

Approach with caution

Indicators of operational risk are not for the faint of heart, nor are they necessarily bearers of good news. But used properly and effectively, they can help businesses identify potential losses before they happen. By Charles Fishkin and Penny Cagan

There is much discussion in the risk management industry about indicators of operational risk. Many practitioners now agree that these tools play a key role in a firm's efforts to manage such risk. Most, however, would also concur that they present conceptual and practical challenges, and therefore need to be used with great care.

What follows is an overview of operational risk indicators, including their advantages, potential misuses, challenges and roles within an overall firm-wide operational risk programme.

What are operational risk indicators?

Operational risk indicators are measures that attempt to identify losses, near-losses or potential losses before they happen. These indicators can be isolated, observed and quantified. If they are understood and applied with prudence, they can provide an opportunity to intervene early and avert problems before they become a source of financial loss or damage to a firm's reputation.

Risk indicators can promote a dialogue about risk awareness among senior management, risk management functions and business units. They can contribute insight into the allocation of limited firm resources, including people, technology and capital. Indicators can also serve as a tool for comparing performance among diverse business units in a single organisation, or across comparable organisations. Risk indicators also offer insight into industry-wide benchmarks and performance profiles.

Some indicators are applicable across the entire organisation, such as the number of new hirings, resignations, staff turnover and salaries. If, for example, employee turnover is high, other associated problems may occur – perhaps increased errors, customer complaints, theft and lost market opportunities. Other types of indicators are applicable to the specific conditions in a business unit. An interesting indicator for a trading unit is 'above-market returns'.

History suggests that problems can be associated with such returns, especially if

management is unwilling to examine why certain traders achieve unusually high results. This is an appropriate indicator for some trading operations, but inadequate for others. A private bank, for example, might want to consider the number of deals that are turned down by the firm's investigations unit due to poor credit quality or the client's background. This might suggest an issue with the types of business the organisation's private bankers are soliciting – pointing to the potential for losses associated with credit worthiness and external fraud.

The use of risk indicators varies across the financial services industry – some firms are doing nothing, while many want to move forward, but are still in the planning and talking phase, waiting for the new Basel Accord to be issued in its final form. Others are using some indicators, but don't have a comprehensive plan in place quite yet. However, a small group of firms are actively using indicators, drawing meaningful conclusions from them and making adjustments as a result. We anticipate that many other

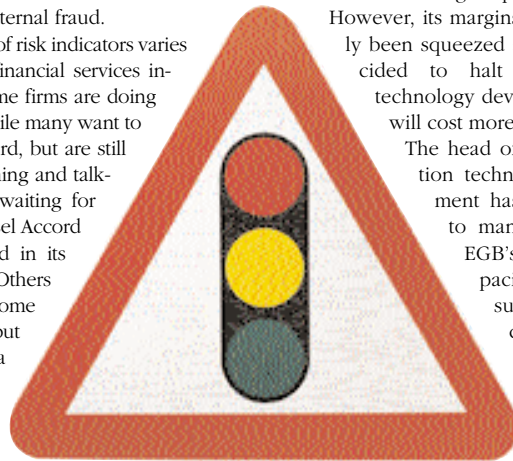
firms will soon begin to invest resources and effort in designing and applying operational risk indicators.

Applying indicators

To further explore the application of indicators, let's consider a fictional bank called Euro-Global (EGB). EGB is located in Europe and owns an online trading subsidiary based in the US. The time is mid-1998. The bank's subsidiary has experienced phenomenal growth and continues to sign up new clients. However, its margins have recently been squeezed and it has decided to halt any further technology development that will cost more than \$10,000.

The head of the information technology department has pointed out to management that EGB's systems capacity is barely sufficient for current demand, and will not be able to meet the forecasted future demand. He has indicated that a significant systems upgrade is now a necessity, which will cost more than \$1 million.

