



Art or science?

If you think it can't happen to you, it probably will. **Carlos Blanco***, **Kevin Dowd*** and **Robert Mark*** explain how to manage operational risk

Operational risk measurement and management is rapidly becoming standardised across financial institutions. A similar, albeit slower, trend towards the standardisation of measurement and management of operational risk is gradually taking place in the energy and commodity space, although the nature of core operational risks is considerably different than the financial space.

Operational risk refers to the risk of financial loss resulting from inadequate or failed internal processes, people and systems, or from external causes, whether deliberate, accidental or natural. It includes the risk of fraud risks, legal risks, and the risks associated with people or systems failing to work as they should. Operational risks therefore permeate all the activities of energy and commodity firms.

Practitioners generally agree that the management of operational risk is lagging behind that of market and credit risk. However, regulatory changes (Basel 2, Sarbanes-Oxley etc) and a litany of high-profile operational-related disasters (Enron and China Aviation Oil, for example) have very much put the subject into the spotlight.

Figure 1 presents a summary of a survey conducted by Risk Management

Association (RMA) of the main reasons for firms to invest in operational risk management.

Classifying operational risks

The management of operational risks requires that a firm first establish a typology of the different types of operational risks it faces.

Figure 2 presents a categorisation of operational risks for a hypothetical firm. This allows the firm to identify the types of risk it faces, the events that can trigger operational loss events, and how those losses might be mitigated.

The firm can also assign a probability (or likelihood) to each type of risk, and the likely severity if the relevant operational risk event occurred. This information can tell management where it needs to devote its attention: the higher the probability or the higher the severity, the more attention is needed. For example, in the energy sector, a key operational risk is the risk of accidents in oil refineries: accidents can have a catastrophic effect on profits. A typical management attention report is shown in Figure 3.

It is also important to look at each operational risk according to a common set of factors such as capacity, capability and availability. For example, if we examine operational risk arising from

the people risk category for a particular business unit, then we could ask:

- ❑ Does the business unit have enough people (capacity) to accomplish its business plan?
- ❑ Do the people have the right skills and experience (capability)?
- ❑ Are the people going to be there when needed (availability)?

Best practice also requires that the risk managers analyse the interactions among the various operational categories. They should also understand the source and nature of each type of operational risk. For example, it might be that a firm's main operational risk exposures arise from change (eg the impact of new systems), complexity (and in particular, the difficulties of managing complexity), and an existing culture of complacency (ie the 'it can't happen to us' mentality).

Operational risk measurement

Operational risk is difficult to quantify for several reasons. Unlike market and credit related events, operational events are highly context dependent. Data on operational events is also generally sparse, and there is often a significant time lag between the occurrence and subsequent discovery of an operational event.

