MANAGING OPERATIONAL RISK

1

Operational Risk Management: The Solution is in the Problem

Peyman Mestchian

SAS UK

"There are risks and costs to a program of action, but they are far less than the long-range risks and costs of comfortable inaction", John F. Kennedy

During the last few years there has been growing interest in the need for firms within the financial services industry to have in place robust systems for managing operational risk. This systematic approach to operational risk management requires a comprehensive control structure that is designed to address the full spectrum of risks faced by firms. The increasing level of interest in operational risk management has been stimulated by a variety of factors:

- the increasing complexity of financial products and trading mechanisms, particularly with the development of derivative products;
- the introduction of further requirements by banking and securities regulators and supervisors with the particular focus on the mechanisms for the "regulatory capital" calculations;
- the acceptance of senior executives that the systems supporting operational risk management have been, and in many cases still are, inadequate, and that good quality risk management requires significant improvement in processes and technologies that are now available for effective operational risk management; and
- the increase in knowledge and expertise in the practical application of statistical techniques to the operational risk management challenge.

The problem

There now appears to be a consensus forming that the definition of operational risk is:

> *the risk of loss resulting from inadequate or failed internal processes, people, and technology or from external events.*[1]

To understand the problem further we need to decompose this definition:

Process risks: These include inefficiencies or ineffectiveness in the various business processes within the organisation. These include value-driving processes (frontoffice) such as sales and marketing, product development and customer support, as well as value-supporting processes (back-office) such as IT, HR and operations.

People risks: These include employee errors, employee misdeeds, employee unavailability and inadequate employee development and recruitment.

Technology risks: These include system failures caused by breakdown, data quality and integrity issues, inadequate capacity and poor project management.

External risks: These include the risk of loss caused by actions of external parties such as competitor behaviour, external fraud, regulatory change, and macro- and socio-economic events.

The interaction of these risks is shown in Figure 1.

THE COMMON FACTOR: DATA

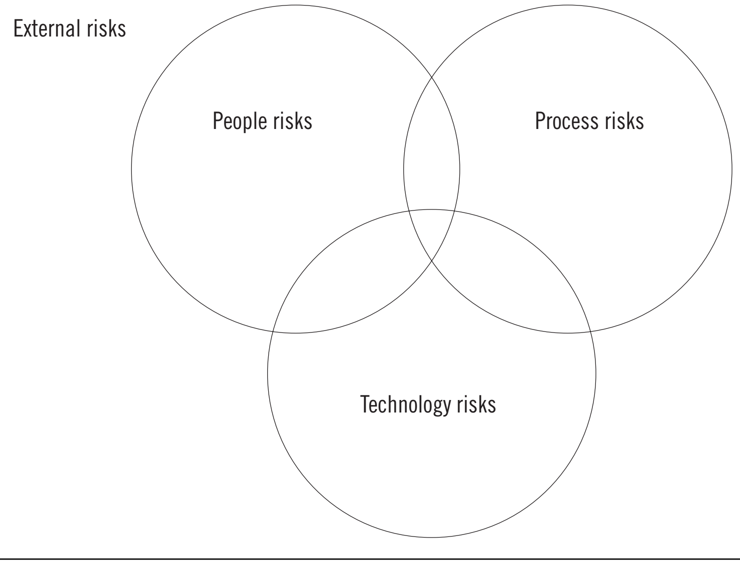
The lack of available or suitable data, especially for larger and unexpected loss events, insufficient statistical samples and the incomplete statistical relationship between cause and effect or control variables all prove that there is significant room to improve data collection and correlation analysis. Successful risk practitioners have recognised this and are working towards alignment of operational risk measures to those of market and credit risk, if only at the level of common language.

The conceptual foundations for modelling operational risk shown here have been given most attention and a case can be made for all of them.

Economic pricing models: These base forecasts on economic models. One such operational risk model uses the capital asset pricing model (CAPM) to suggest a relative distribution of pricing of operational risk among other price determinants for capital.

Scenario analysis/subjective loss estimate models: Used to capture diverse opinions, concerns and experience/expertise of managers and represent them in matrix and graphic form.

1. Taxonomy for operational risk



Statistical/actuarial/loss distribution loss models: Actual loss data are used to construct data representations of loss frequencies and severities in the form of statistical probability distributions in modelling expected losses for the future.

Factor-driven models: Apply loss and/or causal factors to build a bottom-up prediction of loss expectancies. For instance, these models are being applied in operations and processing units in conjunction with Bayesian Belief Networks and value-at-risk.