Operational risk events often evolve



Best practice guidelines

The following includes a few suggestions for firms that wish to embark on a programme – or compare their existing programme – with best practices:

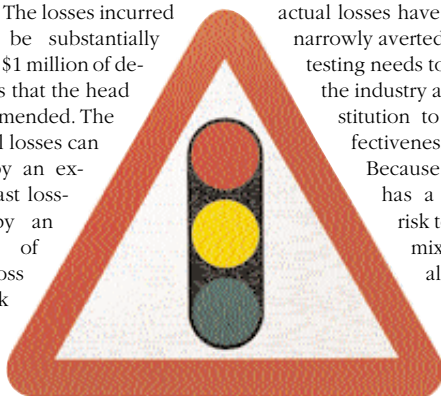
- Set priorities and focus on key risks.
- Explore and mine in-house systems for applicable data.
- Centralise the management of data in one designated unit. This can be an operational risk function or related unit. This function should serve as a centralised site for the collection, reporting and warehousing of the data.
- Link the data collection and reporting to decision-making. Data is only useful if it leads to action.
- Make the process clear and subject to independent investigation.
- Incorporate the results from indicators into the firm's planning process.

through three distinct stages: issues, incidents and losses. As our EGB example suggests, indicators can monitor each of these different stages.

An operational risk event will initially emerge within an organisation as an 'issue'. If properly identified and analysed, an 'issue' can serve as a warning of trouble ahead. Issues often spur initial 'incidents' that may not be attached to actual quantifiable amounts. These incidents then grow into indirect or direct 'losses', which are measurable and reflected in the financial records of the firm. Firms will want to mitigate losses before they occur, with the possible exception being the low-severity losses that are often accepted as a 'cost of doing business'. Ideally, firms should aspire to identify problems in either the issue or incident stage, and before losses hit the balance sheet. Let's examine these concepts in our EGB example.

An 'issue' has arisen within the bank that can be tagged to a risk indicator that tracks a capacity/usage ratio. If the head of information technology is ignored, then the system may begin showing signs of over-use and minor outages might occur. These 'issues' have not yet materialised into actual incidents – but this outcome is possible if the issue is not addressed. Outages that do not result in quantifiable losses can be considered 'incidents'.

If problems are not dealt with at the issue stage, they often move on to become actual realised events – perhaps not serious events that result in monetary losses, but serious enough to indicate that something is amiss within the organisation. These fictional outages could be tracked through the use of risk indicators and are the next safeguard in the tracking and mitigation of an event. If they are ignored, a future breakdown of a significant duration may occur, and EGB would be subject to customer complaints, cancelled contracts, lost business opportunities, mitigation expenses and regulatory fines. The result of all this is a measurable, and perhaps painful, monetary 'loss'. The losses incurred by EGB may be substantially greater than the \$1 million of development costs that the head of IT had recommended. The cost of potential losses can be estimated by an examination of past losses (perhaps by an examination of cases in a loss database). Risk indicators pro-



Risk indicator 1: above-market returns

Kidder Peabody offers an example of circumstances involving above-market returns in a trading operation.

The Joseph Jett bond-trading scandal on Wall Street in 1994 was one of a series of problems that plagued Kidder Peabody and eventually prompted the sale of the once highly-profitable firm.

The US Securities and Exchange Commission accused Kidder of lax supervision, poor management judgement and creating an environment where "employees were unwilling to ask tough questions when money was being made".

Jett was the head of Kidder's government bond trading desk, and billed as a rising star.

It was eventually discovered that Jett had faked \$350 million in profits, and hid \$85 million of real losses.

He was dismissed after his superiors became convinced that he had generated false profits and caused the firm to report hugely inflated earnings. In a very short time, Jett went from being Kidder's 'Man of the Year'

(in 1994) to the catalyst of its failure. He was later partially exonerated by a 1996 arbitration panel that determined he was under the impression – no matter how mistaken – that his trades were making money.

He claims that his trading practices involved the legitimate use of computer-model bond-trading strategies, while critics have labelled these strategies as the equivalent of a 'ponzi scheme'.

Jett's formula was a simple one: "If the strips were underpriced in relation to bonds, buy them, reconstitute them into a bond, then sell the bond. If the strips were overpriced, sell them, then buy and strip the bond."

In short, Jett would finance various bond instruments for less interest than they would later yield.

This is one of several high-profile Wall Street cases that demonstrates how a risk indicator, such as above-market returns – if tracked carefully – could help to detect brewing problems within a trading operation.