However, operational risk is measurable, at least up to a point, and

Figure 1.
Main reasons to invest in operational risk management

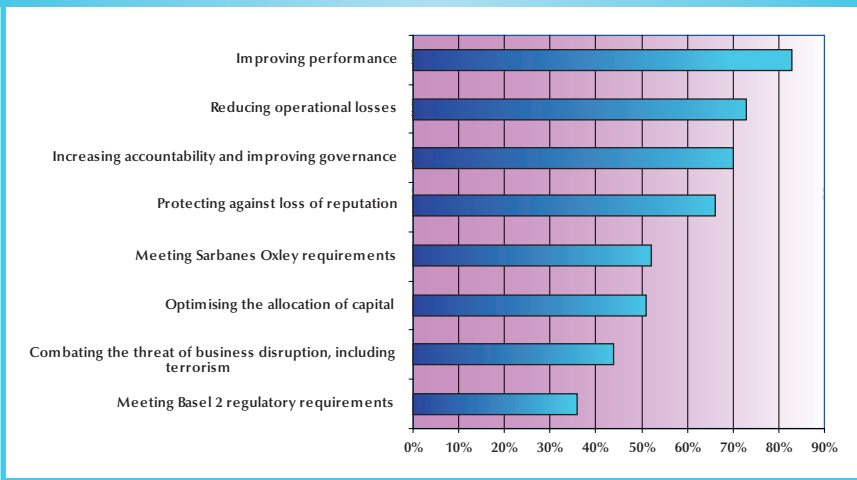
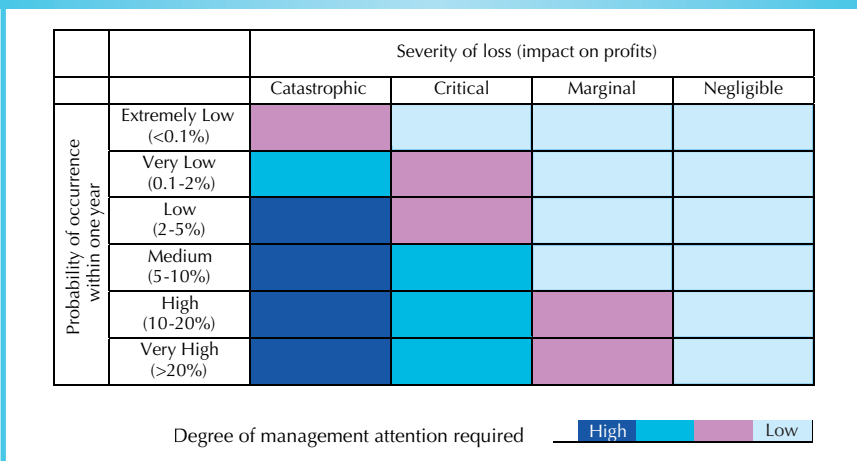


Figure 2.
Sample typology of operational risks for firm XYZ

Risk class	Risk type	Activity or event	Examples	Possible mitigation
People	Internal	Unauthorised activity Lack of skilled personnel	Rogue trading High employee turnover	Partially insured
People	External	Fraud	Theft	Partially insured
Systems	Internal	Model risk	Model/methodology error Mark-to-model error	Technical risk audit Improve quality of models/people
Systems	External	Technology risk	Telecommunication failure Blackouts	Contingency planning insurance
Processes	Internal	Transaction risk	Execution error Settlement error Documentation/contract risk	Improve processes
Asset damage	Internal	Physical asset risk	Pipeline rupture Production loss Unexpected plant outage	Partially insured Contingency planning
Asset damage	External	Physical asset risk	Uninsured or irrecoverable loss or damage to assets	Insurance

Figure 3.
Necessary management attention depends on the frequency and severity of operational events



many different methods have been proposed to estimate operational risk. These methods fall under three broad categories:

Process methods – These focus on the chain of activities that comprise an operation from start to finish, and are motivated by the operational models used in manufacturing processes. Typically, these methods carry out statistical analyses of the events in the process chain, and then infer the probabilities of particular kinds of outcome (eg system failures of one sort or another). These methods include statistical causal methods, reliability analysis methods, Bayesian belief methods, and fuzzy logic methods

Factor methods – These focus on the major determining factors that drive operational risk. For example, one might identify and then track changes in key risk indicators (KRI)s that are correlated with losses due to system risk, might include the age of the computer system, the amount of downtime as a result of system failure, and so on. Although KRIs do not represent direct measures of operational risks as such, they are useful proxies for them. KRIs can be used to monitor changes in operational risk for each business and for each loss type. Once they have been established, changes in KRIs can be mapped to changes in operational VaR (OpVaR). Factor methods also include ‘predictive models’ which use discriminant and similar methods to predict operational events

Loss distribution methods – These methods focus on establishing the distribution of operational risk losses. The loss distribution might be an empirical distribution based on an institution’s own experience or that of some reference institution or group of institutions, or it might be a parametric distribution fitted to some operational loss data set. In the latter case, the chosen distribution might be a normal distribution, a heavy-tailed distribution (eg a ‘t’) or an extreme-value distribution (which would be appropriate if we were concerned about low-probability, high-impact loss events).