The solution

As discussed above, the key elements of operational risk are:

❏ process;
❏ people;
❏ technology; and
❏ external events.

In this chapter we suggest that the key components of successful operational risk management are an exact reflection of these four elements. The one common factor between the four solution areas is the need for a data-driven approach. This data is required for modelling risk as well as ensuring a continuous cycle of performance improvement.

THE PROCESS SOLUTION TO OPERATIONAL RISK

The key steps in an effective operational risk management process, as shown in Figure 2, are:

Step 1 *Setting policy*: Effective operational risk management policies set clear direction for the organisation to follow. They contribute to all aspects of business performance as part of a demonstrable commitment to continuous improvement. Responsibilities to people and the business community are met in ways that fulfil the spirit and letter of the law. Stakeholders' expectations in the activity (whether they are shareholders, employees, or their representatives, customers or society at large) are satisfied. There are cost-effective approaches to preserving and developing tangible and intangible assets, which reduce financial losses and liabilities.

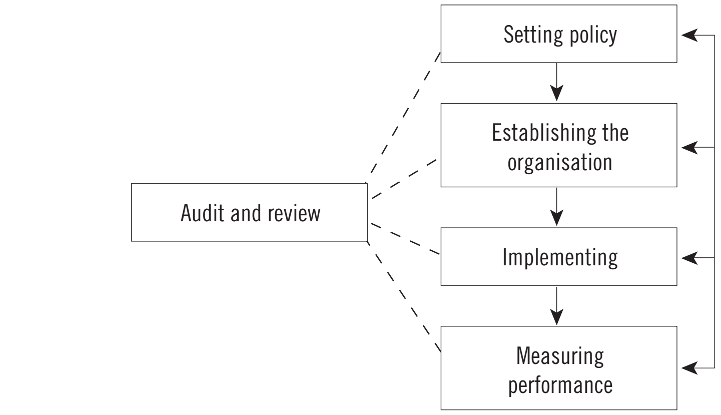
Step 2 *Establishing the organisation*: An effective management structure and arrangements are in place for delivering the policy. All staff should be motivated and empowered to work safely and to protect the long-term success of the firm. The arrangements are:

❏ underpinned by effective staff involvement and participation; and
❏ sustained by effective communication and the promotion of competence which allows all employees and their representatives to make a responsible and informed contribution to the operational risk management effort.

There is a shared common understanding of the organisation's vision, values and beliefs. A positive risk management culture is fostered by the visible and active leadership of senior managers.

Step 3 *Implementation*: There is a planned and systematic approach to implementing the operational risk management policy through an effective operational risk management system. The aim is to minimise risks. Risk assessment methods are used to decide on priorities and to set objectives

2. Operational risk management process



for eliminating hazards and reducing risks. Wherever possible, risks are treated through selection and design of appropriate controls. If risks cannot be controlled internally then various risk transfer methods are considered. The overall capital adequacy is reviewed taking into account the overall operational risk profile of the firm. Performance indicators are established and used for measuring risk. Specific actions to promote a positive operational risk culture are identified and implemented.

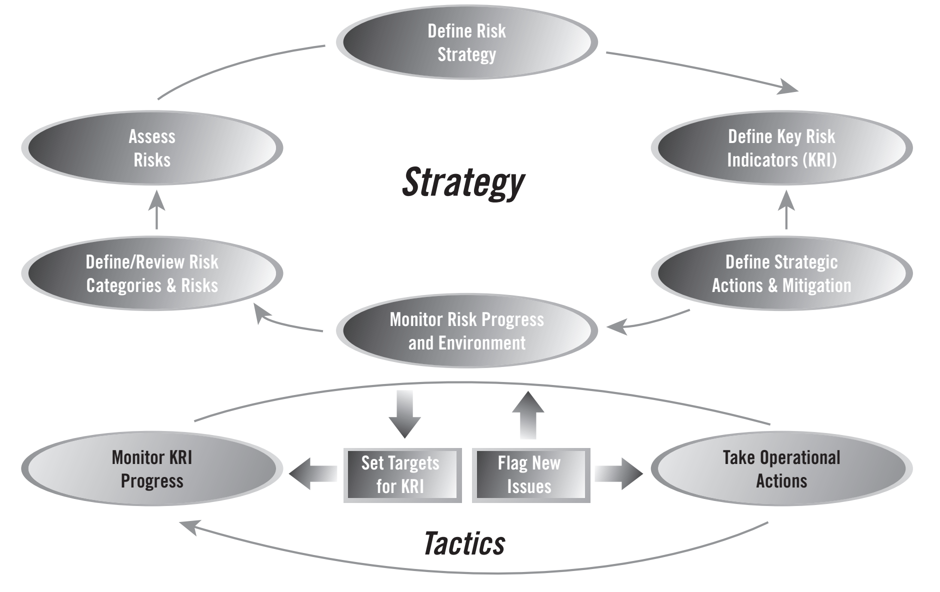
Figure 3 illustrates the key elements of the implementation process.

