People risk: Where are the boundaries?

Received: 8th April, 2008

Patrick McConnell
is Visiting Fellow at Macquarie University Applied Finance Centre in Sydney, where he teaches courses in operational risk, systems risk and enterprise risk management.

Macquarie University Applied Finance Centre, Level 3, 10 Spring Street, Sydney NSW 2000, Australia
Tel: +61 02 4861 5054; E-mail: pjmcconnell@computer.org

Abstract Spurred into action by several well-publicised losses in the financial sector, such as the collapse of the venerable Barings bank in the UK, banking regulators have begun to develop rules for quantifying, managing and disclosing operational risks. The Basel Committee, the world's senior banking regulator, has identified four categories of operational risk, namely, processes, people, systems and external events. This paper addresses the 'people' category. Despite the fact that, under the new regulations, capital must be assigned to cover 'people' risks, the boundaries of this particular risk are not well defined. Without a clear definition of this (or for that matter any other) risk, a firm's risk managers, and the boards that they report to, will not know whether such risks are being managed adequately. This paper develops a framework for analysing people risk and concludes that the scope of such risks cannot be managed solely by specialist operational risk management functions. Because of the sheer breadth of people risk, operational risk managers must reach out to other disciplines to properly understand its scope and to develop common approaches to its management.

Keywords: *operational risk, Basel II, people risk*

INTRODUCTION

The Bank for International Settlements (BIS), the world's senior banking regulator, operates through the Basel Committee on Banking Supervision, which formulates supervisory standards and best practice for action by local banking regulators. Note that while the Basel Committee is not itself a regulatory body, its rules are applied by G10 countries to regulate major banks and used by most of the rest of the world as a regulatory standard. After a prolonged debate in the industry, the Basel Committee published, in 2004, the 'Revised Framework for the International Convergence of Capital Measurement and Capital Standards' — the so-called Basel II Accord.[1]

Under Basel II, banks are required to calculate capital to cover operational risk, which the Committee defined very widely as:

> 'The risk of loss resulting from inadequate or failed internal processes, *people* and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk.'[1]

So people risk is, therefore, one of the four key dimensions of operational risk defined by Basel II.

For the world's largest banks — those hoping to use an 'advanced measurement approach' (AMA) to operational risk — the new Basel II regulations require capital to be set aside to cover 'unexpected' operational losses over a one-year period, to a confidence level of 99.9 per cent.[2] One would imagine that such a high confidence interval would require a very clear understanding of the risks being measured.

However, regulators have been reticent (possibly even deficient) in defining precisely what 'people risk' covers. Without a clear understanding of what precisely constitutes people risk, there can be little hope of fully identifying, assessing and mitigating such risks, as required by Basel II, and even less prospect of calculating the operational risk capital needed to cover these risks.

Before proceeding, it is worth noting that the word 'people' occurs just once in the main Basel II document and then only within the definition of operational risk itself. It is clear that, in Basel II, 'people' refers to more than 'employees' as, for example, 'external fraud' is recognised. However, regulators have provided little further guidance as to the full scope of the term.

This point is important because without an understanding of the boundaries of people risk and, ultimately, operational risk:

- critical risks may be missed, resulting in potentially ruinous losses; and
- operational risk managers may not have the necessary skills to fully understand, and hence help businesses to manage, people risks.

This paper attempts to put some boundaries around the scope of people risk, as defined by Basel II, and concludes that operational risk managers must reach out to other disciplines to help manage what is one of the greatest risks facing financial institutions.

SUBPRIME CRISIS — YET ANOTHER EXAMPLE OF PEOPLE RISK

As the subprime crisis gathers pace to become a fully-fledged banking disaster, it is obvious that this multifaceted phenomenon does not fit neatly into the risk categories laid out by banking regulators in Basel II. The growing list of subprime losses appears to arise from a complex interaction of risks:

- *credit risks* — borrowers unable to repay their loans; exacerbated by
- *market risks* — lack of liquidity deflating market prices for collaterised debt obligations (CDOs) created from loans made to 'subprime' borrowers; aggravated by
- *operational risks* — bad lending, valuation and distribution practices.

