
Practice Papers

Monitoring the operational risk environment effectively

Received (in revised form): 11th December, 2007

David Breden

is Managing Director of HSBC Operational Risk Consultancy and the architect of OpRisk Modeller, a scenario-based commercial risk mapping tool developed by HSBC to meet the needs of the Basel II AMA quantification requirements. Previously he worked for NatWest for over 20 years in both England and Spain and developed and implemented an operational risk management system for the Spanish retail network. He has been involved in operational risk management since 1995 and is both a Fellow and a Director of the Institute of Operational Risk. He is a frequent speaker and writer on operational risk matters.

HSBC Operational Risk Consultancy, Level 16, 8 Canada Square, London E14 5HQ, UK
Tel: +44 (0) 20 7991 0599; Fax: +44 (0) 20 7991 4640; E-mail: david.breden@hsbc.com

Abstract This paper explores the current status of operational risk management practice in financial institutions. It begins by describing the features that distinguish operational risk from other types of risk. It then goes on to describe the key elements in today's market of a forward-looking, proactive, operational risk management framework.

Keywords: *understanding, proactive, forward-looking, preventative*

INTRODUCTION

It is a common theme in all risk management structures that one of the key elements of the risk management process is the monitoring of exposures. This is certainly the position reflected by the Basel Committee on Banking Supervision. In 2003, this body published a paper in which they outlined the basic principles that financial institutions should follow when constructing their operational risk management framework. Principle 5 of the document states that:

'Banks should implement a process to regularly monitor operational risk profiles

and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.'¹

It can be argued that the inclusion of this principle responds to a basic requirement of all risk management structures, but the characteristics of operational risk tend to make the monitoring of exposures to such risks more relevant than most other risk types. It is appropriate, therefore, to begin by considering the key features of operational risk that distinguish it from other types of risk:

- *Operational risk is highly context-dependent:* Operational risk is concerned with the risk of loss resulting from the failure of systems, processes and people and from external events. It is evident that all financial institutions have different processes for performing common tasks, all use different systems and all train their employees in different ways and, indeed, employ different individuals. External threats will vary with location and with the different levels of security deemed appropriate in each case. As a result it is difficult to apply lessons learnt by one institution to another organisation without an account of variations in the firm's context. An example of this might refer to the risk run by a securities firm that has purchased an automated straight-through dealing process that incorporates settlement and reconciliation. This business will find itself subject to a remote but significant risk of system failure that will prevent it from providing normal service to its clients. This can be compared with a traditional firm producing manual deal tickets and settling and reconciling trades independently and which is exposed to a high number of losses due to manual errors — each of which will in normal circumstances have a limited impact on the firm. The two firms provide identical services but their different practices produce diametrically distinct risk profiles.

If one takes this characteristic of operational risk to the next level, one will realise that similar variations occur hour by hour in one's business as circumstances change within units and the performance of individuals fluctuates depending on personal circumstances, tiredness and varying levels of concentration and experience. All unit

managers must control and monitor this risk as a matter of course — if they fail to do so, they run the risk of increased error rates due to entrusting vital transactions to individuals who do not have the necessary experience or frame of mind to complete their assigned task successfully.

- *There is no defined portfolio of operational risks:* Regrettably, financial institutions are subject to a changing array of threats from both internal and external sources as products, systems and processes evolve. The creation of a new delivery channel such as internet banking has given rise to a new set of risks that were unsuspected in the past. Equally, fraudsters and other criminal elements devote much time and effort to the creation of new ways of attacking financial institutions and obliging the industry to be permanently alert to ways of combating these threats.
- *There is no defined risk or portfolio size:* When considering an individual credit risk or a portfolio of such risks, it is easy to identify the amount of exposure with which the lender is faced. The same cannot be said about operational risk, where it is impossible to state how great an institution's exposure might be as a result of an internal fraud or systems failure. Here the amount of loss will depend on the underlying circumstances of the event. This feature obliges the firm to understand the factors that might influence the potential size of loss and monitor these factors in an attempt to identify particularly threatening situations.

Each of these factors highlights the need for effective monitoring of the operational risk environment if an institution is to protect itself adequately

against extreme operational risks. Concern is likely to centre on the potential extreme event to which the organisation is known to be exposed, but is yet to experience.

Before considering the main mechanisms for monitoring the operational risk environment it is necessary to consider the foundations on which the monitoring framework must be based.