❏ *Define / review risk categories and risks*: The first step is to agree and capture the common definitions for risk categories, risks, events and their interdependencies. This is a top-down approach, where risks are tied to loss events. A process view can be taken, where conflict and inefficiencies are isolated and categorised.
❏ *Assess risks*: Some form of initial assessment of all risks based on impact and probability is needed to create a common view of the most significant risks. These can be visualised using risk maps.
❏ *Define risk strategy*: For the most important risks, based on agreement on acceptable levels of each risk.
❏ *Key risk indicators (KRIs)*: KRIs are used to track risks as they move toward the target acceptable levels. Thresholds are assigned, above which alerts and escalation procedures are triggered.
❏ *Define strategic actions and mitigation*: To ensure that KRI values move towards defined tolerance levels and stay there, strategic actions have to be defined. KRIs typically measure the probability level of risk. At the impact level, actions to mitigate risks need to be defined.
❏ *Monitor risk progress and environment*: Reporting on the progress of KRIs highlights critical areas where thresholds are breached and require actions. Periodic re-assessment of the risks via self-assessment allows the firm to identify changes in the environment and the impact on the risks.

The above strategic view is supported with tactical activities. To ensure that line managers and staff across the wider organisation participate in the risk management process, the following should be carried out.

❏ *Set targets for KRI*: The first step of such a cascade is to select the risks and KRIs applicable to a given organisational unit and to set appropriate targets or thresholds for these KRIs.
❏ *Monitor KRI progress*: The time intervals for monitoring KRIs at the tactical level

3. Key elements of the implementation process


Define Risk Strategy
Assess Risks
Define Key Risk Indicators (KRI)
Strategy
Define/Review Risk Categories & Risks
Define Strategic Actions & Mitigation
Monitor Risk Progress and Environment
Monitor KRI Progress
Set Targets for KRI
Flag New Issues
Take Operational Actions
Tactics

are shorter (eg, weekly intervals), while top level monitoring can be monthly or quarterly.

- *Take operational actions*: By implementing shorter time intervals for monitoring operational actions a business unit manager can address risks before they escalate to higher levels. Consequently, top management can focus attention on wider and more important issues.
- *Flag new issues*: New loss events, near-misses, or simply changes in the environment make it essential that managers flag issues to senior management using the risk management process.

Step 4 *Measuring performance*: Performance of the operational risk management system is measured against standards to reveal when and where improvement is needed. Proactive self-monitoring reveals how effectively the operational risk management system is functioning. This looks at both internal and external risk factors. If controls fail, reactive monitoring discovers why, by investigating risk events that could cause loss. The objectives of active and reactive monitoring are:

- to determine the immediate causes of sub-standard performance; and
- to identify the underlying causes and the implications for the design and operation of the operational risk management system.

Step 5 *Auditing and reviewing*: The organisation learns from all relevant experience and applies the lessons. There is a systematic review of performance based on data from monitoring activities and from independent audits of the whole risk management system. These form the basis of self-regulation and of complying with various national and international standards. There is a strong commitment to continuous improvement involving the constant development of policies, systems and techniques of risk measurement and control. Performance is assessed by:

- internal reference to key performance indicators; and
- external comparison with the performance of business competitors and best practice.

Finally, the feedback loop is an essential aspect of the operational risk management process. This is not a one-off activity and an ongoing continuous improvement cycle is critical to the success of the overall system.

THE PEOPLE SOLUTION TO OPERATIONAL RISK

Loss events are seldom random events. They generally arise from failures of control and involve multiple contributory factors. The immediate cause may be a human or technical failure, but they usually arise from organisational failings which are the responsibility of management. Successful policies aim to exploit the strengths of employees. They aim to minimise the contribution of human limitations and fallibilities by examining how the organisation is structured and how jobs and systems are designed.