In addition, it is apparent in the subprime crisis that there are also strategic risks, such as the unsustainable funding strategies adopted by Northern Rock, and reputation risks affecting a long list of blue-chip investment banks, including UBS, Merrill and Barclays. However, although important, these latter risks have been consigned to the 'too-hard basket' by Basel regulators.

The subprime crisis fits somewhere within Basel's definition of operational risk as some of the losses have undoubtedly been 'caused' by 'people'.

In the subprime CDO market, for example, there is evidence of people behaving badly at all stages of the securitisation process:

- *origination:* lax lending practices by brokers and lenders and misstatements by subprime borrowers regarding their ability to repay their loans;
- *structuring:* lack of adequate due diligence on the composition of the asset pools underlying subprime CDO issues;
- *rating:* conflicts of interest in the close cooperation between rating agencies and issuers as to the mechanisms for attaining the highest possible ratings for CDOs, compounded by the fact that rating agencies were slow to reverse their original high ratings when problems began to appear;
- *funding:* lack of understanding of the risks of holding CDOs and, in particular, pricing them in times of crisis;
- *distribution:* lack of information provided to CDO buyers on the potential losses that could be sustained in purchasing these highly-rated but poorly-understood securities; and so on.

Already heads have begun to roll in brokerage houses, banks and rating agencies, and some well-known names have gone under, such as Bear Stearns in the USA and Northern Rock in the UK. Elsewhere, the world's largest financial institutions have sought to raise capital to cover massive write-downs. Legislators in the major economies have begun to initiate formal inquiries and, inevitably, potentially ruinous class-action lawsuits have started to be filed around the world. 2008 is thus shaping up to be the year of 'what happened to cause the subprime crisis?'

While the long-anticipated raising of interest rates by central banks around the world during 2007 was the initial trigger for large-scale subprime losses, it was the inherent shakiness of the underlying CDO securities, bolstered as they were by little-understood derivatives, which caused the underlying problems to explode. Many of the problems that caused the subprime crisis appear to be man (ie people) made.

Unfortunately, the 2008 subprime crisis is not unique. For example, the initial public offering (IPO) scandal of the early 2000s was somewhat similar, although less dramatic, arising from serious ethical lapses throughout the investment banking industry, in bringing new companies to market.

Under Basel II, banks are required to set up an independent operational risk management (ORM) function with clear responsibilities for, *inter alia*, 'developing strategies to identify, assess, monitor and control/mitigate operational risk'.[1] But, among the many imponderables raised by Basel II, the question must be asked as to how exactly should the sub-category of 'people risk' be identified, assessed and controlled/mitigated? While mis-selling of securities would undoubtedly fall within the Basel definition of operational risk (specifically defined in Annex 7 as 'improper business or market practices' within the loss event category 'clients, products and business practices'[1]), it is obviously impractical for individual banks to be expected to actively manage the origination of suspect loans by unethical third-party brokers on the other side of the world.

So precisely where does Basel II enter the picture and where exactly are the boundaries of people risk?

PEOPLE RISK FRAMEWORK

In order to answer this question, a generic 'people risk framework' is shown in Figure 1. In this framework, people risk can be considered as occurring within four distinct, escalating areas:

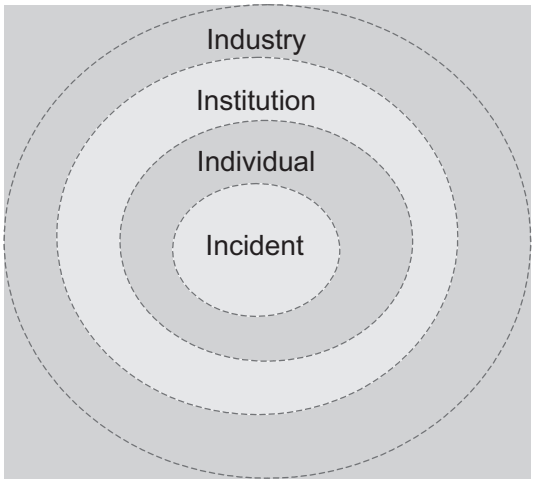

Figure 1: People risk framework

- *Incident:* how do people, especially employees, react when an unforeseen 'incident' happens?, for example, the processing of an incorrect transaction?
- *Individual:* how does an individual (or a small group of individuals) behave with respect to their responsibilities, for example, representations made to customers or bullying of colleagues?
- *Institution:* how does the firm behave with respect to the behaviour of the individuals it employs and with whom it deals, for example, turning a blind eye to profitable, but suspect, transactions?
- *Industry:* how does the industry as a whole behave, for example, in structuring and selling dangerous, potentially illegal, products and services?

Figure 2 shows the same '4Is Framework' with respect to the frequency and severity of operational losses arising from the four areas of people risk identified above:

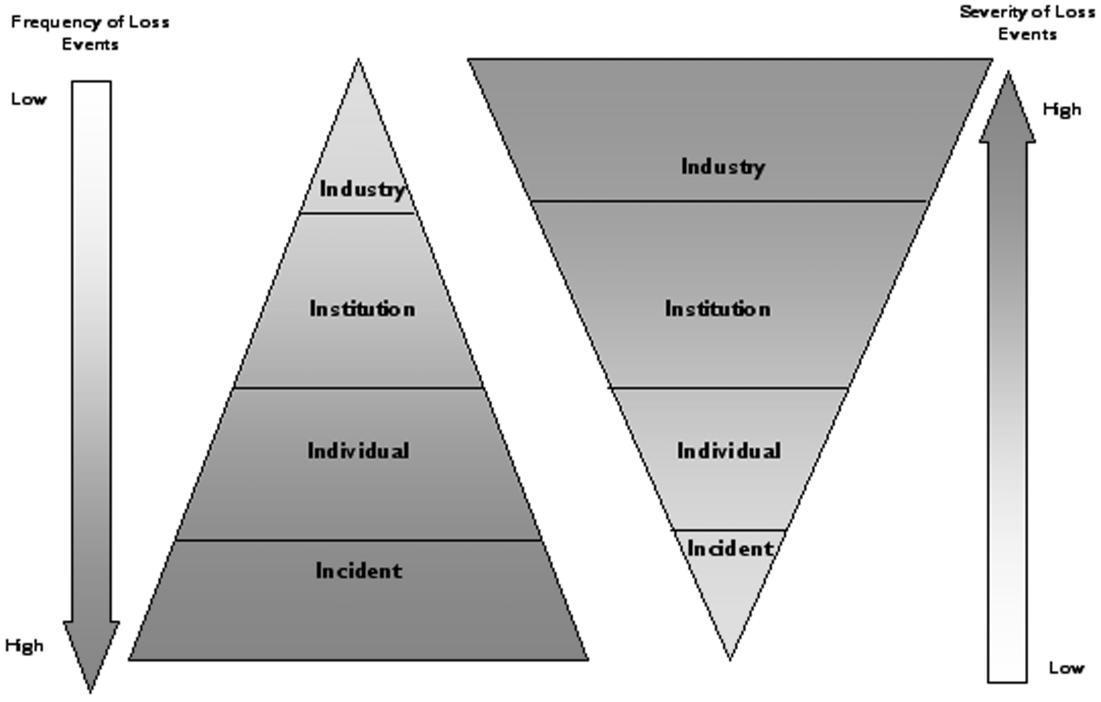

Figure 2: Frequency and severity of losses

- *Incident:* while many loss-making incidents will occur in any large firm, the magnitude/severity of each incident tends to be limited by the very nature of standard operating controls within a mature operation.
- *Individual:* inevitably, some individuals in a firm will break its rules and precipitate losses, either by fraud or by incurring fines. However, the size of such losses will not typically be very large — sometimes, but rarely, in the millions of dollars.
- *Institution:* history has shown that some institutions are dysfunctional, displaying scant regard to their responsibilities to their customers and employees, usually in pursuit of large profits. While rare, the severity of the losses occasioned by the unethical behaviour of individuals at all levels of such a firm can be massive, for example, the collapse of Enron.
- *Industry:* periodically, the banking industry loses its ethical compass and, as with the subprime and IPO scandals, very significant losses occur, often in the form of regulatory fines.

