Being Clear About Risk: Defining Who Is Responsible For What

Dr Dominic Cooper C. Psychol AFBPsS FIOSH RSP
BSMS Inc, Franklin, IN 46131, USA

Introduction

Enterprise-wide risk management is a major concern to financial institutions as illustrated by the near-collapse of the hedge fund Long-Term Capital Management in September 1999. In essence, enterprise risk refers to issues arising from any number of unpredictable internal and external events that will affect the financial well being of the institution. In practice this requires the application of risk management techniques across the entire spectrum of an organisation's activities to ensure any processes that *potentially* could lead to losses are identified, assessed and controlled. To bring about a well-managed business, high returns and strong shareholder value, it is imperative that integrated approaches that focus on the interaction between credit risk, market risk and operational risk are taken so that the full extent of exposure arising from any one particular risk can be identified.

Credit Risk

Credit Risk refers to 'the risk that a counterparty will fail to perform its obligations'. The degree of exposure is usually measured as the '*sum of the replacement cost of the position, plus an estimate of the potential future exposure from the instrument due to market changes'*, where the replacement cost is equal to current market prices, or estimates of the present value of future payments required for each contract, given current market conditions. Credit analysts need to evaluate both settlement and pre-settlement credit risk at customer level across all products. Although loans form the largest proportion of credit risk, other types of financial instruments such as interbank transactions, swaps, bonds, equities, options and transaction settlements also pose credit risks. The measurement of credit risk should account for the specific nature of the credit and the associated contractual and financial conditions; the exposure profile until maturity in relation to potential market movements and the existence, quality and effectiveness of collateral or guarantees. This can perhaps best be achieved by ensuring that current information is available pertaining to [1] the financial position of the counterparty; [2] compliance of credits with existing covenants; [3] the use to which credits are put; [4] levels of debt servicing; and [5] that levels of collateral are aligned with a counterparty's credit line. The degree of exposure to credit risks will also be determined by the particular settlement arrangements, and include factors such as the settlement timing, the finality of the payment and the role of third parties such as intermediaries and clearing houses. Perhaps the largest source of credit risk emanates from high concentrations in particular markets, which arises from strategic decision-making (i.e. the board) to attain a leadership position or an attempt to diversify income streams. Importantly, this illustrates the interactive nature of credit and operational risk (see below), reinforcing the need to adopt an integrated approach to enterprise risk.

Who bears responsibility for identifying credits risk exposures?

Given the various instruments / markets / products and processes involved in the assessment of credit risk, it is inevitable that many disparate functions are involved. The could include credit analyses functions, credit approval functions, lead underwriters, traders, risk managers, business managers, etc. This fact alone highlights the need for an overarching integrative credit risk process, particularly as anyone counterparty may have been granted various forms of credit in different areas of the organisation. Thus, creating a management

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

information system that facilitates the sharing of information across these disparate functions is an important first step to assessing the degree of credit risk exposure. Without this, risks cannot be netted across different trading books and markets, and neither can the impact of external events over the entire exposure be fully assessed.

Market Risk

Financial institutions have always faced the risk of losses in on and off-balance-sheet positions arising from undesirable market movements. The risks arising from adverse movements in the level or volatility of market prices of interest rate instruments, equities, commodities and currencies are commonly termed market risk. Market risk is usually measured as the Value-at-Risk (VAR) i.e., time-series models of the distributions of portfolio returns. This is often determined by an evaluation of the potential gain/loss in a position / portfolio that is associated with a price movement at a given probability level (e.g. 99%) over a specified time horizon, mitigated by the institutions ability to take the appropriate action to reduce its loss. VAR 'backtesting' should be conducted on a daily basis to compare original estimates against actual daily changes in a given portfolio value. Backtests attempt to determine if an organisations 99th percentile risk measure actually covers 99% of the institutions trading outcomes. Typically backtesting results are interpreted within three colour coded categories: Green (0-4 exceptions, out of 250 observations) which indicates the risk model is reasonably accurate and represents no real problems; Yellow (5-9 exceptions) which indicates that some problems exist and that the modelling assumptions need to be re-examined; and Red (10 or more exceptions) which indicates that the models assumptions are wholly inaccurate and warrant serious attention. However, because VAR models do not provide a complete picture of the organisations risk exposure to extreme events, it is also necessary to conduct stress-testing that gauges how vulnerable an organisations portfolio is to plausible, but exceptional events should they take place. The output from such models allows risk managers, senior managers and business-unit managers to set limits on positions, determine levels of capital charges on traders and trading units and further test risk managers modelling assumptions.