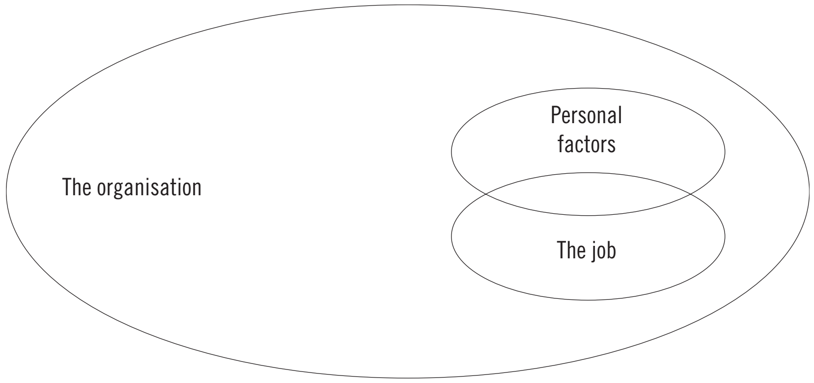
Firms that are good at managing operational risk create an effective framework to maximise the contribution of individuals and groups. Operational risk objectives are regarded in the same way as other business objectives. They become part of the culture and this is recognised explicitly by making operational risk a line management responsibility. The approach has to start at the top. Visible and active support, strong leadership and commitment of senior managers and directors are fundamental to the success of operational risk management. Senior managers communicate the beliefs which underlie the policy through their individual behaviour and management practice. Operational risk is a boardroom issue and a board member takes direct responsibility for the co-ordination of effort. The whole organisation shares the management perception and beliefs about the importance of operational risk and the need to achieve the policy objectives.

Figure 4 shows the interaction of the human factors that affect operational risk.

Organisational factors: These have a major influence on individual and group behaviour, yet it is common for them to be overlooked during the design of work and when investigating loss events. Organisations need to establish their own risk management culture that promotes employee involvement and commitment at all levels. This culture should emphasise that deviation from established risk management standards is unacceptable.

Job factors: These directly influence individual performance and the control of risks. Tasks should be designed according to sound financial and operational principles to take into account the limitations of human performance. Mismatches between job requirements and individuals' capabilities increase the potential for human error. Matching the job to the individual ensures that people are not overloaded; this contributes to consistent performance. This involves taking into account the

4. The human factor



individual's information and decision-making requirements as well as his or her perception of the task. Mismatches between job requirements and the individual's capabilities increase the potential for human error.

Personal factors: The attributes that employees bring to their jobs may be strengths or weaknesses in relation to the demands of a particular task. They include attributes such as habits, attitudes, skills and personality, which influence behaviour in complex ways. Negative effects on task performance cannot always be mitigated by job design solutions. Some characteristics, such as skills and attitude, can be modified by training and experience; others, such as personality, are relatively permanent and cannot be modified within the work context. People therefore need to be matched to their jobs through appropriate selection techniques.

THE TECHNOLOGY SOLUTION TO OPERATIONAL RISK AND MEETING THE DATA CHALLENGE

It goes without saying that technology solutions for operational risk management are the least developed element of the risk management infrastructure. However, recent developments in the definition of operational risk together with advances in risk quantification and data management technology have led to the development of a number of key technological components for an enterprise-wide operational risk management system.

Figure 5 describes some of the key elements of the operational risk technology developed by SAS.

Self-assessment of risks

It is generally accepted that in many organisations there is a need for an initial assessment ('health check') of operational risks, taken from a wide and geographically dispersed selection of individuals across the firm. The most effective – and repeatable – process to support such an exercise is to make it easy to capture the results and store them in a robust database that reliably manages them and allows them to be analysed with ease. Some firms prefer a more interactive, regular "group workshop" approach to gathering data, but whatever approach is taken, the key task is to capture and store the data in a standard manner.

The proposed SAS solution includes fully web-enabled, highly configurable questionnaires that are distributed selectively to any or all of the target individuals and groups responsible for any number of risk categories. The process includes approvals and escalation levels to ensure that responses are consolidated and consistent as the key summary data is filtered up the organisation. Lastly, the process can also be automated and scheduled with ease, making it possible to conduct these reviews on a regular basis.