In this framework, the frequency of losses and the severity of losses are inversely related. Thus, the severity of losses is high at the top of the hierarchy, with increasing frequency of losses towards the lower end.

As Basel II concentrates on ensuring that firms maintain capital to cover 'unexpected losses' from 'low-frequency, high-severity' events,[1] it would appear that the greatest losses occur at the institution and industry levels. Banks and regulators, however, have tended to concentrate on the higher frequency, lower severity areas of individual and incident risks. Are risk managers missing the greatest sources of operational risk?

INTENTION

When considering 'people risk' and how to manage it, a key aspect is the 'intention' of the person(s) involved. Do the people involved *intend* to do something that has the potential to cause losses, or not?

Incident

With an unexpected 'incident', it is rarely the intention of the people involved to do anything that might cause a loss, but it is the stress of their jobs, their lack of knowledge, or just plain errors that causes them to make 'bad decisions' that result in negative outcomes, ie losses. Experience has shown that a well-trained workforce, supported by good systems and policies, will make fewer mistakes than stressed, unhappy or inexperienced workers.[3]

To reduce operational risk at the incident level, firms must therefore ensure that there are sufficient trained staff (supported by good systems) to cope with the volume of work thrown at them. An environment where there are experienced, approachable supervisors available to help cope with unusual 'incidents' will also help to ensure that small problems do not grow into large losses. Active support from human resources (HR) experts is needed to mitigate/resolve areas of potential risk, such as lack of training or under-staffing.

From an ORM perspective, there must be mechanisms to monitor losses resulting from such incidents and key risk indicators (KRIs), such as staff dissatisfaction/turnover must be developed in conjunction with HR to alert management to potential problems. Techniques, such as Six Sigma, have also proved successful in other industries to

help to address such problems of 'operational quality'.

Individual

It is at the level of the 'individual', or group of individuals, that 'intention' becomes important.

If a person scrupulously follows the operational policies and procedures laid down by a firm and a loss results then the individual cannot reasonably be held to blame. For example, if a credit officer diligently performs all the checks needed to grant a loan but a borrower has produced convincing, but false, documentation then it is the process, rather than the person, which is to blame (under Basel II, this would be an example of process risk rather than people risk). On the other hand, if a credit officer, due to internal or external pressures, either does not perform sufficient checks or suspects, but does not pursue, false documents, it is obviously 'intentional' and under the Basel II definition would constitute people risk.

Three types of intentional 'misbehaviour' by an individual need to be considered:

- *illegal:* an individual's intention to break civil or securities laws, such as theft or insider trading;
- *unethical:* intentional behaviour that, while not quite illegal, is frowned upon, such as bullying. Unethical behaviour by individuals, such as bullying and sexism, has recently caused firms to be fined heavily in civil proceedings — counting as losses under Basel II — for example, compensation for sexism against a female employee at BNP London in 2004. And
- *inappropriate:* intentionally breaking specific policies of the firm, such as using the firm's facilities for private use.

Unfortunately, the lines between these categories are often blurred and in many situations identical behaviour by one individual (usually a junior) can result in dismissal but be tolerated if perpetrated by another, more senior, individual. The Barings, Allied Irish Bank (AIB), National Australia Bank (NAB) and Société Générale cases all illustrate how inappropriate behaviour can lead to unethical actions that, if tolerated, can lead to illegal activities and can, in extreme circumstances, result in serious losses to the firm.[4–8]

Because there are so many possible opportunities for personal wrongdoing, the identification, assessment and mitigation of individual risks is extremely difficult. The compliance function is normally tasked with protecting a firm from illegal activities and, ideally, should participate in the ORM process of managing the more serious illegal individual risks. However, it is senior management, with support from HR and strong personnel policies, who must address unethical and 'inappropriate people risks'.