Operational Risks

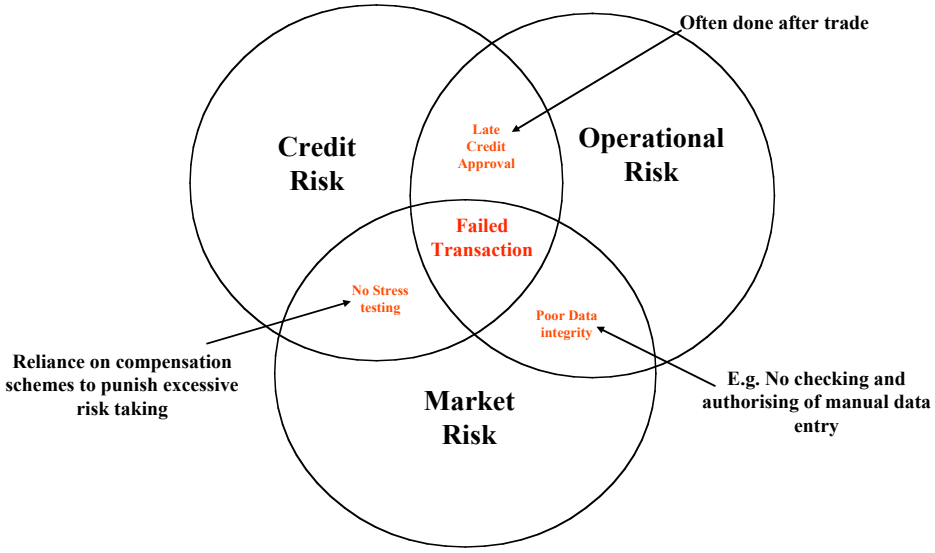
Both credit and market risk is underpinned by a strong human element (i.e. a need for people to follow procedures, engage in particular activities, etc.). This is usually referred to as Operational Risk which primarily refers to breakdowns in internal control systems and corporate governance that can lead to financial losses through error, fraud or failure to perform in a timely manner or cause the interests of the bank to be compromised in some other way, for example, by its dealers, lending officers or other staff exceeding their authority or conducting business in an unethical or risky manner. Although fraud is a major issue, it is relatively infrequent in contrast to issues of human error and failure to perform in a particular manner. Very often the individual losses incurred from these two factors are quite small, but over the course of a year can increment to a significant amount. Figure one illustrates how such operational risks can link with credit and market risk resulting in the high possibility of a failed transaction.

In this scenario, due to staff shortages in the front office combined with a lack of readily available data regarding the percentage of credit limits already utilised, counterparty credit approval was undertaken after trade capture had taken place. Similarly, the integrity of the manually entered data used to determine pricing models was also not checked by finance prior to release because the authorised person was attending a meeting. Due to conceptual problems with the notion of stress testing, a decision had previously been made at senior

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

management level to rely on the use of compensation packages (e.g. annual bonuses) to punish excessive risk-taking. In combination, these three operational risks give rise to the very real possibility of a failed transaction. Again, this scenario reinforces the need to adopt an integrative approach to all three types of risk.