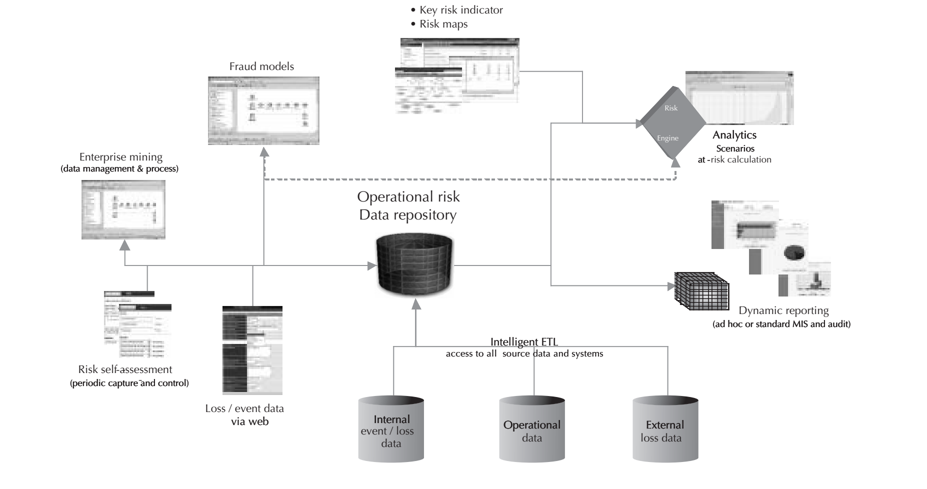
Each risk has a questionnaire dynamically linked to it. By selecting any of the assigned topics for risk assessment, the user can assess the risk based on impact (severity, qualitatively or quantitatively) and probability (frequency), specify root causes, assign specific amounts to impacts, indicate whether risks are acceptable and indicate that if risks are unacceptable, what measures or controls are in place to mitigate those risks.

The content of questionnaires is configurable and can be extended to include more complex elements, qualitative and quantitative impacts. The entire process can be managed from a single location with relative ease and distributed via intranet.

Risk maps

Having captured the results of risk self-assessments, SAS provides the capability to generate sets of dynamic, multi-dimensional views of the risks showing the responses submitted by each user and reflecting impacts and probabilities. Risk maps are

5. SAS operational risk architecture



particularly useful at a senior level of the organisation, where it quickly becomes clear what the key areas of risk – or opportunity – are.

Users can view the data at any level of detail or aggregation and can also select categories (highest, lowest, top 10, etc). Group managers can select the specified risks of a business unit to see how each user rates the risk, or select a specific risk and view its ranking. The value of the risk map is its ability to isolate those risks (or opportunities) that give the firm a clear perspective on where to act.

Data access

The primary data sources for an operational risk system are:

- self assessment data (discussed above);
- internal event / loss data;
- operational data; and
- external loss data.

A key requirement for any solution is for users to be able to select blocks of loss data for analysis from multiple databases holding loss data. Each of these data sources is reviewed below and data management issues are then discussed.

Internal event / loss data

To facilitate the process of feeding the internal event/loss data model, users have secure access to a web-based application, similar to the self-assessment and scorecard modules. A series of configurable input screens allow assigned users to capture all relevant data associated with specific events and losses, such as:

- event category;
- general information (eg, event id, status flag, regulatory flag);
- categories (four-dimensional, multi-level, event-type, cause-type, effect-type, insurance policy);
- descriptions;
- status:
  - event dates (eg, start, end, reported, booked, last update);
  - process (eg, detected by, reported by, reported to, open/closed);
- organisational structures:
  - country, region, branch, division, area, product group, regulatory business line;
- loss amounts:

  - ● actual loss, potential loss, recoveries;
  - ● currency;
- ❑ correlated events; and
- ❑ exposure indicator.

Operational data
The SAS system can act as the ultimate integrator of operational risk information and needs access to operational data to feed its early warning indicators and to assign the right level of detail to loss events. For example, when faced with a sporadically failing IT system, one would want to know the system's details, the number of hours the problem has persisted, and so on. This data can be manually captured in the risk scorecard or ideally sourced from operational databases already in use. Accessing this data in an automated, rapid and user-friendly manner is crucial to the risk warehouse.

External loss data
Regulators welcome the inclusion of external loss data, but these databases are in their infancy. The best-known initiative is the ORX pool set-up by major global banks. The British Bankers' Association has also established a data pool known as GOLD. However, these data pools will only contain losses above a certain threshold.

Only 10 data fields are captured. External loss data cannot be integrated directly into the internal loss database and needs to go through a scaling process where the loss is transformed to correctly reflect the profile of the client's own organisation. No standard market method exists for scaling data; almost every bank uses its own algorithms.

Data management
All successful risk management projects share a strong emphasis on complete management of input data and computed results. The SAS solution includes data management tools to manage the data repository and supports complete definition and management of the entire inflow process, including the risk model. All metadata is documented and every step of the ETL (Extract–Transform–Load) process can be visualised graphically.

Also included in the solution is support for full creation of dynamic HTML documentation, including hyperlinks and deep drill-down capabilities that use all of the metadata in the environment. This is especially useful to provide valid and current documentation to anyone who needs to understand the model.