The complexity of people risks at the individual level requires that, in order to perform the role required of it, ORM functions must 'reach out' to other 'softer' disciplines, such as HR and compliance, to be partners in the management of these risks. (At this point, it should be noted that operational risk managers in an ORM function are not themselves responsible for managing risks — that can only be done by business managers; the role of ORM is to design and monitor the proper operation of robust operational risk policies and frameworks.) As regards individual staff, operational risk managers can only ever see one part of a bigger picture.

For example, in carrying out risk assessment exercises, an operational risk manager may witness individuals indulging in what appears to be unethical behaviour, such as bullying, or may observe that a particular operating unit is understaffed. However, HR will see a different part of the same picture, such as evidence/complaints of other malpractices by individuals. In such a situation, additional information supplied by a risk manager may be sufficient to expedite corrective action. Conversely, a particular individual may have personal problems causing his/her unusual behaviour that, with some HR counselling, can be corrected fairly quickly. In the example of an overworked department (giving rise to real operational risks), HR may already be in the process of recruiting new staff. If so, risk management can help to support the staffing business case; if not, then HR may need to be convinced of the need to approach management for additional staffing levels.

To be effective, therefore, operational risk managers must be able to communicate with, and influence, other professionals and senior management to address such difficult, often unpleasant, issues affecting individuals.

Institution

Individuals operate within the norms of the institutions in which they work. In service industries, such as banking, it is people, at all levels of the organisation, who determine how the institution, as a whole, behaves (obviously, certain individuals such as the board and senior executives impact the 'behaviour' of a firm more than others).

For example, the regulator's report into the foreign exchange losses at NAB concluded that the firm's 'culture' was one of the root causes of the problem — 'bad news was not welcome'.[9] Similar comments were made in other cases, such as AIB and Barings. It is the social 'interactions' between people that cause problems in dysfunctional institutions.

In such cases, individuals are obviously at fault, either through their unethical actions or, more often, their lack of action in following through on suspicions of unethical behaviour — the 'it's not my job' mentality. Often, in these situations, fundamental policies and processes are circumvented (giving rise to 'process risk'), but it is the lack of strong management support for their own policies, usually in pursuit of profits, that legitimises individuals in 'breaking the rules'. If the 'tone' of the people at the top of an institution is wrong, its risk culture will be deficient.

A good example of how a deficient risk culture can destroy an institution is the case of Riggs Bank, a mid-sized financial institution headquartered in Washington, DC, which was fined $25m for 'money laundering' and was eventually swallowed up by PNC Bank in 2005. For most of its existence, Riggs Bank was 'plugged into' the US establishment, working closely with the CIA and occupying offices inside some US embassies. Riggs' management, feeling safe within the establishment, clearly broke new anti-money laundering laws in moving 'dirty money' around the world in the early 2000s. However, Riggs' management maintained that they were doing nothing wrong — they just failed to appreciate that the new rules applied to them as well.

Given that a case such as Riggs falls within the definition of people risk in Basel II, how should an ORM function

within a firm measure and manage its risk culture?

Changing the culture of any institution is not easy, even if management supports such a revolution. HR must, of course, be involved in changing a firm's culture, but they too may be part of the problem. In order to understand how to diagnose and remedy deficient organisational cultures, ORM professionals must understand the theories of organisational psychology and cooperate with experts in organisational change, such as HR, in finding and proposing ways forward.

Industry

Operational losses can occur across the whole financial services industry as a consequence of actions of individuals in various institutions, not necessarily colluding, but caught up in a rush to make profits in new markets.