The measurement of operational risk is as much art as it is science, and some useful guidelines are the following:
1. Focus on material risks, not those that are relatively easy to measure or manage

2. Keep an eye open for the unexpected. Recall that failure of imagination was cited as the main risk management failure by the September 11 Commission in the US
3. Observe operational failures by competing firms and use them as “stress tests” for what could happen to your firm
4. Combine qualitative with quantitative approaches, and don’t worry too much about achieving the theoretical ideal of consistency: perfect consistency is impossible to achieve in any case
5. Focus on operational risk level changes, not on the absolute measures
6. Remember that operational risks are often interrelated to market, credit and liquidity risks.

Mitigating operational risk

Operational risk should be analysed by management to decide on possible corrective actions to control the firm’s operational risks. Operational risks can be mitigated in the following ways:

Improved internal controls

Improving the internal control environment can reduce operational risk in many ways. In this context, it is also important to keep in mind that Sarbanes-Oxley (SOX) requires that the chief executive officer and the chief financial officer of publicly traded corporations take personal responsibility for designing, establishing and maintaining the firm’s controls and procedures. The Act also seeks to make sure that the board of the company includes members who are experts in understanding financial reports and audit committee functions, and also have experience with internal and accounting controls.

The framework that is emerging as the industry standard is the one developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), a private industry initiative organised in the US in 1985. COSO’s emphasis on internal control has emerged as an important element of the overall risk governance exercise, particularly with the advent of SOX.

Recent examples of internal control breakdowns are the debacle of China Aviation Oil Singapore (\$550m) in unauthorised derivatives trades, and the metal derivatives trading loss of Sojitz Holding Corporation (\$153m). Curiously, Standard & Poor’s Ratings

Who should assess operational risks?

Some firms have operational risks assessed by the relevant line managers. A common argument in favour of self-assessment is that risk managers cannot know as much about the business line as the business manager, and therefore cannot second guess his/her decisions. However, this confuses the roles of the business and risk managers. The operational risk manager is trained in evaluating risk from the available information. In any case, the independent risk management function is obliged to become involved in the gathering and processing of data in order to ensure objectivity, consistency and transparency. Another problem with relying only on self-assessment is that it is highly unlikely that a business manager who is incompetent or committing fraud would accurately self-assess the operational risk of their business unit.

An optimal structure consists of risk managers partnering with business managers to provide an accurate view of the risks at a reasonable cost. In order to accomplish their task, risk managers must be placed “in the flow” of all relevant business management information. This can be accomplished by inviting them to sit on the various regular key business management meetings, and by ensuring that they received regular management reports.

The firm should also conduct technical risk audits performed by independent risk specialists; these would examine the adequacy and effectiveness of the firm’s processes for measuring and monitoring risk, and also evaluate the firm’s risk policies and risk documentation. □

Model risk and SOX

The use of derivatives pricing and risk models can introduce significant model risk. For example, Enron was able to inflate earnings due to the manipulation of forward curves. Most energy and commodity trading firms dealing with exotic derivatives and structured products use a variety of derivatives pricing models, many of them implemented in spreadsheets. Some of those models, particularly those provided by third-parties, are the source of substantial model risk if they are not used adequately. In addition, many of those models are poorly documented and rarely understood by internal and external auditors.

Any internal or external audit of risk and pricing models should start with the analysis of the forward curves being used throughout the firm, as well as the process to calibrate various model parameters. If the firm lacks standard forward curves, then units within the same firm might report different values for similar transactions. If the processes to generate, store and use forward curves are not documented, audited, and standardised across a firm then the firm’s operational risk systems are inadequate and should generate a non-compliance warning. □

Services had raised Sojitz’s long-term corporate credit rating only the day before the loss announcement.

Operational mitigation

Controls should clearly extend to the hedging of physical assets to minimise the impact of operational failures. In some cases this may require investing in new assets (people, technology, physical assets) or divesting from those assets.

Insurance/risk transfer

Another way to reduce operational risk is to transfer the risk to a third-party. For example, energy and commodity related firms can transfer some

of their operational risks to third parties such as insurance companies or investment banks. Outage insurance is a typical example (see box *Outage insurance*). Each firm must perform cost-benefit analysis in order to evaluate whether they should purchase insurance or transfer certain risks to third parties that have expertise to manage those risks. However, these risk transfers can be expensive.