Risk analysis
The first level of analysis starts from the operational risk data repository. Using the available statistical analysis tools within the risk engine, a user can determine the best fit of:

- ❑ frequency distributions of loss events, such as poisson, negative binomial, binomial, hyper geometric and geometric; and
- ❑ severity distribution of loss events, such as log-normal, Pareto, exponential, gamma, beta and Weibull.

Using the maximum likelihood estimation (MLE) and other similar techniques, a user can fit a curve of data points to two or more combinations of these distributions and then perform Monte Carlo simulation(s) using the joint distribution.

Monte Carlo simulations include using either the expected loss frequency or a user-defined frequency to define the arrival rate of losses, and either the fitted severity distribution or the empirical distribution of losses to define the severity of each loss. The process combines frequency and severity distributions to generate the combined loss distribution. The number of trials required, the time period to be covered (eg, one year) and reports of these results are all user-defined, eg, expected (mean) loss, median loss, minimum loss, maximum loss, 99% confidence level and user-specified confidence level (eg, 99.75%). Users can also include or exclude zero and negative losses (ie, gains) from the analysis; if zero losses are included, the system forms a composite distribution, which includes a probability of the loss being zero, and a severity distribution contingent on the loss being non-zero.

Monte Carlo simulations can be run simultaneously using data sets that apply to a number of different lines of business, each of which has had frequency and severity distributions fitted. Results can be reported for each of the data sets individually, for the combination of all data sets, and for all intervening levels of the line of business hierarchy, with some of the results being additive up the hierarchy and others not.

A second – optional – level of analysis focuses around fraud models, by exploring and modelling fraud behaviour by mining through transaction data to uncover previously unknown patterns. The resulting models are fed into the risk engine, which then computes capital-at-risk – a measure that expresses how much one can potentially lose, within a timeframe and with a specified confidence level – and performs scenario / stress analysis.

Result presentation

The scorecard is an ideal presentation layer for operational risk, an approach that integrates "top-down" and "bottom-up" perspectives. Scorecards present graphic cause–effect flows, as illustrated in Figure 6 for an operational risk environment.

The scorecard is also an ideal communication channel to link causes with the actions to be taken by those affected by or responsible for actions. As a result, every employee in the organisation is brought into the process.

This approach brings together the early warning indicators, capital at risk figures, self-assessment and loss data. Advanced reporting features allow risk managers, senior management and others to access and communicate risk measures across the entire enterprise, fuelling better decision-making. The risk scorecard makes it possible for management to retain a strategic vision without losing sight of, or access to, the details.

Performance tracking

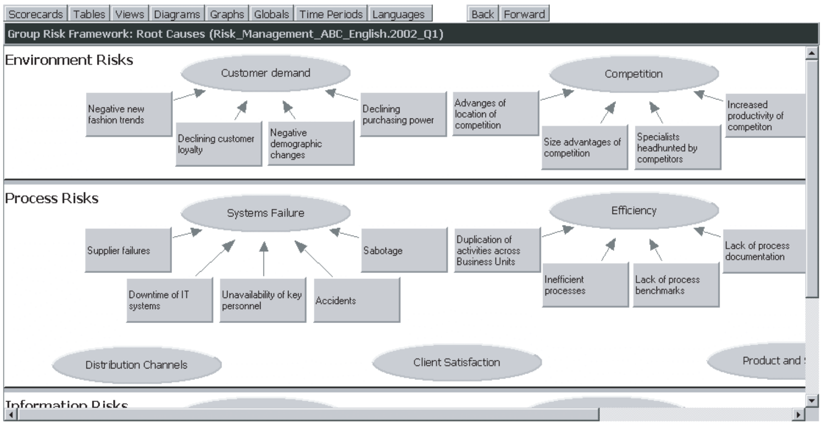
Key risk indicators (early warning indicators) are used to track the risk exposures linked to each of the defined risks. These can be viewed at the global framework level, or for a particular business unit. As with the risk maps, the loss event database can be presented in a variety of ways in the form of views, graphs and diagrams. In these cases the user has complete control over both the display of loss event types and what information to display in the views. In Figure 6, the view has been configured to show only the internal scores and comparison against external scores. Using advanced analytics and reporting a user can drill-down through the scorecard data for more detailed analysis. For example, it would be possible to drill-down on IT failure rates to get a standard report on system down times, generated from the risk data details. Integrating the qualitative and quantitative measures into the scorecard is achieved simply by configuring it to pick up the result calculations from the risk engine.

Event (loss) analysis

As with the risk maps, the loss event database may be presented in a variety of ways in the form of views, graphs and diagrams.

Users have the ability to graph loss events over time (at a detailed or summary level). Users can also comment on (or review comments on) loss events, in the same manner as outlined earlier.