Figure one: Interactions between Operational, Credit & Market Risks



Identifying Operational Risks

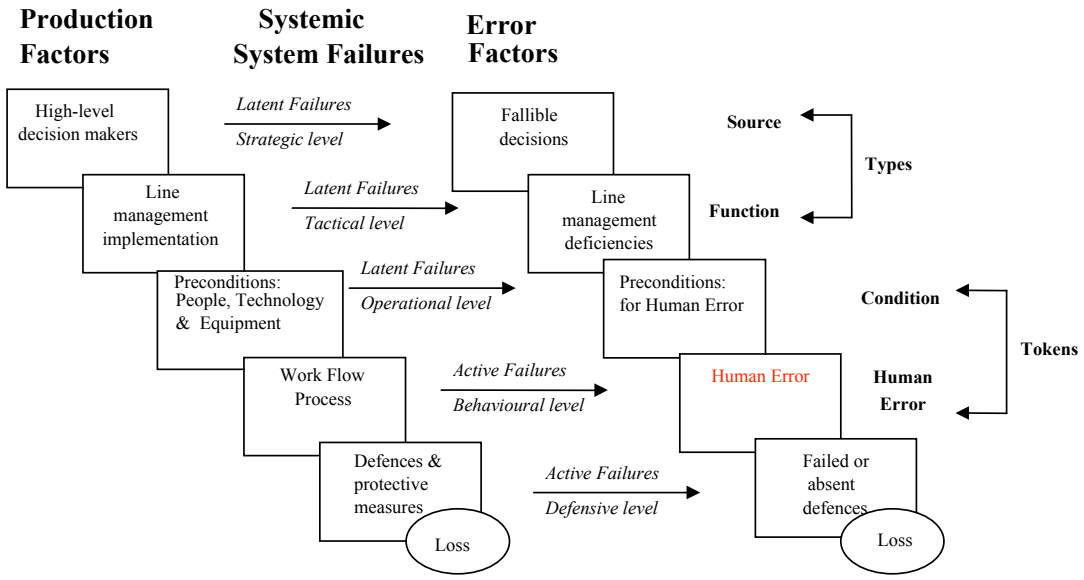
Eliminating operational risks offers a way to reduce potential losses and also improve the operational effectiveness and efficiency of the institution. After Reason (1990), figure two provides a useful framework for identifying how, and at what organisational level, operational risks could be introduced into a company. The framework consists of five contributory factors common to all forms of production systems. Each element represents a key component where systemic system failures, can and do occur, and what the common operational risks factors associated with each of the key components are.

Latent & Active Failures

When considering the human contribution to systemic system failures it is necessary to make the distinction between latent and active failures: Latent failures lie dormant for a period of time and their consequences are not felt immediately, whereas the consequences for an active failure are immediately apparent. Latent failures tend to be associated with those activities that are removed both in time and space from 'front-line' operational activities. Conversely, active failures tend to be associated with the performance of those involved in front-line operations. Whereas latent failures increase the potential for loss across a broad spectrum of activities, over a much greater period of time, active failures tend to be constrained to one type of activity at a particular moment in time. Importantly, latent failures significantly increase the likelihood of active failures occurring, therefore it is vital that they are found and eliminated.

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

Figure one: A Strategic Framework for Identifying Operational Risks



Operational Risk Sources

The sources of operational risks can be characterised as either Failure Types or Failure Tokens. Failure types are related to deficiencies in managerial and organisational factors (e.g. a lack of a risk assessment policy and no internal audit schedule), whereas Failure Tokens refer to unsatisfactory conditions related to technology (e.g. no tolerance levels set for direct market feeds), equipment (e.g. lack of software compatibility) and people (e.g. no systematic selection process), and individual actions during operations at the 'coal-face' (e.g. failure to sign off, 'off market trades'). Again, the most effective method of reducing operational risk is to identify and neutralise the failure types rather than failure tokens as this focuses on the early stages of the development of operational risks.

Strategic Level: High-level decision making.

The first key component refers to high-level decision making at the strategic level. These include the architects and high level managers of a system. The decision-makers set the appropriate goals for the system, in response to inputs from the wider external market and regulatory environment, and also provide the resources for goal-achievement, whether it be money, equipment, people, or time. Their aim is to deploy these resources in the most efficient and timely manner to maximise productivity and profits. Utilising the example in figure one, the senior management team had made a decision to use compensations schemes to avoid excessive risk taking (i.e. behavioural level) in the front office in lieu of stress-testing as they had conceptual difficulties about the use of such models because they are not typically associated with probability testing.

Tactical Level: Line-management implementation

It is usually line-managers who implement the policies and instructions emanating from the high-level decision-makers. Each of these, however, will approach their task in a slightly different manner, dependent upon their management style, their reinforcement history and their perceptions of how important the decision / instruction is in relation to their other duties. In the above example, line management implementation of the data integrity cross-checking and authorisation process did not take place simply because the responsible person forgot to arrange a suitable alternative while attending a meeting.

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

Operational Level: Preconditions for Operational Risk

The preconditions for introducing operational risk are primarily related to people, technology and equipment. These are latent states that create the potential for human error. The exact nature and severity of any errors will be dependent upon the tasks being performed, the situational influences and the presence of operational risks. Each of these latter factors can contribute to a large number of errors, depending upon the prevailing circumstances. Technology and equipment preconditions tend to be related to IT hardware, Information systems and procurement systems. People issues tend to be related to human resources in terms of the recruitment, selection, placement and retention of employees, their training, and their reward packages. In the above scenario, both staff shortages and the lack of real-time availability of data relating to the percentage of credit limits already utilised by the counterparty contributed to the late credit party approval.