Capital attribution

Despite the difficulties in measuring operational risk, it is important to attribute economic capital to operational

Figure 4.

Allocation of operational losses

Operational losses	Expected event (high probability, low losses)	Unexpected event (low probability, high losses)	
		Severe financial impact	Catastrophic financial impact
Covered by	Business plan	Operational risk capital	Insurance

Outage insurance

Outage insurance is particularly relevant for firms that have sold power forward at fixed prices. It is also relevant for utilities that must supply power and are exposed to the risk of a power shortage due to an outage or to the default of a counterparty that was expected to deliver power at fixed prices.

To reduce the cost of outage insurance, some firms have included additional triggers such as combinations of a forced outage and power prices exceeding a particular threshold before the policy pays off.

It is important to have the right analytics in order to evaluate whether the risk reduction achieved with insurance is worth the cost to the firm. It is also important to evaluate the various possible risk transfer mechanisms available, and choose the ones most suitable. This requires that the firm have a good simulation engine that can produce accurate price and volume scenarios under real-time constraints. □

Technical risk audit

A technical risk audit is designed to evaluate the policies and procedures as well as models used to measure and manage risk. Risk always finds the weakest link, and companies that take a reactive approach to risk management are likely to fall behind the curve. A sample of operational risk-related questions follows:

1. How do you measure operational risk?
2. What has the firm learned from the operational risk management failures of other firms?
3. What is the scope of the risks categorised as operational risks?
4. Do you complement the normal operational risk analysis with stress tests?
5. Do you maintain a database with historical losses related to operational failures?
6. How do you harmonise operational risk metrics and stress test methodologies?
7. What is the interval between the actual operational risk event and the detection of a loss?
8. Do you benchmark operational losses against industry standards?
9. Is there a pattern of common causes that could be mitigated in the major operational losses?
10. Are major operational failures associated with large market and credit losses?
11. Do you incorporate operations and operational risk in stress tests? □

risks: business units that take more operational risks should incur a transparent higher capital charge.

Unexpected failures can be broken down into those that would cause severe financial impact to the firm, and those whose impact would be catastrophic. Catastrophic failures are not utilised for the purposes of capital allocation. There are certain events that the firm will have to cover with insurance if it is to survive them. For example, liabilities

related with environmental disasters such as Exxon Valdez could easily wipe out the entire capital of an energy firm; firms would therefore need insurance to cover that type of catastrophic risk.

Once a good operational risk measurement system is in place, risk-adjusted return on capital (RAROC) can be used to link risk and expected return. In order to calculate RAROC measures, each unit need to estimate:

- Expected losses
- Economic capital for unexpected operational losses
- Revenues generated by taking operational risks.

RAROC provides a framework to evaluate the trade off in a risk-return space of the cost of acquiring certain insurance policies to protect against operation risks. For example, it may be argued that that one should retain the risk if the risk-adjusted cost of capital to support the asset is less than the cost of insuring it. This sort of risk/reward approach can bring discipline to an insurance program that has evolved over time into a rather ad hoc set of policies – for example where one type of risk is insured while another is not, with very little underlying rationale.

Operational and operations risks have received a great deal of attention recently.

New regulatory and governance requirements have placed an increasing emphasis on the role of senior managements and members of the Board to ensure that the firm establishes a risk-aware business culture and a corporate environment in which best-practice operational risk management can flourish.

The increasing complexity and interaction of the risks involved in energy or commodity related firms mean that enterprise wide risk education and awareness should be a critical item in the agenda of senior executives and boards of directors. It is also important to conduct regular risk audits (see box *Technical risk audit*) to monitor the firm's risk management. By its very nature, all firms are exposed to operational risk. At the end of the day, senior managers need to remember that it is their personal responsibility to ensure that the firm is adequately managing it. □

*Carlos Blanco

(carlos@blackswanrisk.com) is MD of Black Swan Risk Advisors, *Kevin Dowd (kevin@blackswanrisk.com) is director of research of Black Swan Risk Advisors and professor of financial risk management at Nottingham University Business School in England, and *Robert Mark (bmark.blackdiamond@tmo.blackberry.net) is the CEO of Black Diamond.