6. Risks: hierarchy of causes



Group Risk Framework: Root Causes (Risk_Management_ABC_English.2002_Q1)

Scorecards
Tables
Views
Diagrams
Graphs
Globals
Time Periods
Languages
Back
Forward
Environment Risks
Customer demand
Negative new fashion trends
Declining customer loyalty
Negative demographic changes
Declining purchasing power
Competition
Advanges of location of competition
Size advantages of competition
Specialists headhunted by competitors
Increased productivity of competiton
Process Risks
Systems Failure
Supplier failures
Downtime of IT systems
Unavailability of key personnel
Accidents
Sabotage
Efficiency
Duplication of activities across Business Units
Inefficient processes
Lack of process benchmarks
Lack of process documentation
Distribution Channels
Client Satisfaction
Product and
Information Risks

Finally, due to the dynamic nature of risk management, it is important for any technology solution not only to meet today's requirements, but also be flexible enough to evolve and meet the future expectations of regulators, risk managers and top management.

To be successful, firms must establish a link between qualitative and quantitative risk measures and build a process with which they can leverage this knowledge.

THE EXTERNAL SOLUTION TO OPERATIONAL RISK

So far in the discussion we have focused on the use of various internal mechanisms, namely people, process and technology, for managing operational risk. However, where appropriate, organisations do have access to external sources of operational risk management.

Insurance

In recent times financial services firms have invested significant amounts of time and money to identify ways of managing and hedging market and credit risk. This includes instruments such as credit derivatives used for hedging against counterparty default. These instruments are often supported by sophisticated information systems used for modelling and managing exposures.

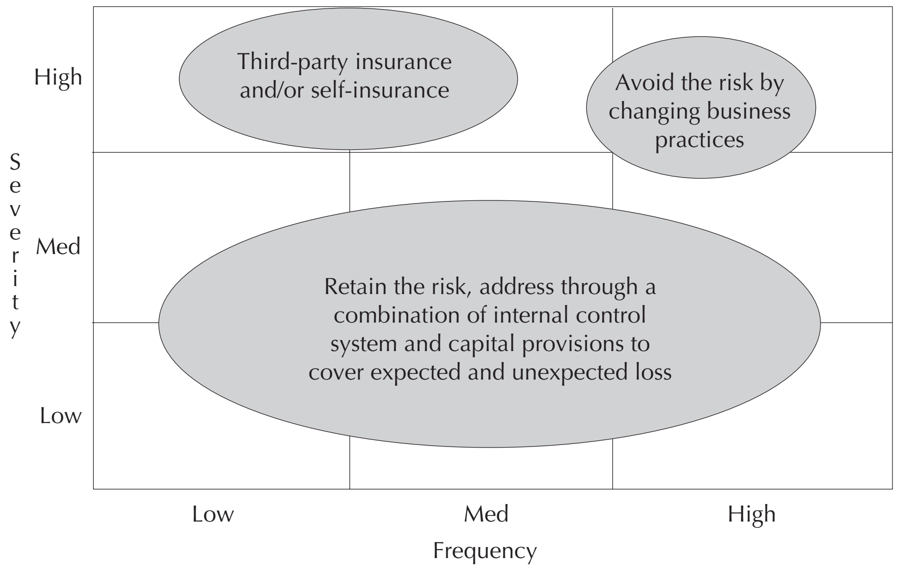
The attention of hedging experts has now turned to operational risk. A key tool here is insurance. Elements of operational risk have been insured for some time. Examples include property coverage, fire, workers compensation, employer's liability and professional indemnity. Insurance provides financial services firms with the means of taking risk off their balance sheet and avoiding the significant costs of capital associated with the provisions for risk.

Demand for traditional insurance coverage has increased dramatically in recent times as senior executives wake up to the potential horrors presented by various operational risks, and the insurers are responding; there has been a move toward multi-risk coverage programmes comprising of multi-billion dollar limits. Moreover, the market for alternative risk transfer has been growing in recent years. Multi-year, multi-line coverage whereby the various lines of coverage are bundled into one complete package and spread over five to 10 years as opposed to the traditional annually renewable policy have become more popular. This gives both premium and transaction savings to the client as well as wider coverage.

One way to look at the decision-making process for operational risk insurance is to categorise by severity and frequency on a risk map, as shown in Figure 7.