Studies of empirical operational loss event data (including Moscadelli,[10] Dutta and Perry,[11] Dahen and Dionne[12] and Jobst[13]) which analysed both data collected in regulatory loss data collection exercises and in external loss databases (such as OPVantage), have found the largest concentration of losses, by severity, occurs in a small number of Basel II loss event types, namely clients, products and business practices (CPBP) and employee practices and workplace safety (EPWS).

It should be noted that the largest losses in these two categories tend to be fines levied on firms, in the first category (CPBP) for actions against clients, and the second (EPWS) against employees. The underlying causes of these losses, however, are not the regulatory or legal fines *per se*, but the actions of the individuals in the institutions that caused the fines to be levied, ie people risk.

An example of such fines is the $400m levied by the US Securities and Exchange Commission against the brokerage arm of Citigroup in April 2003. Citicorp was just one of ten firms fined a total of over $1.4bn for breaches related to 'undue influence of investment banking interests on securities research at brokerage firms'.[14] These fines, which were part of the fallout from the IPO scandal of the early 2000s, are examples of the 'low-frequency, high-severity' losses that firms are required to include in their assessment of operational risk capital under Basel II.

Fines of this magnitude are levied not because of the unethical/illegal activities of one individual, or a small group of individuals, or even a single institution, but because of the across-the-board failure of ethical standards in the industry (although not yet fully clear, it is already apparent that a similar breakdown in ethical standards has triggered the subprime crisis). Blame is spread across many firms to send a message to boards, executives and staff that such behaviour will not be tolerated in future — ie closing the door after the horse has bolted.

The theories of behavioural finance[15] show how 'financial bubbles' arise as a consequence of the so-called 'herding instinct'. As part of a 'herd', individuals can suspend their normal, ethical decision-making behaviour and, because 'everyone else is doing it', begin to act unethically. Likewise, at the institution level, normal risk management caution can be countered by references to changing industry practices, even industry structure — the 'new paradigm' argument.

It would be a brave operational risk

manager who would buck an industry-wide and seemingly profitable trend such as subprime securitisation. Nor is it obvious who should perform the vital role of sceptic in such circumstances, as traditional industry-level bodies, such as regulators and rating agencies, have proven to be slow to react to such problems, often disastrously.

Risk managers cannot be expected to act as industry regulators but there is, however, a forum in which industry-wide risks can be assessed from the perspective of a firm — scenario analysis. Firms, subject to an Advanced Measurement Approach under Basel II, are required to assess so-called 'business environment and controls factors', which would naturally include the sources of future profits and associated risks. If ORM managers are able to work with disciplines, such as strategic planning, to ensure that 'industry level' issues are raised and properly addressed during risk self-assessments and scenario analysis exercises, then such risks can be reported to senior management and the board for their attention. This does, however, require independent thinking and an understanding of behavioural finance.

Risk managers can also play a role in advising legislators in tackling industry-level issues by acting as expert witnesses when such topics are being discussed. The best way to achieve this is to develop credibility as a profession, through improved education and consistent practices.

DIFFICULT ROLE OF OPERATIONAL RISK MANAGERS

Unlike credit risk managers (through approvals) and market risk managers (through, for example, limits on 'Greeks'), operational risk managers cannot *directly* influence the level of risk in their firm. They are forced to act indirectly through influence rather than by direction.

This situation puts operational risk managers in a very difficult position within the organisation — they have lots of responsibility but little direct power. Of course, they can develop KRIs and embed them in the firm but they cannot direct the organisational changes that will ultimately impact upon such indicators.

For example, staff turnover is a widely used KRI that may give an indication that all is not right in the organisation, but the skills needed to identify the root causes (eg salary levels) lie outside of the ORM function (in the case of salaries with HR). For such a KRI, operational risk managers must actively seek the help of HR to identify the root causes of staff turnover and to encourage them to develop workable mitigation strategies to put to senior management for approval. Unfortunately, staff turnover is one of the easier KRIs to put in place, while other people risks, such as bullying, are not so tractable.