THE FOUNDATIONS OF AN EFFECTIVE MONITORING FRAMEWORK

Before the risk environment can be monitored, the board and senior management of the institution need to define the type of environment that the operational risk management team is required to monitor. It is a common misconception that the operational risk manager exists to prevent operational risk, but this is not the case. Operational risk is present in everything we do and can only be avoided if the organisation closes its doors and ceases trading. Just as any bank that wishes to make profits from lending must accept a degree of credit loss, so an institution must accept that operational losses will always occur. It is of course possible to introduce multiple levels of control, repeated checks and balances and higher security levels, but the result of such action will be to increase cost levels, slow down processing speeds and ultimately impact negatively on the bottom line of the profit and loss account. As a result, the board needs to define where the firm is to sit in the spectrum between a business with low controls that seeks to maximise short-term profit and accepts that it may be subject to frequent and significant operational losses (and the possible

displeasure of the regulatory authorities) and a highly-controlled environment where repeated checks and controls lead to low service levels and low profits.

The UK Financial Services Authority has introduced a requirement that certain insurance firms define their level of tolerance or appetite for operational risk — but the definition or description of risk tolerance levels can be considered a valuable practice for all financial institutions:

‘When establishing and maintaining its business plan and prudential risk management systems, a firm must document . . . a description of its policies towards market, credit . . . liquidity, operational, insurance and group risk . . . including its appetite or tolerance for these risks.’²

This apparently simple requirement will in fact involve the firm in some reflection. The risk appetite will undoubtedly vary according to the type of risk that is under consideration. It is clear that most firms have very low tolerance levels for cases of internal fraud, where the extent of the impact is largely irrelevant in deciding on action to be taken against the perpetrator. As a contrast, other risks will be accepted as a cost of doing business, always provided that losses are contained within acceptable limits. So, any firm that issues credit cards will expect to be subject to a degree of claims and will set budgets for such losses that will be included in the overall pricing matrix.

Risk tolerance will also vary with the firm’s situation. As an example, a firm that has recently acquired a new business in a new and unfamiliar trading area will probably wish to restrict routine

operational losses to avoid market suspicion that they lack the knowledge and experience to control their new acquisition properly.

To be able to define tolerance levels, the business will need to have a clear picture — as far as is possible — of the risks that it faces. This will oblige the firm to carry out a comprehensive risk identification and assessment exercise. This will need to identify not only the areas where the firm knows that it has exposure, but also areas where processes or systems are weak, and mistakes or external attacks are possible. It is likely that it will be those risks of which the board is unaware that will prove the most unwelcome and the most likely to lead to the need to amend profit forecasts or report lower than expected results.

To identify latent risks within operations and support functions, the firm will not be able to satisfy itself with a high-level review of exposures, but will need to harness the knowledge of the staff with ground-level knowledge of the organisation's systems, processes, people and exposure to external threats. To do this it may choose to conduct detailed facilitated workshops or may be able to gather the required information through a risk self-assessment process. Whichever methodology is chosen, the firm will need to understand the nature of the risks it faces, the likelihood of those risks and the potential impact of those risks, both in normal and extreme circumstances. Finally, it will need to understand what control structures are in place and how effective these structures are in preventing loss.

Once a clear picture of exposures is gained, it will be possible to grade the risks present, set tolerance levels and

define actions to be taken in the event that risks exceed desired tolerance levels. This can be done by introducing additional controls, transferring the risk or avoiding the risk. Of course, this decision would be informed by a full cost-benefit analysis, whereby the firm evaluates the cost of the proposed additional control or transfer framework against the enhanced risk experience which should reduce loss exposures in the future.

All of this will be encapsulated in policies and procedures and enforced around the business.

With this foundation in place the organisation is now in a position to consider how to monitor the environment going forward.

TECHNIQUES FOR MONITORING THE OPERATIONAL RISK ENVIRONMENT

Risk self-assessment

This paper previously highlighted the fact that the operational risk environment is subject to continual change as new external threats emerge and the institution's own processes, systems and people change. This clearly implies that the firm cannot be satisfied with a one-off risk assessment. Any new product, system or process should be subject to regular reviews of the environment *in addition to* the initial operational risk assessment.

For a large organisation it is unlikely that it will be practical to organise regular workshops. As such, most large firms have developed a self-assessment methodology where key business representatives indicate how their risk profile changes. The process will identify

new and increased risks as well as reflecting enhancements to the control framework introduced to address those risks that have been identified as exceeding tolerance levels.

It should be noted that this process will be likely to require an oversight and challenge process that is led and supported by senior management to ensure that the process is conducted with rigour and does not become a simple box-ticking exercise.

The process will continue to identify risks that exceed tolerance levels and a process will need to be established that will require business units to suggest enhanced controls or mitigation and will set out timeframes for these enhancements to be carried out while identifying the individual responsible for putting the enhancements in place.

