction processing business components, an RMI is calculated at the operational process level as described in the section 'Processing Risk in More Detail' above. The RMI is determined by mapping the actual status of business components and processes to standardized Best Practice Scoring Templates (BPSTs) and

extracting the applicable scores which are used in an RMI calculation, prorated on a scale of zero to 100. Figure 10 provides an overview.

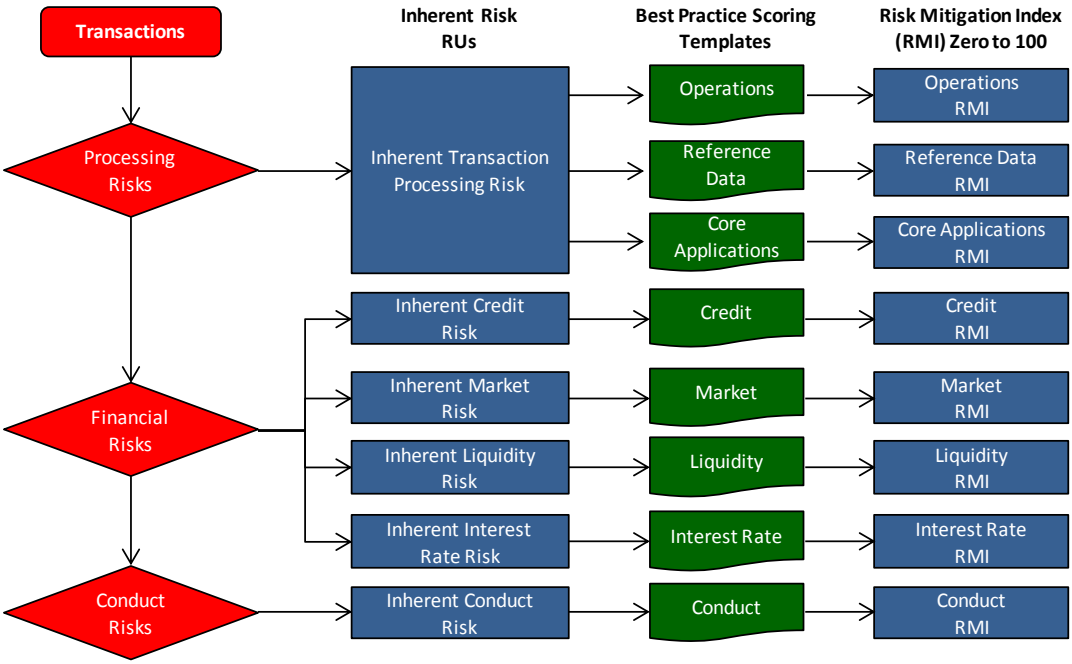

Figure 10 – Calculation of the Risk Mitigation Index (RMI)

Examples of two BPSTs are shown in Figure 11 that provide the primary input for the calculation of the RMI. In this case, they relate to the Operations component of processing risk; there are other BPSTs for Data Management and Core Applications Management as part of processing risk and also for the other key risk types: credit, market, liquidity, interest rate and conduct risk. A summary of BPSTs is provided in Figure 12.

Best Practice Categories	Weight-ing	Score
Control	10	0 to 100
People	10	0 to 100
Execution	10	0 to 100
Business Recovery	8	0 to 100
Risk Awareness	6	0 to 100
Performance Monitoring	6	0 to 100
Logical Access Mgt	4	0 to 100
Vault (Custodial) Mgt	4	0 to 100
Policies & Procedures	2	0 to 100

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

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)

Figure 11 – Sample Best Practice Scoring Templates (BPSTs)

The design of BPSTs is the result of consultation with subject matter experts who determine the key features of management and control structures that are relied on to minimize the probability of operational failure.

In the case of the operations component of processing risk the following nine features or best practice categories were determined by subject matter experts (the composition of best practice categories are specifically aligned to the attributes of the respective risk types):

1. Control
2. People
3. Execution
4. Business Recovery
5. Risk Awareness
6. Performance Monitoring
7. Logical Access Management
8. Vault (Custodial) Management
9. Policies & Procedures

These nine categories are then weighted by subject matter experts on a scale of 1 to 10 according to the degree of reliance typically placed on each one when managing through stress conditions. In Figure 11 it can be seen that Control, People and Execution were assigned a maximum '10' weighting. This means that these categories must be functioning to a standard of excellence if operational failure in stress conditions is to be avoided.