Operational risk managers in decentralised roles (ie part of the business line rather than the central risk function) have a particularly difficult path to tread. For example, a risk manager may, as part of an operational risk assessment exercise, be the first to detect possible illegal behaviour, such as suppression of critical reports or manipulation of profit figures. Who does he/she report this to? Obviously, business line management must be informed as quickly as possible, but if the issue is ignored or downplayed,

then what to do? As the risk manager reports to the same business management, his/her position will be delicate — doubly so if the business line is responsible for determining bonuses. This is by no means a hypothetical situation, as demonstrated in the NAB case, where market risk managers did report problems with the rogue traders' activities but were ignored by the business line; worse still they were bullied and abused.[9] (It should be noted that this whistle-blowing did not help the risk managers when the axe finally fell — they too were sacked.) Without a clear line of organisational responsibility back to a chief risk officer, or equivalent, and a clear set of rules of conduct, a risk manager will have nowhere to turn, if pressurised by business line managers and staff.

The ethical dilemma of risk managers *vis-à-vis* detecting illegal/unethical behaviour is similar to that of other professionals, such as internal auditors. The Professional Risk Managers' International Association (PRMIA) has developed standards of best practice, conduct and ethics for risk managers faced with such dilemmas,[16] which parallel a similar code of ethics developed by the Institute of Internal Auditors[17] (see Heaston and Cooper[18] for some of the difficulties of applying an ethics code in real situations). However, the profession of operational risk management is not yet fully developed in the financial sector, and boards and executives may not be aware of the need for risk managers to operate within a proper ethics framework. There is a need therefore not only to educate risk managers on their ethical responsibilities but also to communicate the need for clear ethical standards and independent operation to senior management. In practice, this education will have to be undertaken by risk managers themselves, further highlighting the need for acquiring high-level communication skills.

As Basel II requires that risk management functions be independently audited, a standard set of practices would also allow risk managers to be evaluated objectively as to their own ethical performance. Regardless of ethical issues, however, in many situations where potentially illegal issues are raised, operational risk managers will have to work with internal auditors to investigate evidence collected, particularly where forensic accounting skills are needed. There is a potential conflict of interest here in that the audit function may be called upon to support risk management — one of the functions that it audits — and a clear *modus operandi* will have to be developed to handle any conflicts that may arise.

When looking at the scope of people risk in the firm, it is obvious that operational risk professionals cannot 'go it alone' but must identify the disciplines (inside and outside of the firm) that will help them to bring all risks to the attention of management. This requires softer skills, such as influencing, rather than (or, more properly, in addition to) the quantitative skills traditionally associated with ORM.

SUMMARY

People risk is one of the greatest risks facing financial institutions and the fundamental cause of some of the largest operational risk losses experienced by financial institutions. Actions by individuals have been behind some of the low-frequency, high-severity losses

that must be actively managed by banks under new Basel II regulations.

It is however difficult to put a boundary around people risk, as it arises not only in the day-to-day operations of individual firms but also in unethical or even illegal activities across the entire industry.

This paper proposes a framework for identifying and classifying people risks and concludes that ORM functions must reach out to other disciplines, in particular HR, compliance and strategic planning, in order to effectively encompass the full breadth of people risk. To conform to the requirements placed upon them by Basel II, ORM professionals must also become familiar with disciplines such as Six Sigma, organisational psychology and behavioural finance, in order to help their firms manage people risk. Educators must also consider how to satisfy the needs of ORM professionals for acquiring such 'soft' skills.

Operational risk managers must recognise that they can see only one part (albeit a very important part) of what is usually a complex, confused picture, and they need to search out other professionals with whom they can cooperate to construct a 'full' picture of potential problems so that management can take action.

In summary, people risk is too broad a risk category to be managed by a single discipline, however well trained, and risk managers must cooperate with experts in other fields to tackle those risks that give rise to the industry's greatest operational losses.

References

1 Basel Committee on Banking Supervision (2004) 'International Convergence of Capital Measurement and Capital Standards — A Revised Framework', Bank for International Settlements, Basel, available at: http://www.bis.org/publ/bcbs128.htm (comprehensive version 2006 (accessed August 2008)).