Source: Excerpted from Zurich IC Squared First Operational Risk Data Base

vide the IT professional and management with a quantifiable measure for tracking well-defined and targeted issues within a business unit or organisation.

Challenges of risk indicators

Risk indicators present distinct challenges, and they cannot be expected to function as 'drop and run' solutions.

tors and associated targets that can be applied broadly. This situation suggests that each institution will need to begin with a set of indicators that reflect the experience and personal judgement of its managers.

Once data is collected and compared with actual experience, then predictive qualities can be established and adjusted as needed. The act of selecting, back-test-

Whatever technology solutions are selected, they should help managers comprehend the meaning of the indicators. Firms should avoid collecting too much data and sustaining information 'overload'

Often the most dangerous problems are discovered only in retrospect, and after actual losses have occurred or been narrowly averted. Significant back-testing needs to be undertaken in the industry and within each institution to establish the effectiveness of indicators. Because each institution has a different culture, risk tolerance, business mix and organisational structure, there is not a standard library of indica-

ing and adjusting risk indicators will provide invaluable insight and knowledge into an institution's operational risk profile.

The use of risk indicators does not necessarily require a significant investment in systems and data collection software. Indicators can be tracked in spreadsheets or commonly used data management software produced by established vendors. Whatever technology solutions are selected, they should help managers comprehend the meaning of the indicators.

Firms should avoid collecting too much data and sustaining information

'overload'. A useful approach is often the preparation of a high-level summary of a firm's overall risk profile, using a combination of key words, arrows and primary colours.

Of course, whenever you ask managers to expose flaws in their units, there is the temptation to soften the details. Managers might be tempted to classify data so as to display their departments in a positive light or, conversely, to categorise events such as near-misses or other problems as mitigated by their adept management skills (the 'rescuer' syndrome). Other difficulties might arise if senior executives manage to indicators rather than to real risks. And management might become too focused on 'the numbers' or indicator levels, and respond by allocating attention and resources to problems that are not likely to occur again, instead of devoting their energy to more pressing and potentially risky situations.

It is a complicated task to classify data and create loss hierarchies and related taxonomies that reflect the risk profile of an organisation. Indicators are often derived from prior loss events. A common practice is to aggregate the performance of individual indicators into an overall score. For instance, a trading unit might settle on 15 different relevant indicators, including failed trades, percentage above or below average market returns, number of unauthorised trades, etc. These indicators might then be amalgamated, using various methods, into a single indicator that would later be aggregated with indicators from other business units, and included in a top-level risk report.

There are further challenges faced by indicators. The effort will not be successful unless it has backing from the senior members of the organisation.

This is because the business unit managers will need a mandate from their superiors in order to embrace the cultural changes that come along with the deployment of an operational risk programme. Otherwise, the effort needed to be successful will be either actively or, perhaps more dangerously, passively blocked at the business unit level. Significant work and initial investment will be required by an organisation, both at the outset and

Risk indicator 2: number of unauthorised trading incidents

Griffin Trading Company offers an example of unauthorised trading.

In a people-related risk case, Chicago-based Griffin Trading Company was declared in default on December 24, 1998, after John Park, one of the firm's London-based clearing clients, lost £6.3 million (about \$12.3 million) trading German government derivatives. John Park was a trader with a firm called GLH Derivatives that used facilities provided by Griffin. Park took such large positions in the Eurex market on December 21-22, 1998 that both Griffin and GLH were unable to meet his trading obligations.

Griffin and GLH consequently ceased operations, and Griffin went into immediate liquidation. Park was in serious violation of his proscribed limits: he had bought about 9,000 lots of German Bund futures - 10 times his limit of 900 contracts.

The first 900 trades were traded through Griffin, while the rest were made through Eurex executing broker Tullett & Tokyo, a London-based firm. When the market fell from its opening

position of 116.29 on December 21, 1998, to a closing position of 115.25 on December 22, 1998 - Park had lost millions.

Park had exceeded his limits on a regular basis between July and December 1998, and there is evidence that Griffin's management was aware of this, but failed to take appropriate action.

After the loss surfaced on December 22, 1998, Griffin was forced into bankruptcy and was closed by the Securities and Futures Authority (SFA) in London. The SFA ruled on February 19, 2001 that Park was unfit to be registered as a broker in any capacity.