There are two types of BPSTs: the one on the left of Figure 11 (Execution) is based on operating benchmarks and the one on the right (Business Recovery) on best practice components.

For the benchmark-based templates subject matter experts are again consulted to determine the sub-categories that comprise a best practice category. In the case of 'Execution' they were determined to be:

1. The degree of automation or S-T-P rate (straight through processing)
2. The quality of inputs expressed as the average percentage of inputs that is either rejected or repaired prior to processing
3. The robustness of the core systems measured by the number of system failures in a year

The benchmarks are then weighted according to their potential to cause operational failure by scaling them within a range of 1 to 100.

Process Owners in operations then use the best practice scoring template to determine an actual score for 'Execution' relative to their particular process on a scale between zero and 100. For example, if they reject or repair 5% of the input prior to processing they score '75' for this sub-category.

The actual score that is used for 'Execution' will be the lowest score of the three sub-categories because the negative impact of a low scoring sub-category negates the positive impact of a high scoring sub-category. For example, the operational value-added of a 100% straight-through processing process is lost if the core application is unstable, that is, it is unavailable for whatever reason more than 12 times in a year.

For the 'Business Recovery' best practice scoring template subject matter experts are again consulted to determine the components that comprise a best practice business recovery plan. Each component is then weighted on a scale of 1 to 100 according to their relative contribution to a best practice business recovery plan; these are the values shown in brackets next to each component in the BPST on the right of Figure 11. Process Owners then score the category relative to their process starting with a maximum score of 100 and then deducting the amount in brackets for each component that is missing or not complied with.

BPSTs have been developed for each risk type and comprise 'generic' templates that are valid for multiple risk types. 'Technical' templates are unique to a particular risk type as shown in Figure 12.

Generic	Technical	
• Internal Control	**Operations**	**Market Risk**
• People	• Vault (Custodial) Management	• Trading Limit Administration
• Execution	**Reference Data**	• Market Data Analytics
• Business Continuity	• Data Quality Management	**Credit Risk**
• Risk Awareness	• Uniqueness	• Credit Assessment & Approval
• Performance Monitoring	• Vendor Data Services	• Credit Quality Assurance
• Logical Access Management	**Core Applications**	**Liquidity Risk**
• Policies & Procedures	• Systems Maintenance	• Liquidity Buffer Management
• Model Management	• Migration & Acceptance	**Conduct Risk**
	• Vendor Management	• Product Approval
	Interest Rate	• Incentive Programs
	• Interest Rate Exposure Mgt	• Customer Profiling

Figure 12 – BPST Summary

The residual risk in RUs is then calculated which is the inherent risk reduced by the RMI as a percentage as shown in Figure 13.