Behavioural Level: Human Error

When something goes wrong it is usually labelled as Human Error, although in reality the cause of the error is often due to a lack of training or the required resources are not available, or people are being rewarded in some way for not doing something the way that the company intends. Within this strategic framework, Human Error is concerned with people's behaviour that induces active failures, where the consequences are far more immediately apparent, than latent failures. Errors at this level tend to interact with the risks associated with the latent failures induced at the strategic, tactical and operational levels of the organisation, usually resulting in the risks being realised. Human Error is defined as the '*failure of planned actions to achieve their desired ends'* (Reason, 1990). However, there are a number of different classifications of human error, each of which has different causes. Actions may fail to achieve goals because of:

- *Failures in Training.* Human errors often occur because people [a] do not know what to do; or [b] they do not know how to do something. A lack of training is a common cause of error.

- *Failures in execution.* These can be related to 'Slips' where there is attentional/perceptual failures during a largely automatic task in familiar surroundings, and a distraction in the immediate vicinity (e.g. errors in manual data entry); or 'Lapses' which are memory failures primarily caused by cognitive overload (e.g. processing too much information at any one time). Slips are largely overt and observable whereas Lapses are internal and therefore not observable.

- *Failures in planning.* This refers to people following a faulty plan that is inadequate for achieving its intended goal. These errors are termed 'Mistakes' and generally involve a mismatch between the prior intention and the intended consequences. Mistakes can be Rule based or Knowledge based. Rule-based mistakes refer to the failure to follow or apply a good rule or applying a bad or poor rule. Knowledge-based mistakes refer to instant problem-solving, when no pre-programmed solutions or rules are available (much like a traders day to day environment). Mistakes generally constitute a bigger risk than slips or lapses, but are also harder to detect.

- *Failures in control.* This refers to those deliberate or unintentional violations that are deviations from standard operating procedures that may be determined by either

☎ +1 (317) 736 8980
e-mail: **dom@bloomington.in.us** website**: www.bsafe.net**

organisational (e.g. competing priorities) or individual (e.g. personality, mood, etc.) factors. In the above scenario, for example, integrity checking of data was overlooked because of the need for the finance person to attend a meeting. Similarly, undertaking credit approvals after the event unnecessarily increased credit risk. *Routine violations* involve following the path of least effort or taking short cuts. These type of violations quickly become habitual if the consequences for taking the short cut is perceived to be rewarding (e.g. saves time and gets the job done) each time they engage in the behaviour. *Optimising violations* refer to thrill seeking while still achieving the original goal. Traders setting their own targets that are twice those set by their manager provide an example of this, as goal-achievement will usually require an increase in the traders risk-taking behaviour. *Necessary violations* are those perceived to be essential just to get the job done. In the above scenario, both the failures to obtain credit approval until after the event, and the release of poor integrity data could fall into this category. Organisational failings (e.g. staff shortages), and / or the desire to make the job easier provoke such violations. These two factors often lead to this type of violation becoming a habitual or routine violation.

Defensive Level: Failed or Absent Defences

The failure of a company's defences is perhaps one of the greatest sources of operational risks. Organisational defences are generally put in place to minimise losses should a risk be realised. Familiar examples of defences include internal and external audits, computer-based restrictions on trading limits, Straight Through Processing (STP), and the segregation of trading and settlement functions. Such defences may be absent as illustrated by the lack of stress testing in the above scenario (caused by strategic decision making); Existing defences may be breached, again as illustrated by the lack data scrubbing checks (caused by line-management implementation at the tactical level); or defences may be bypassed, as illustrated by the lack of credit approval checks (caused by the traders violations at the behavioural level).

Relationships between levels.