The SFA also found a senior officer of Griffin negligent in his failure to manage and control Griffin's risks. As well as failing to implement adequate controls over the company, he did not monitor trading limits and concealed losses from his firm's senior management. Griffin's compliance officer was found to have neglected his duty to act with due skill, care and diligence.

Source: Excerpted from Zurich IC Squared First Operational Risk Database

over time. The entire process - from beginning to end - must be detailed at the start so that all parties understand the expectations. A well-stated and comprehensive plan can reduce arguments and help avoid resistance to the effort.

Often firms start a process such as an indicator programme with great enthusiasm, but lose interest or cannot sustain the effort. After the initial burst of enthusiasm, firms may lose sight of long-term benefits. Changes in senior management can also stymie an indicator effort, as can mergers, staff changes, lack of feedback from senior management or general inaction. Senior management may question the expense or necessity if earnings fall and cost-cutting is imposed. To obtain the benefit, firms need to remain disciplined and focused on their ongoing efforts. This requires time and a change in behaviour.

Managers and staff also need to understand the importance of the undertaking. If the initial data is not properly categorised and identified - and managed by an employee who does not understand the business - the top-level indicators will be jeopardised. Data collection and categorisation is best not delegated to the most junior employees and tainted with the label of 'data entry', since it offers the greatest opportunity for missteps. Moreover, the process must be subject to independent scruti-

ny and review by internal audit. This extra step will also lessen the temptation to 'cook the books'. Once data is collected and quantified, it tends to become legitimised and serves as the basis for future decision-making. It is difficult to unravel the decision-making process and discover the false inputs once the data is accepted as 'fact'.

Data collection

Data collection, moreover, presents its own special challenges. Some data can be collected manually, but other data already exists within a bank and it is a matter of finding where it resides. For example, employee turnover data is generally collected by a human resources department. The number of security incidents are usually tracked by a security and investigations unit (internal incidents of fraud, failed background checks on employees, missing funds, etc). It might be a matter of identifying the likely data sources within a firm and purchasing or building the software systems that will offer aggregation and reporting capabilities.

Candidates for risk indicators can exist in various places:

- human resources (employee turnover, employee sick days, employee errors, aggregate grading of employee reviews)



- security and investigations (failed background checks, internal and external incidents of fraud, number of employee reported incidents)
- legal (number and amount of lawsuits, fines and warnings from regulatory agencies, employee-initiated discrimination claims, customer-initiated legal actions)
- middle and back offices (transaction volumes, transaction activity and other related data)
- financial controllers (financial and accounting related indicators).

Conclusion

Indicators are not a substitute for a fully realised risk management programme. They are an essential component of the process, but not the process itself. Indicators can only be effective if a firm has a commitment to create a culture of risk awareness, starting at the top level of the firm. Firms need to commit to the necessary resources and 'risk intelligence' in order to act upon information gathered from indicators.

This means using the data to assess a firm's approach and change course as needed. Adjustments may be needed

during the gathering, analysis and testing of risk indicators. Every activity in the process affects both what has come before and what will come later.

Indicators are invaluable if properly used and interpreted. If they are used other than as an education and information tool, if they are not re-examined on a continual basis and redesigned as information is tracked and interpreted, then they become obsolete and ultimately irrelevant.

Monitoring risk and establishing indicators is highly iterative: indicators are selected and, over time, they start informing the decision-making process itself, which in turn informs the complexion and character of the indicators. The 'informing process' is a large part of risk management – this is not a discipline that fares well under a 'drop it in and forget about it' approach. If indicators are used as information tools, then over time a risk management culture will become richer and more ingrained within an organisation, helping to promote outcomes that all firms seek – the avoidance of serious direct and indirect losses, a culture that promotes ongoing improvement, the achievement of a competitive advantage and increasing value for stakeholders. □

Charles Fishkin works for KPMG LLP and Penny Cagan works for Zurich IC Squared, a subsidiary of Zurich Financial Services Group. Both are based in New York and members of the operational risk committee of the International Association of Financial Engineers (IAFE).

All information provided is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation. The views and opinions are those of the authors and do not necessarily represent the views and opinions of any other organisation, including KPMG LLP, Zurich IC Squared or the IAFE