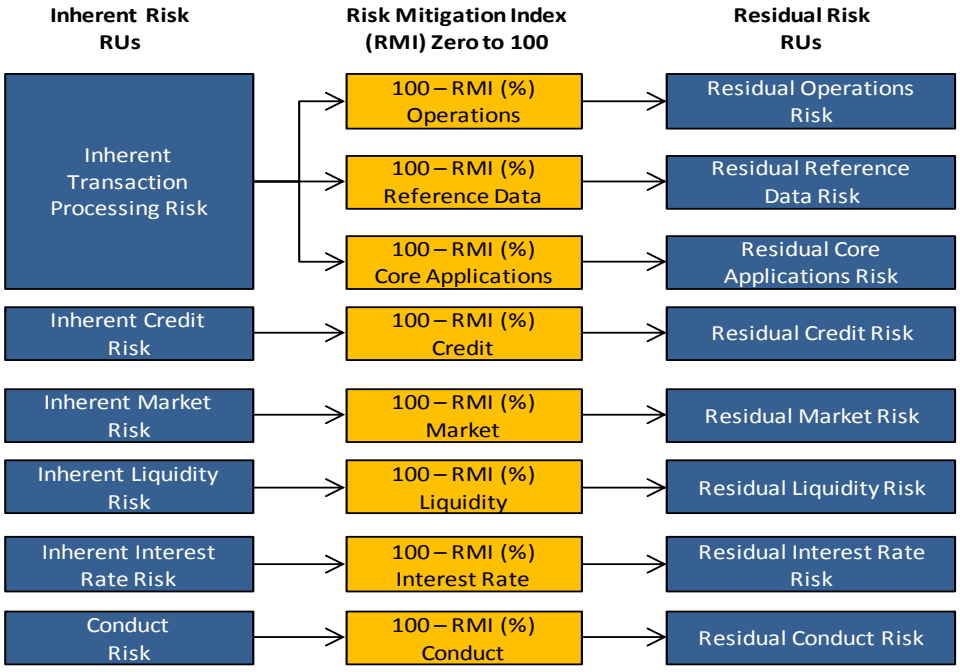

Figure 13 – Calculation of Residual Risk in RUs

Target Scores and Risk Reduction Plans

The scores input to the BPSTs are performed in two passes, (1) current score, and (2) target score, whereby the target score represents the risk mitigation status that can be reasonably achieved within a predetermined timeframe usually tied to the firm's periodic business planning cycles.

When determining target scores the actions that are required to close the gap between the two scores are recorded. Risk Accounting calculates the risk reduction impact in the form of residual risk RUs attributable to each action and the corresponding improvement in the RMI. This information is used to construct a fully prioritised 'Risk Reduction Plan' as shown in Figure 14 that takes the current residual RUs and RMI for selected organisational components, e.g. Group, Division, Department, Production Team etc., and lists the actions in order of their risk reduction impact and maps these to the target measurements of residual RUs and RMIs.

Action Description	Action Ref	Residual (RUs)	RMI
Current Assessment		**1,008**	**42.5**
Develop, implement and test a best practice Business Recovery plan	A0025	233	13.0
Assign independent risk management function to the unit and develop / implement the corporate risk management programme	A0026	165	9.0
Ensure log-on IDs / passwords are cancelled for leavers and that the practice of password sharing is eliminated	A0027	132	8.0
Implement call-back confirmation procedures on payment instructions received via facsimile and implement an independent check of end-of-day cash positions before their communication to Treasury by e-mail	A0028	100	5.7
Complete documentation of policies and procedures in line with corporate standards and ensure staff awareness of them and ready access to them.	A0029	59	3.0
The general ledger only requires single stage input. Any input errors are first detected during the month end reconciliation process. Independent sight verifications of daily inputs should be implemented and an upgrade of the general ledger to dual stage input be considered.	A0030	58	3.0
To reduce the high incidence of data input errors a programme of training should be undertaken with the source departments and tracking reports implemented that identify offending units.	A0031	31	1.8
All others	Various	104	6.8
Target		**126**	**92.8**

Figure 14 – Sample Risk Reduction Plan

The Risk Accounting Calculations and Scorecard

A sample scorecard is shown in Figure 15. The calculation of the three core metrics can be represented as follows:

The **inherent risk** for each transaction:

$$RU_{INH} = \sum(VBW \times RT_{EUF})$$

Where:

- RU_{INH} is the amount of Inherent Risk Units
- VBW is the Value Band Weighting
- RT_{EUF} is the Exposure Uncertainty Factor for each applicable Risk Type

The **Risk Mitigation Index (RMI)** for each business component and, for operations components, each process:

$$RMI = \frac{\sum(BPST_{S1\text{-}9} \times BPST_{W1\text{-}9} \times RU_{INH})}{\sum(BPST_{M1\text{-}9} \times BPST_{W1\text{-}9} \times RU_{INH})}$$

Actual Score Aggregate Algorithm

Maximum Score Aggregate Algorithm

Where:

- RMI is the Risk Mitigation Index
- $BPST_S$ is the Best Practice Scoring Template category scores
- $BPST_W$ is the Best Practice Scoring Template category weightings
- $BPST_M$ is the Best Practice Scoring Template category maximum score (100)
- RU_{INH} is the amount of inherent Risk Units

The **residual risk**:

$$RU_{RES} = \left(\frac{100 - RMI}{100}\right) \times RU_{INH}$$

Where:

- RU_{RES} is the amount of Residual Risk Units
- RMI is the Risk Mitigation Index
- RU_{INH} is the amount of Inherent Risk Units