2 Cruz, M. G. (2002) 'Modelling, Measuring and Hedging Operational Risk', Wiley, Chichester.

3 Blacker, K., Weinstein, B. and Mills, R. (2003) 'People risk and organisational culture', discussion paper, Henley Management College, available at: http://www.henley.reading.ac.uk/henleyres03.nsf/pages/hcri_discussion papers (accessed August 2008).

4 Zhang, P. G. (1995) 'Barings Bankruptcy and Financial Derivatives', World Scientific, New York.

5 McConnell, P. J. (1998) 'Barings: Development of a disaster', *International Journal of Project and Business Risk*, Vol. 2, No. 1, pp. 59–74.

6 McConnell, P. J. (2003) 'AIB/Allfirst — Development of another disaster', working paper, Henley Management College, available at: http://hmcweb.henleymc.ac.uk/elibrary/hwpr02.nsf/papers36C0168EBA45FC9E80/256CFC004FO316 (accessed August 2008).

7 McConnell, P. J. (2005) 'NAB — Learning from disaster', working paper, Henley Management College, available at: http://hmcweb.henleymc.ac.uk/elibrary/hwpr02.nsf/papers/B3BFC4DD3943D96380256FC6005A708F (accessed August 2008).

8 Société Générale (2008) 'Progress Report of the Special Committee of the Board of Directors of Société Générale', Société Générale, February, available at: http://www.sp.socgen.com/sdp/sdp.nsf/V3ID/6D44E7AEF3D68993C12573F700567904/$file/comiteSpecialFevrier08gb.pdf (accessed August 2008).

9 Australian Prudential Regulatory Authority (2004) 'Report into Irregular Currency Options Trading at the

National Australia Bank', Australian Prudential Regulatory Authority, March, available at: http://www.nabgroup.com/vgnmedia/downld/APRA report_24 march04.pdf (accessed August 2008).
10 Moscadelli, M. (2004) 'The modeling of operational risk: Experience with the analysis of the data collected by the Basel Committee', working paper 517, Bank of Italy, available at: http://www.bancaditalia.it/pubblicazioni/econo/temidi/td04/td517/terna_517.pdf (accessed August 2008).
11 Dutta, K. and Perry, J. (2006) 'A tale of tales: An empirical analysis of loss distribution models for estimating operational risk capital', working paper, Federal Reserve Bank of Boston, available at: http://www.bos.frb.org/economic/wp/wp2006/wp0613.htm (accessed August 2008).
12 Dahen, H. and Dionne, G. (2007) 'Scaling Models for the Severity and Frequency of External Operational Loss Data' HEC, Montreal, available at: http://neumann.hec.ca/gestiondesrisques/07-01.pdf (accessed August 2008).
13 Jobst, A. (2007) 'Constraints of consistent operational risk measurement and regulation: Data collection and loss reporting', working paper, International Monetary Fund, available at: http://www.inf.org/external/pubs/ft/wp/2007/wp07254.pdf (accessed August 2008).
14 Securities and Exchange Commission (SEC) (2003) 'Ten of nation's top investment firms settle enforcement actions involving conflicts of interest between research and investment banking', press release, SEC, Washington DC, 28th April, available at: http://www.sec.gov/news/press/2003-54.htm (accesssed August 2008).
15 Celati, L. (2004) 'The Dark Side of Risk Management: How People Frame Decisions in Financial Markets', Prentice Hall/Financial Times, London.
16 Professional Risk Managers' International Association (2008) 'Standards of best practice, conduct & ethics', available at: http://prmia.org/pdf/Conduct.pdf (accessed August 2008).
17 Institute of Internal Auditors (2008) 'Code of ethics', available at: http://www.theiia.org/guidance/standards-and-practices/professional-practices-framework/code-of-ethics/ (accessed August 2008).
18 Heaston, P. H. and Cooper, R. W. (1993) 'The ethical environment of the internal auditor — The ethical environment', *Internal Auditor*, June, pp. 18–23.