It is important to recognise that the relationships between each of these contributory levels are many-to-many. Latent failures can abound within a company's management systems at the strategic, tactical and operational levels, and can be introduced at any moment in time. They can lie dormant for a number of years before they combine with an active failure to penetrate the systems many layers of defences. Latent failures primarily emanate from decisions made at the strategic, tactical and operational levels and serve to create operational risks within individual workplaces. Active failures caused by human error at the behavioural level and failed or absent defences at the defensive level often provide the triggering event where the operational risks created by the latent failures are realised. Using Applied Behavioural Analytic tools, it is relatively simple to work back from each of these undesired behaviours to identify the factors that led to the undesired behaviour, and the factors maintaining such undesired behaviours. Once these are identified, further investigations can pinpoint weaknesses in the associated management systems and where these reside within the operational risk model above. In this way the interaction between human error and management systems can be identified and addressed. One major advantage of this approach is that such analyses can be conducted as soon as the error / undesired behaviour is identified as such (assuming people have the requisite knowledge).

☎ +1 (317) 736 8980
e-mail: **dom@bloomington.in.us** website: **www.bsafe.net**

Assessing Risks

Risk is a multifaceted concept that in essence refers to 'the possibility of loss' presented by the existence of perceived threats within a given situation. The purpose of risk assessment therefore is '*to make sure losses are avoided'*. A number of methods for assessing risk are available which include Business Process Mapping (BPM), Risk Questionnaires, Risk Adjusted Return on Capital (RAROC), Value at Risk (VAR) and Stress testing. The details of each of these procedures are beyond the scope of this paper. However, it must be recognised that the *outcome is much more important than the actual procedure used*.

Risk Assessment components

The critical components of the risk construct are [a] potential losses (i.e. identification); [b] the significance of those losses (i.e. severity or effect) and [c] the certainty of those losses (i.e. likelihood). This breakdown provides a practical means of subjectively assessing and quantifying risks. Once the existence of perceived threats have been identified, we can use severity and likelihood ratings to produce a risk rating (i.e. severity X likelihood = risk rating). The frequency with which a perceived threat is present in the working environment can also be used to weight the derived risk ratings to assist further in the prioritisation of remedial actions.

Risk Assessment Process

In my view, it is better to keep the process as simple as possible, so that all levels of personnel can undertake risk assessments in a consistent manner across the institution as a whole. The risk assessment process is perhaps best tackled in the first instance by dividing the work into manageable categories (e.g. Front, middle and back office operations, Human resources, IT, New Products, Finance, Outsourcing, etc.). The second step is to identify the areas of work where losses could occur within each of these discrete categories (e.g. Pricing, Trade Capture, Trade Processing and Transaction Management in the trading division). Aspects to consider include:

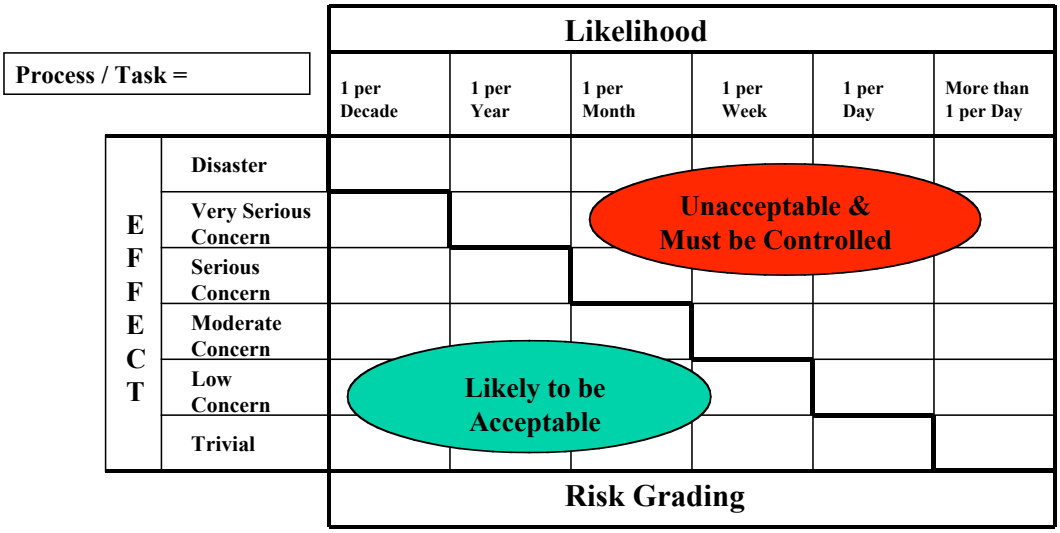
- The type of activity or work being carried out
- Whether the task activity is of a short or long duration
- Who undertakes the work or activity
- What technology, equipment and materials are involved
- What overlaps are there with other functions, departments, business units, product lines, etc.
- Where the work or activity takes place
- When a particular activity takes place.
- How the work is carried out
- How many people are involved
- The potential for management system failures
- The potential for technical failures
- The potential for human error failures
- What the consequences would be of a failure in any area of the activity

There is also a strong case for examining the associated organisational policies or practices that have been identified as being associated with the creation of risks, or reinforcement of risk-taking behaviour.