Activity Descriptions & Weightings	Activity Weighting	Control Evaluation	People	Execution	Business Continuity	Risk Awareness	Performance Monitoring	Logical Access Management	Vault (Custodial) Management	Policies & Procedures	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)	Actual Score Aggregate	Maximum Score Aggregate
		10	10	10	8	6	6	4	4	2					
Commercial Loan Operations															
Handling & distribution	1														
Documentation preparation	4														
Document Preparation	5	20	55	65	0	0	10	100	100	50	12	39.3	7	27,171	69,078
Control	4														
Prepare, capture & control transactions	4														
Control	4														
Booking and Funding	12	30	60	55	0	60	50	50	100	0	28	45.2	15	74,881	165,788
Control	4														
Prepare, capture & control transactions	4														
Repayments	8	20	60	30	0	20	30	30	100	10	18	32.3	12	35,736	110,525
Handling & distribution	1														
Transaction amendments	2														
Query Resolution	3	25	60	75	0	50	100	100	100	60	7	57.0	3	23,625	41,447
Handling & distribution	1														
Transaction amendments	2														
Exception Processing	3	100	30	97	0	70	80	80	100	80	7	67.5	2	27,977	41,447
Total	**31**	**32.1**	**56.3**	**56.2**	**-**	**40.0**	**46.1**	**60.6**	**100.0**	**24.2**	**71**	**44.2**	**40**	**189,390**	**428,285**
Actual Score Aggregate		22,911	40,181	40,088	-	17,131	19,756	17,316	28,552	3,454	**189,390**				
Maximum Score Aggregate		71,381	71,381	71,381	57,105	42,829	42,829	28,552	28,552	14,276	**428,285**				

Figure 15 – A Sample Scorecard for Processing (Operational Systems) Risk

The Actual Score Aggregate Algorithms and Maximum Score Aggregate Algorithms are aggregated across the horizontal and vertical dimensions of the enterprise and are used to calculate the RMI for each reportable component which can be, for example, organisational (group, business line, department, process etc.) or product, customer, legal entity and location. The aggregate algorithms also function as a control mechanism to prove the accuracy of reports.

Sample Risk Accounting Reports

A scorecard, as shown in Figure 15, is created for all business components and all processes within operations business components. The Risk Accounting software aggregates these scorecards at required reporting levels through to the total group level.

Sample Risk Accounting reports have been included below for illustration purposes. Figure 16 shows the consolidated group risk report by product. It can be noted that the total Inherent Risk (16,057 RUs) and the aggregate algorithms (Actual: 703,824,598 / Maximum: 984,707,980) function as control totals to prove the accuracy of reports. The actual and maximum aggregate algorithms are also used to calculate the RMI at each reporting level.

Total All Products	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)	Actual and Maximum Aggregate Algorithms	
FX Forwards	1,092	72.6	299	58,711,787	80,856,680
Commercial Loans (Secured)	1,754	70.1	524	25,482,516	36,350,420
Fixed Term Deposits	351	74.2	91	13,415,490	18,090,000
Repos	513	73.2	137	16,574,490	22,636,800
Cross Currency Swaps	1,454	74.1	377	80,002,908	107,989,200
Futures	1,571	72.0	440	113,501,524	157,709,200
CDOs	5,218	69.2	1,608	169,255,839	244,612,500
Equities	1,390	71.6	395	77,599,640	108,369,400
Fixed Income	2,550	71.6	725	139,169,984	194,420,980
Payment Orders	162	73.9	42	10,110,420	13,672,800
Total	**16,057**	**71.5**	**4,580**	703,824,598	984,707,980

Figure 16 – Sample Total Risk Report by Product

Figure 17 shows the same total risk report shown in Figure 16 but broken down by best practice categories rather than by product.

Figure 18 again shows the same total risk report but, in this case, broken down by business component. A product specific risk report can be produced in this format for each product shown in Figure 16.

Risk Accounting's method of risk data aggregation is to aggregate the Actual and Maximum Score Aggregates and recalculate the RMI at each reporting level. The calculated RMI is applied to the Inherent Risk RUs in order to calculate the Residual Risk RUs. As the enterprise only processes a transaction once along its respective end-to-end processing cycle, the Inherent Risk RUs and Residual Risk RUs relative to Processing Risk are not summed.