It should be noted that as multinational firms have increased in size and capital it has become more attractive for them to self-insure by setting up internal

7. Risk map of the decision-making process for operational risk insurance


Third-party insurance and/or self-insurance
Avoid the risk by changing business practices
Retain the risk, address through a combination of internal control system and capital provisions to cover expected and unexpected loss
Severity
High
Med
Low
Low
Med
High
Frequency

investment funds. This has the advantage of avoiding the regular two-way transaction costs of making claims and paying premiums on a regular basis as well as reduction in the actual premium. For a large organisation the savings can amount to several million dollars. Moreover, by setting up these funds in the form of offshore captives, large organisations can benefit from additional financial and tax advantages.

Outsourcing

Another method for transferring risks to an external entity is outsourcing. Essentially, this allows financial institutions to select the various business processes or functions that are non-core and high risk to a third party. Recent examples of this have been the outsourcing of non-core back-office functions such as IT and/or HR. The third-party firms often benefit from economies of scale and specialisation and can pass on cost savings as well as quality improvements to the client. The critical success factor is the nature of the relationship and the service level agreement between the two companies. The management of this interface has its own operational risks but, if managed effectively, it can be an elegant mechanism for transferring risk.

In addition to transferring risk, outsourcing has several other business benefits. These include:

❏ cost control;
❏ access to best-practice tools and methodologies;
❏ freeing up capital and resources to focus on core business; and
❏ reduction in bureaucracy and administrative burden.

The future

Each solution area covered in this chapter has its own direction in future development. In many cases, these future developments will address gaps in current thinking and clarify ambiguities in current understanding.

Two main driving forces will influence the direction of operational risk management.

Firstly, the application of existing business management approaches to operational risk management will gain pace over the next few years. For example, operational risk management tools and techniques have been developed and established within non-financial organisations for many years. These have been around for decades in safety-critical industries such as energy, defence, aviation and transportation. Many of the methods and tools developed in these sectors can be applied to managing risks in the financial services sector. Some of the leading management tools applicable to operational risk management are:

- ❏ *Reliability-centred management*: This is comprised of a set of methods and techniques by which an organisation can use process, equipment and control failure data to develop a flexible and cohesive operational maintenance and resilience capability.
- ❏ *Behaviour-based management*: This applies the principles of total quality management coupled with the latest thinking in organisational behaviour and statistical techniques to the issue of unsafe behaviours and attitudes by employees. It has had several decades of success in the manufacturing and industrial sectors.
- ❏ *Knowledge management*: In recent years many leading organisations have invested in the latest systems and processes for managing their intangible assets. It has been shown that individual and organisational knowledge can be utilised to create more efficient and effective business processes. This has direct relevance to operational risk management as existing knowledge management systems can be used to identify potential risk events as well as assist in the communication of risk prevention initiatives and best-practices. Of particular relevance is the application of the latest text-mining technology. This technology allows organisations to scan and interrogate unstructured data (ie, data that is not in any specific database) and identify clues about risk events before and/or after their occurrence. Research has shown that 80% of all organisational data is in an unstructured format (eg, Word documents, spreadsheets, presentations, reports, emails and intranet). Therefore, a systematic approach for identifying operational risk events can only be complete when this data is utilised.
- ❏ *Activity-based management*: Activity-based costing and activity based management systems became prevalent in the 1990s. The aim of these systems is to achieve greater accuracy in cost allocation and provide "true" economic information to management and help them make decisions to satisfy customers and improve profits. This activity-based view of the business is highly relevant to operational risk management as it assists in decisions concerning pricing, product mix, costs reductions, process improvement, process or product redesign, and planning or managing activities. Moreover, this approach can be directly linked to the risk scorecard and key indicator approaches described earlier in the technology section.

The second key driving force for further development of operational risk management as a discipline is new regulatory requirements focusing on adequacy of capital allocation and implementing sound systems of internal control. A significant gap in current understanding is the link between backward-looking historical risk event data which can be modelled using well established statistical methods and the forward-looking self-assessment and risk indicator data, which is derived from input by key personnel and operational databases. It is not yet clear how these three sets of data can be mathematically aggregated to arrive at a single economic capital calculation. It is envisaged that more advanced mathematical techniques such as Bayesian analysis and fuzzy logic may be applied to this problem. This is an area that requires further research.

Ultimately, regulatory compliance is not the best reason for implementing operational risk management systems and processes. A purely regulatory view will in general lead to firms implementing the minimum possible to achieve compliance and not realising the full business benefits of effective risk management. Thinking beyond Basel II and focusing on the significant and unquestionable returns on investment that can be derived from effective operational risk management will move this discipline into the next phase of development and embed it as part of the day-to-day activity of every business unit within a financial services organisation.

[1] *Basel Committee on Banking Supervision 2001.*