The third step is to evaluate each of the risks identified and grade them by multiplying the likelihood of an event occurring. Figure three provides a simple risk assessment matrix that also takes into account the frequency with which a risk may be realized.

☎ +1 (317) 736 8980
e-mail: **dom@bloomington.in.us** website**: www.bsafe.net**

Figure three: Simple Risk Assessment Matrix



A perusal of the matrix reveals that risk events will take place within two extremes: that of a low frequency event with a high impact, and that of a high frequency event with a low impact. For practical purposes any risk grading that falls into the upper half of the matrix is unacceptable and must be controlled. Those falling into the lower half of the matrix are likely to be acceptable and can be ignored until such time as the upper half have been addressed. Attention can then be turned to those risks falling in the lower half.

Determining the severity or effect at each level might best be achieved by arbitrarily assigning a monetary loss value to each. At the very least this will provide a reasonable degree of objectivity and consistency across disparate departments and functions when conducting risk assessments. This also helps to ensure consistency of reporting of risk exposure levels to the senior management team / board.

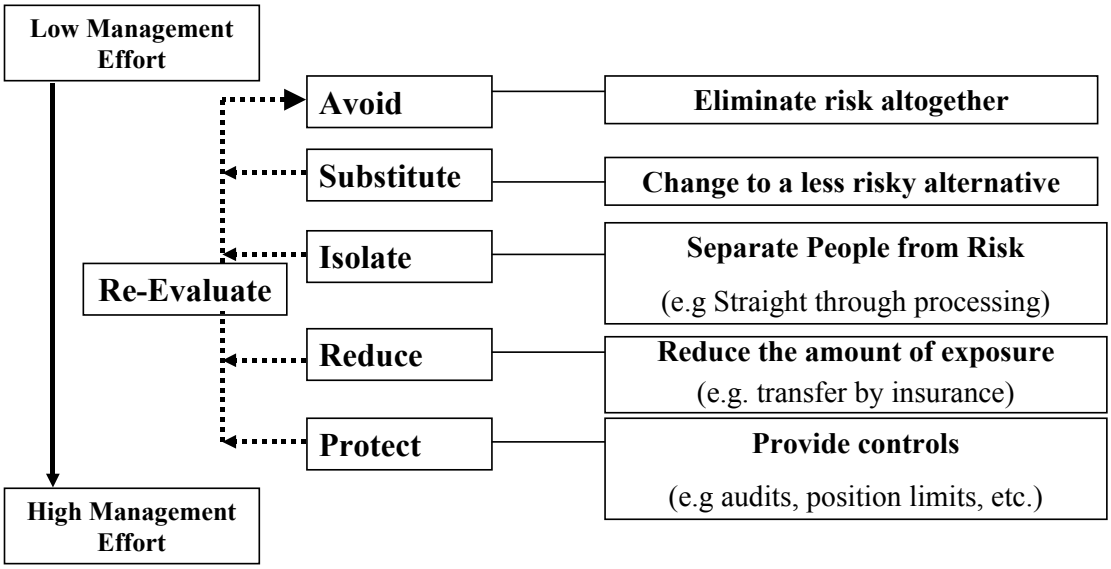
Prepare Risk Control Action Plans

Having identified those risks requiring control measures, it is necessary to determine *what* control measures will reduce the risk to an acceptable level. In principle there are two strategies that can be adopted. The first is to reduce the likelihood of the event recurring, the second is to reduce the severity or effect of the risk. If both strategies can be used to control a particular risk, so much the better. Choosing and *implementing* the most appropriate risk control measure will determine the success or failure of the risk reduction effort. Unfortunately, regardless of the size and nature of organisations it is all too common for risks to be identified without the appropriate remedial actions being taken. Which control measure(s) to put in place, however, is dependent upon the type of activity that has been assessed and how thoroughly the activity has been assessed.