Best Practice Categories	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)	Actual and Maximum Aggregate Algorithms	
Generic					
Internal Control	1,801	75.6	439	**83,524,430**	**110,427,330**
People	2,547	72.7	696	**113,544,897**	**156,214,350**
Execution	2,432	59.4	988	**88,525,192**	**149,119,960**
Business Continuity	1,503	87.2	192	**80,394,159**	**92,163,250**
Risk Awareness	1,439	68.7	450	**60,620,221**	**88,231,270**
Performance Monitoring	1,418	67.2	466	**58,416,476**	**86,964,200**
Logical Access Management	1,039	68.6	326	**43,747,983**	**63,744,080**
Policies & Procedures	610	76.8	142	**28,707,808**	**37,398,900**
Model Management	87	47.4	46	**2,515,905**	**5,310,180**
Technical					
Processing					
Vault (Custodial) Management	619	100.0	0	**37,925,154**	**37,932,200**
Reference Data					
Data Quality Management	256	64.6	91	**10,162,090**	**15,725,700**
Uniqueness	103	47.9	53	**3,012,858**	**6,290,280**
Vendor Data Services	103	79.6	21	**5,008,378**	**6,290,280**
Core Applications					
Systems Maintenance	705	67.3	230	**29,100,920**	**43,212,400**
Migration & Acceptance	705	65.9	240	**28,471,635**	**43,212,400**
Vendor Management	423	82.6	73	**21,423,009**	**25,927,440**
Market Risk					
Trading Limit Administration	29	69.8	9	**1,231,950**	**1,765,800**
Market Data Analytics	17	61.0	7	**646,776**	**1,059,480**
Credit Risk					
Credit Assessment & Approval	39	34.0	26	**814,210**	**2,397,200**
Credit Quality Assurance	16	33.4	10	**319,800**	**958,880**
Liquidity Risk					
Liquidity Buffer Management	34	75.0	8	**1,559,775**	**2,079,700**
Conduct Risk					
Product Approval	43	51.3	21	**1,352,250**	**2,635,500**
Incentive Programs	34	43.0	20	**906,540**	**2,108,400**
Customer Profiling	34	38.9	21	**819,380**	**2,108,400**
Interest Rate					
Exposure Management	23	75.0	6	**1,072,800**	**1,430,400**
	16,057	**71.5**	**4,580**	**703,824,598**	**984,707,980**