The technique is aimed at ensuring that the firm is monitoring the variations in its risk environment and taking appropriate action in the light of these variations.

Loss database

One of the earliest tools generally introduced by firms to monitor the risk environment is a loss database. This commonsense measure responds to a basic instinct for self-preservation among risk managers, as it is to be expected that board members may accept an unexpected loss the first time that it occurs, but are unlikely to be so understanding if similar losses recur without apparent effective action from risk management or from the business unit.

Most firms will therefore have a process in place to collect information on losses that have occurred within the organisation and will seek to gather data

that will enable them, not only to produce statistics showing the impact of operational risk, but also data that will enable the risk management function to ensure that the business unit takes the necessary action to introduce preventative measures thereby ensuring losses that exceed defined tolerance levels do not recur.

The loss data collected in the database will provide the firm with information on the sort of losses that occur within the organisation, and many firms will supplement this data by recording 'near misses' and errors to illustrate areas that may give rise to losses in the future if no effective action is taken. That said, the loss database will provide little or no information on low-probability, high-impact losses which will be the events that the business will be most eager to avoid and which by definition the business is least likely to have suffered.

To fill this void, firms will also need to examine the losses that have occurred and consider whether these losses, under different circumstances, might result in a substantially greater loss. Such investigation will involve the firm identifying the key parameters that drive the loss and then subjecting these parameters to stress. If the event is then capable of producing losses that exceed tolerance levels, the firm would be wise to put in place measures to prevent the larger event crystallising at some time in the future — providing that the cost of such measures is not prohibitive when compared with the benefits gained. Firms will also look to publicly reported events, or industry or public loss databases, to gather data from events that happen to competitors. As previously mentioned, operational risk is

context-dependent. As such, it should not be assumed that such events are relevant. Nonetheless, these events can be analysed to see whether or not they do provide valuable data on potential exposures. If an exposure exists then action can be taken to learn a lesson from the external experience and preventative measures can be put in place before the organisation suffers a loss.

Intelligent use of the loss database, enriched by stress tests on internal events and scenarios based on external events, will have the result that the loss database will not only monitor the losses that have been suffered and allow the organisation to take reactive action, but will also permit it to move proactively to prevent losses that may impact on business in the future.

Key risk indicators

Many fields of activity have developed measures to signal an increased level of risk in the environment: a red alert may be declared if enemy troops are seen massing on a country's border; likewise an alert will be sounded in a nuclear power station if the core temperature exceeds prudential limits. Many financial institutions have sought to replicate these methodologies by developing key risk indicators (KRIs). Such indicators will be based on identifying measurable elements of a firm's activity that can be seen to have a direct correlation with levels of risk in the business. It is not a case of merely collecting statistics to measure performance levels, but rather of monitoring those statistics which indicate whether the business is becoming more or less risky. A frequent indicator of risk could be the volume of errors, complaints or unreconciled items

seen in the business. All of these factors are linked to basic business failings that would tend to show failings in the quality of basic processes that could be linked to the probability of higher volumes of loss. In other cases, identifying links between a statistical indicator and risk levels is more difficult, and will involve the business in clearly understanding the factors that drive particular losses.

An example of this can be seen if looking to identify KRIs to monitor the risk environment in an overseas payment business. In general terms, losses connected with such activity are determined by certain variables. These include:

- *The amount of the payment:* It is unlikely that significant loss will be suffered if a payment of US\$50 goes astray. If a mistake is made with a payment of US\$50m, however, then any interest or damages claim is likely to be of much greater severity.
- *The underlying volatility of the currency pair concerned:* If an error is made in performing a payment, then when it becomes necessary to unwind the transaction, the extent of the loss will be influenced by wide fluctuations between the currencies concerned. Wide fluctuations will obviously result in significant loss when the movement is against the firm.
- *Time taken to resolve the event:* Interest is likely to be one of the main elements in any payment to resolve an operational error. The longer the period required to resolve the issue, the greater the potential interest claim.
- *The identity and location of the counterparty:* Certain banks may have liquidity issues that make it convenient for them to retain

funds paid to them in error for a lengthy period while they resolve matters. In other cases, a lack of hard currency or the presence of exchange controls in a country may lead to delays that will increase the level of interest claims.

Looking at this example, one might conclude that appropriate KRIs include:

- the number of payments above a monetary figure that would be considered significant by the firm;
- the number of transactions that are conducted in currency pairs where volatility exceeds a predefined level;
- the number of transactions that are conducted with countries or counterparties where payment difficulties may be present;
- the number of unreconciled items outstanding on internal suspense accounts that have been outstanding for longer than x days.