Although risk control measures must satisfy the needs of the organisation and the needs of the job, the control measures for any type of risk are basically the same. In essence, based on the two principles of risk avoidance or risk reduction, there is a hierarchy of control (ASIRP) that should be employed that is shown in figure four.

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

Figure four: Hierarchy of risk control measures



In accordance with this hierarchy of control the first efforts should be to avoid the risk altogether. If this is not possible, efforts should then be made to combat the risk at source by substitution, and so on. Where possible therefore:

- Eliminate the risk altogether
- Change the activity or process to one that is less risky
- Separate people from the processes to reduce risk
- Design a system that reduces the risk to an acceptable level
- Provide written procedural controls
- Provide adequate supervision
- Identify training needs and provide training,
- Provide instructions/information
- Provide other controls such as auditing

Whichever your preferred control measure is, always re-evaluate the chosen option to see if the risk (or aspects of it) cannot be eliminated. In many instances, a combination of the above control measures may need to be employed. Often, however, it is feasible that any number of alternative measures would reduce the risk. In these instances, the hierarchy of control should always be used as a guide to decide which measure to use. Importantly, the amount of managerial or supervisory effort needed to establish and maintain the above controls is in inverse rank order: i.e. the amount of effort needed to protect systems is infinitely much greater than that required to eliminate the risk altogether. Once a control measure has been proposed or put in place, a further risk assessment needs to be undertaken to ensure that the original risk(s) have indeed been reduced or eliminated, or that no new risks have been inadvertently introduced. If the control measures are found to be unsatisfactory, a further round of risk assessments to identify the appropriate control measure(s) will be necessary. This makes the point that the risk assessment process is an iterative one. The exercise must be repeated over and over, until such time as it is impossible to reduce the risks any further.

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

Prioritising Risk Control Decisions

Some of your risk control measures will be easy to implement and will exert a high impact, others will be hard to implement and may not exert any significant impact on the risks. One method for ascertaining this, prior to finalising the decision about which control measure to put in place, is to make use of an impact grid as shown in figure five. Any item falling into the easy to do / high impact category would be done first as this gives some quick wins. Items falling into the easy to do / low impact quadrant might be left, unless a cumulative effect can be demonstrated over a number of items, that would make effort involved in implementing the remedial actions worthwhile. Similarly, any item falling into the hard to do/ low impact

Figure five: Remedial Action Impact Grid

		IMPACT	
		LOW	**HIGH**
DIFFICULTY	**EASY TO DO**		Disabling User ID's after 30 days of non-use Transfer risk via insurance Data Scrubbing
	HARD TO DO	Stress Testing	Install Straight Through Processing system Conduct Internal Audits

quadrant needs to be thought about as cost / benefit grounds may not make the effort worthwhile. Obviously items falling in to the hard to do / high impact quadrant would need to be costed. More often than not, however, remedial actions in this quadrant tend to be the most worthwhile although they take longer to implement and involve a lot more effort.

Document the risks

It also makes good commercial sense to record and document each risk assessment so that it is possible to check that all of an institution's activities have been assessed. The advantages of keeping such records outweigh the perceived bureaucracy, as they can be used in many ways. For example, they can be used to:

- Demonstrate to board members, shareholders and regulatory bodies that the organisation is actually identifying, assessing and controlling risks;
- Identify or reinforce the need for capital expenditure to be allocated to control the risks;
- Reduce management's time during periodic reviews of risks
- Identify staff training needs

Risk assessment records must include the measures chosen to eliminate or control the risks, and the reasons for choosing them. As such the record is focused primarily on the activities taking place, while taking into account any particular situational constraints, the risks posed and the solutions to overcome them. Importantly, such documentation should be readily

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

accessible, not placed on a shelf to collect dust. In principle, a good management information system should be developed to make such risk assessment documentation available to those who need access to it.

Review and Revise

Once risk control measures are put in place, they need to be periodically reviewed (e.g. every 24 months) and updated, so that any changes in circumstances can be accommodated (this requirement emphasises the need to record every risk assessment). The timing of these reviews may also be dictated by number of circumstances that include:

- the occurrence of losses or errors
- addressing any recommendations arising from internal audits
- receiving suggestions or complaints from employees and others
- the introduction of new equipment, technology or materials
- planning and introducing new working methods
- the introduction of amendments to existing legislation
- the introduction of new legislation

Whatever remedial actions arise from these reviews, it cannot be emphasised enough how important it is to ensure that they are put into effect. This is normally best achieved by allocating the responsibility for doing so to a named person, who must complete these within a specified timescale. However, there is still a need for checks to be made that the named person has actually completed the remedial actions by the due date.