Figure 17 – Sample Total Risk Report by Best Practice Category

Total All Products	Inherent Risk (Risk Units)	Risk Mitigation Index (RMI)	Residual Risk (Risk Units)	Actual and Maximum Aggregate Algorithms	
Processing Risks					
Transaction Processing Risk					
Product & Service Pricing	1,186	66.8	393	4,755,860	7,116,000
Deal Structuring	1,186	60.7	466	4,317,040	7,116,000
Order Management	4,420	65.2	1,540	17,281,418	26,518,800
Pre-Trade Validation	4,420	70.0	1,326	18,563,160	26,518,800
Quote/Price Management	5,586	70.0	1,676	23,461,620	33,516,600
Trade Execution & Capture	4,916	79.2	1,024	23,352,425	29,497,800
Cash Management	5,748	68.0	1,839	23,452,248	34,488,600
Trade Confirmation & Matching	4,916	56.0	2,163	16,518,768	29,497,800
Position Control & Amendments	4,916	79.7	1,000	23,499,914	29,497,800
Transaction Reporting	4,916	70.8	1,434	20,894,275	29,497,800
Credit Limit Monitoring	4,916	85.2	729	25,122,293	29,497,800
Trading Limit Monitoring	4,916	86.7	656	25,564,760	29,497,800
Trade Settlements	4,916	85.8	696	25,318,945	29,497,800
Depot/Custody/Collateral Management	4,636	64.5	1,646	17,940,546	27,814,800
Loans Processing	265	53.4	123	848,834	1,588,800
Payments	5,748	92.5	431	31,901,955	34,488,600
Nostro Reconcilement	5,748	91.7	479	31,614,550	34,488,600
Trading Account Reconciliations	4,230	67.2	1,389	17,044,885	25,377,000
G/L Proofs & Substantiation	5,748	86.3	786	29,775,158	34,488,600
Management Reporting	5,748	64.2	2,060	22,130,185	34,488,600
Regulatory & External Reporting	5,748	62.0	2,184	21,382,932	34,488,600
Transaction Processing Risk	**5,748**	**74.6**	**1,457**	**424,741,771**	**568,983,000**
Data Quality					
Client & Counterparty	5,748	63.9	2,073	20,578,198	32,189,360
Market Data	4,230	56.6	1,835	13,407,515	23,685,200
Products & Instruments	5,748	88.6	657	28,510,576	32,189,360
Data Quality	**5,748**	**71.0**	**1,669**	**62,496,289**	**88,063,920**
Core Applications					
Client & Counterparty Data	5,748	78.9	1,215	28,108,209	35,638,220
Market Data	4,230	54.5	1,924	14,295,710	26,222,900
Products & Instruments Data	5,748	66.6	1,919	23,739,653	35,638,220
Trading System	4,392	48.4	2,267	13,174,500	27,227,300
Global Loan System	265	60.6	104	995,648	1,641,760
Funds Transfer System	5,586	65.8	1,910	22,791,288	34,633,820
Global Nostros System	5,748	88.1	686	31,384,626	35,638,220
Global Ledger System	5,748	60.6	2,262	21,612,856	35,638,220
Funding & Liquidity System	5,748	76.6	1,344	27,303,475	35,638,220
Core Applications	**5,748**	**68.5**	**1,813**	**183,405,965**	**267,916,880**
Total Processing Risks	**5,748**	**72.5**	**1,580**	**670,644,025**	**924,963,800**
Financial Risks					
Market Risk	1,766	52.8	834	5,776,616	10,947,960
Credit Risk	2,397	51.8	1,155	7,450,546	14,383,200
Liquidity Risk	2,080	62.9	772	8,110,830	12,894,140
IRRBB	1,430	61.9	544	5,492,736	8,868,480
	7,673	**57.0**	**3,302**	**26,830,728**	**47,093,780**
Conduct Risk					
Conduct Risk	2,636	50.2	1,313	6,349,845	12,650,400
Total Product Risks	**16,057**	**71.5**	**4,580**	**703,824,598**	**984,707,980**

Figure 18 – Sample Total Risk Report by Business Component

Interpreting Risk Accounting's Core Metrics

Inherent Risk RUs is representative of the transaction's maximum possible loss; the risk mitigation index (RMI) is a measure of the effectiveness of the enterprise in mitigating inherent risk through the effective management and control of the firm's operating environment; and Residual Risk RUs is representative of the probability of unexpected loss. The probability of unexpected loss can be thought of as the portion of Inherent Risk RUs not covered by effective risk mitigation. Risk Accounting allows these metrics to be aggregated horizontally and vertically across the enterprise.

If the risk mitigation index (RMI) is low the probability of unexpected loss is high. Or said another way, if the credit RMI is low there's a high probability that loans have been approved or disbursed that shouldn't have been approved or disbursed. Another example is if the market RMI is low there is a high probability that traders are operating unauthorized positions.

As previously commented, the adoption of a new risk metric for risk reporting – the Risk Unit - will challenge the sensibilities of many. One aspect that will perhaps enhance the RU's attractiveness is the prospect that, through the statistical correlation of exposures to risk in RUs and actual loss history, the monetary value of an RU can be derived over time (see the section 'The Risk Unit (RU)' above). This opens up many possibilities for risk reporting encompassing enterprise risk management (ERM), BCBS 239 compliance, risk appetite setting and monitoring, and capital management:

- An integrated framework of **Risk Data Controls** can be created through a monovalent risk measurement system using a standardised risk metric, the RU. Transactions are tagged with RUs thereby enabling effective and controlled risk data aggregation.
- **Reconciling Risk Data to Accounting Data**: The source of data for Risk Accounting is the general ledger and it runs in parallel with management accounting so risk data is directly tied to an already proven and trusted source of accounting data.
- **Build to a Single Authoritative Source for Risk Data**: The Risk Accounting system - as an extension of the general ledger and management accounting – will become the single authoritative source of risk data. All risk reports will be reconcilable to that source. This also provides a solution for principle 6 of BCBS 239 'Adaptability' as on-demand, ad-hoc risk reports can be generated from that single source.
- **Capital Adequacy**: The Risk Accounting method can be used to restate a firm's balance sheet in RUs to produce a 'Risk Balance Sheet'. As discussed above, it will be possible over time to derive the monetary value of an RU. That being the case the opportunity exists to use Risk Balance Sheets in RUs as a basis for determining capital adequacy.
- **Regulatory Capital**: Using the same thinking as for capital adequacy, Risk Accounting also creates the potential for regulators to use RUs in the determination of minimum regulatory capital requirements.
- **Capital Ratios**: Risk Accounting enables the explicit and dynamic calculation of exposure to risk using a standardised risk metric for all forms of risk – the RU - that can be used to provide more relevant, risk-based calculations of capital ratios.
- **Processing, Credit, Market, Liquidity, Interest Rate and Conduct Risk**: The explicit and dynamic calculation of exposures to these risks is a natural output of the Risk Accounting method by design.
- **Stress Testing**: The additional, more comprehensive and representative risk information provided by Risk Accounting, which is directly comparable within and between firms, should lead to less reliance on stress testing to determine the exposure to risk of whole enterprises. Particularly

significant here is that Risk Accounting calculates an enterprise's inherent risk as being representative of its maximum possible loss thereby obviating the need to apply stress testing techniques to derive this value.

- **Risk Appetite Setting & Monitoring**: A firm's risk appetite can be more meaningfully determined using RUs. Given that the general ledger, management accounting and risk accounting are all tied together and are drawn from a common source of data, a firm's risk plan in RUs can be produced in exactly the same format as its financial plan and together they comprise the firm's business plan. It also means that if a firm's risk appetite is set in RUs and reporting is also in RUs, the potential is created for the real-time reporting of excesses over approved risk appetite limits.

A Framework for True ERM and Positive Risk Cultures

The Risk Accounting method and system described in this paper provides the foundation for complying with BCBS 239 by creating a true enterprise risk management (ERM) system. It should become the framework for effective risk governance and improvements in risk culture. Without a common monovalent risk exposure metric – the RU – a framework of effective risk controls cannot be realized. Neither can the mature and proven control features that have evolved relative to accounting data be adapted for risk data to conform to the regulatory requirements contained in BCBS 239.

Risk Accounting also provides the *de facto* metric for risk culture... the RMI, which blends all the risk attributes from across the enterprise into a single metric. Banks' stakeholders including customers, investors, regulators and governments will be able to conclude whether a bank is effectively managing risk by reference to its reported RMI. Through benchmarking RMIs within and between banks a framework of incentives can be created that will provide assurance that improvements in risk culture are being effectively monitored and proactively promoted.

Compliance with BCBS 239 is now set as a mandate for supervisory reviews of firms designated as global systemically important banks (G-SIBs) beginning in 2016 and selected others designated as domestic systemically important banks (D-SIBs). BCBS 239 recognizes that banks' inability to properly identify and aggregate risk data across many business silos has left the financial system vulnerable to unaccounted and unobserved risks that provide the breeding ground for negative cultures to evolve. It is, presumably, with this in mind that BCBS 239 calls for accounting-type controls to be applied to risk data, along with the ability to reconcile risk data to the books and records of the firm.

A new risk-adjusted culture remains to be constructed against the backdrop of the prevalent short-term performance and incentive culture that has characterized much of finance in the last half century. The road to transforming such negative cultures must begin with the design and implementation of effective risk accounting and risk control systems. These imperatives are the stepping-stones to governing and overseeing fundamental cultural change that gets us to a new societal norm in the promising next stage in the evolution of the global financial system.

Conclusion

To summarize, the key features of Risk Accounting are that it is simple; there is no reliance on complex quantitative modeling techniques. The tables and templates are the product of input and validation by subject matter experts which means their knowledge and intellect are embedded in the actual fabric of the risk measurement system making the outputs understandable and actionable. Management will be able to identify risk mitigating projects directly from the outputs of the system.

Report production is timely as calculations of exposure to risk in RUs are performed upon transaction capture in accounting systems and, consequently, can be reported in real-time or near real-time.

Calculations of exposure to risk are representative of the risks actually accepted and, perhaps most importantly, the outputs in RUs and the RMIs are aggregatable; they can be validly aggregated by various categories such as organization, risk type, location, customer, product etc. The outputs are directly comparable within and between financial firms provided standardized tables and templates are applied.

Finally, the outputs are auditable as Risk Accounting uses a standardized measurement based metric.