If it becomes evident that more large payments are being made in volatile currencies or to difficult destinations, then the firm will be able to introduce additional controls to apply more rigorous checks to payments with these characteristics.

There are certain basic rules to bear in mind when creating KRIs:

- There should not be too many KRIs, as monitoring becomes onerous and may lead to disenchantment in the business unit that is gathering data.
- KRIs should be easy to gather, and should preferably be produced automatically by the system.
- The measure should be a proven indicator of changing levels of risk.
- It is helpful to create a basic threshold and

an action threshold for each KRI. When limits are breached, all parties should understand what action they should take to address the perceived increase in risk levels. Such action should be decided in advance and implemented automatically in a similar fashion to a call to action stations in a military environment.

- KRIs must be validated to demonstrate that a KRI movement is truly reflective of a changed level of risk.

The objective of KRIs is to alert the business to an increased level of risk so that it can react immediately and address the problem before it can cause loss to the business. A basic problem with many KRIs is that they are collected after the event and consequently advise firms that their risk increased in a business unit last month. Such information may come too late to allow risk management to control the situation, so it is interesting to note the evolution of software in certain areas that allows firms to identify in real-time suspicious transactions from a money-laundering perspective or transactions where key data are missing and where cut-off times are approaching. Such software allows high-risk transactions to be identified and corrected, and it is to be hoped that further developments will lead to software applications capable of providing real-time monitoring of risk levels in the environment.

Monitoring control effectiveness

In many cases, loss due to operational risk is caused by control failure where a series of individual controls is improperly implemented leading to loss. The effectiveness of control procedures is often the realm of internal audit, or in some cases compliance, and the

operational risk manager should be aware of the contents of internal audit reports and compliance reviews, especially insofar as they indicate the degree to which the business unit concerned is effective in following defined control structures. If a business unit is identified as being ineffective in implementing control structures, then it is likely that the risk of loss for that unit is higher than in a unit which implements controls effectively. This should signal a need for action within the business to address the problem in the business unit before the lax observation of control structures gives rise to increased levels of loss.

In some cases, businesses will also use a control self-assessment tool to remind staff in a diverse organisation of the required standards of control and will require the business units to certify compliance with these standards. Where shortcomings are identified, these can be rectified by the development of an action plan with a clear assignment of responsibilities and the definition of expected completion times. This methodology may be effective in geographically diverse, rules-based organisations.

The reporting structure

An essential final component of the monitoring process is to ensure that key aspects of the risk environment are communicated to all interested parties. This does not mean simply submitting statistical reports to senior management and the board (although this will undoubtedly be necessary) but also includes communicating relevant information to the business unit, to enable business management to address areas of concern promptly.

There is also a need to create channels that will allow the business units to raise concerns and report issues promptly up the line, with the knowledge that these concerns will be evaluated and appropriate action taken based on perceived levels of risk.

THE WAY FORWARD

The purpose of monitoring the risk environment is not to eliminate risk. As already indicated, it is impossible to eradicate operational risk from any active business. The aim in monitoring the operational risk environment is to avoid the high-impact risks that will damage the business and may threaten its continued independent existence. If this is the objective of the monitoring activity, then the organisation cannot afford to be reactive in the management of operational risk. Quality tools are needed that are capable of predicting areas of increasing exposure so that the business can proactively manage these exposures and prevent the crystallisation of potential extreme risks that have previously been described. This will require a real understanding of the risks being faced, and the factors that may determine the eventual size of loss if the risk materialises. These factors can then be monitored and action taken when danger threatens.

Unfortunately the operational risk manager is often seen as either wishing to introduce additional uneconomic controls to prevent loss, or as the administrator of a database and of other statistical tools necessary to produce reports that do not add value to the business. By developing procedures that proactively identify areas of increasing and significant exposure, and ensuring that these areas are addressed promptly

by the business units that own the risk, the operational risk manager can in reality help the firm manage and avoid the potentially fatal unexpected event, demonstrating a clear contribution to the ongoing health of the organisation.

NOTE

The views expressed in this paper are the author's personal views and do not necessarily represent the views of the HSBC Group.

References

- 1 Basel Committee on Banking Supervision (2003) 'Sound practices for the management and supervision of operational risk', available at: <http://www.bis.org/publ/bcbs96.pdf?noframes=1> (accessed 7th January, 2008).
- 2 FSA (2007) Full Handbook 'Senior Management Arrangements, Systems and Controls', SYSC 14.1.19 – 14.1.19.2, available at: <http://fsahandbook.info/FSA/html/handbook/SYSC> (accessed 7th January, 2008).

Copyright of *Journal of Risk Management in Financial Institutions* is the property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.