Matching delegated responsibilities with the requisite authority

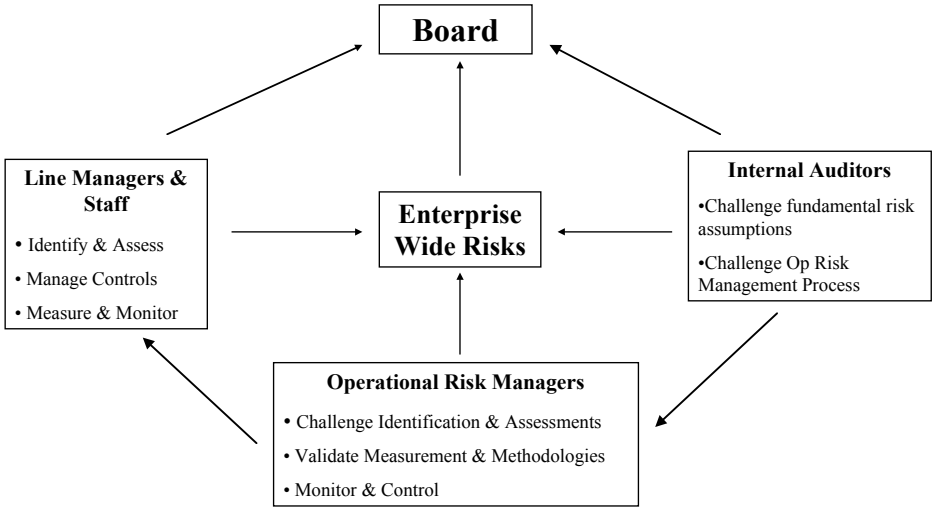
Establishing an enterprise wide risk management culture will not be easy as people are challenged to move out of their comfort zones and have to find new ways of working. Developing an organisation risk management structure where people are clear about their roles is the obvious first step. Figure six provides an overview of the responsibilities that should be assigned to four discrete functions: The board, Internal Auditors, Operational Risk Managers, Line managers and staff. As I hope to have illustrated, everybody has a role to play.

In principle, the board of directors is ultimately responsible for oversight of the entire process. In practice it is wise to delegate oversight to one nominated director, who is responsible for overseeing the entire effort and is held accountable for doing so. The role of the internal auditors is to ensure the risk management processes are functioning as intended. Not only does this incorporate the actual audit role, but also includes them challenging the fundamental risk assumptions of the institution, and the operational risk management process. Similarly Operational Risk Managers, rather than being responsible for actually controlling risks, they are primarily concerned with providing the framework for developing an enterprise wide risk culture and providing training in risk management to line functions. Moreover, they need to challenge line-management's risk assessments and control measures, and ensure that the appropriate risk controls are put in place and are working as intended as well as ensuring that the risks identified have been sufficiently documented. They should also oversee the development of a risk management information system to ensure that there is consistency in approach across the institution, and that risk data is available in real time. Line-management and staff are the people who should conduct the actual risk assessments in their sphere of influence, as they are the people who possess the intimate knowledge of the products,

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net

services, and operations within their control. This also helps to bring about ownership of, and commitment to, the risk management process throughout the institution

Figure six: Risk Management Structure (After Pagett, 2000)



.

Summary

In summary, many credit and market risks emanate from operational risks. A model is offered to enable risk managers to identify where operational risks can be introduced within five organisational levels. A complete risk assessment process drawn from the safety discipline (see Cooper, 1998) and functional roles are also described to enable institutions to create an effective and consistent enterprise wide risk culture.

References

Cooper, M.D. (1998) *Improving Safety Culture: A Practical Guide*. J Wiley & Sons, Chichester. ISBN 0-471-95821-2

Pagett, T (2000) Internal Audit- Challenged from within. *Operational Risk Manager*, July / Aug; Issue 6, pp 11-13.

Reason, J. (1990) *Human Error.* Cambridge University Press. ISBN 0-521-31419-4.

☎ +1 (317) 736 8980
e-mail: dom@bloomington.in.us website: www.bsafe.net