

Standard operating procedures

Operational risk and bank decision making: putting Basle into perspective

Specific rules for the capitalisation of operational risk are one of the more controversial features of the proposed revision to the Basle Capital Accord. How should banks start to address them? By Penny Cagan

The past decade has witnessed dramatic changes in the global banking industry. Increased cross-border activity, consolidation, regulatory reform and technological innovation have all played their parts in encouraging greater transparency, liquidity and uniformity of the international standards applied to the banking industry. At the same time, the boundaries between the different sectors of the financial services industry have begun to crumble. Companies such as Sony and Ikea are also pushing the reaches of the industry and establishing banking enterprises that more closely resemble consumer businesses than financial ones.

Wherever there is change, there is risk. In the case of the financial services industry, trading in new markets generates new market risks; lending to new borrowers results in new credit risks; and embracing new business processes and policies leads to new operational risks. The pace of change in recent years has translated into a pressing need to open up discussions on how to measure and manage all these new threats – and to revisit some of the not-so-new ones that continue to plague the industry.

And besides the industry's inherent incentives to master the management of operational risk, there is also regulatory pressure being applied. What should banks do about all the documents coming out of Switzerland? Or perhaps a more appropriate question is: which banks

should do anything about the documents coming out of Switzerland? Should middle-tier banks even care what the Bank for International Settlements (BIS) recommends in terms of capital allocation? And even if they had the time or interest, where should they begin in addressing those recommendations?

This article will discuss the implications of the BIS proposals for smaller banks, some parts where this sector may want to challenge the consultative paper and where to begin when designing an operational risk programme. Let's begin by briefly reviewing the definition of operational risk, and what the consultative paper proposes when it comes to the capital that should be held to cushion against operational risks.

Defining, measuring and managing

A good first step in embarking on an operational risk programme is to read the relevant supplement of the consultation docu-

ment for the revised Capital Accord issued by the Basle Committee of the Bank for International Settlements in January 2001 (available from www.bis.org). There is a lot of discussion in this document, but what is most remarkable when you read through it is how much guidance the committee is asking for from industry practitioners.

Again and again during the course of the document, the BIS requests feedback on a variety of topics. Some issues involved are very basic; for example, the discipline of operational risk management is so new that the BIS has only recently settled upon a "final" definition of operational risk. This definition, based on the one formulated by the British Bankers' Association, is as follows:

The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events

The above definition includes legal risk, but not strategic or reputational risks. But while the BIS may have heroically settled upon a definition, the industry is still arguing over exactly what it means, or how it relates to their attempts to put operational risk management on a sound footing. While this definition has eliminated some sources of uncertainty (for example, it does not include the risks arising from botched business or strategic decisions, which were implied in earlier discussions), others remain.

For example, the BIS specifically

“While the BIS has settled on a definition of operational risk, the industry is still arguing over exactly what it means”

excludes reputational risk. Reputational risk is one of the key hazards for financial services companies, whose good name is often a key intellectual property asset. Damage to that good name is one of the most difficult risks to overcome: you usually can't pay a fine or take a charge (no matter how painful) that will quickly reduce the risk to your firm's reputation.

So quantifying and capitalising reputational risk is no easy matter – and does not sit easily with attempts to quantify and capitalise many other forms of operational risk, such as systems failures or payment errors. That, in turn, has led to suggestions that reputational risk should not, in fact, be considered operational risk. Given these kinds of questions, would-be practitioners can be forgiven for frequently asking: "How can I manage something when there is not even industry agreement over what it is?"

Part of the answer is that operational risk *measurement* is not the same thing as operational risk *management*. Quantifying those operational risks that lend themselves to quantification and neglecting the rest does not constitute best practice in operational risk management. As we will later discuss, and as the BIS consultation document acknowledges, there is a pronounced need for greater discussion (and management) of the qualitative aspects of operational risk.

So far, however, the banking industry has largely focused its efforts on coming up with measurement techniques that will allow it to take advantage of the "evolutionary" capital regime proposed by the Basle Committee on banking risks. But the best measurement techniques and capital models in the world will not reduce operational risks unless used in co-ordination with inherently solid management processes. While these techniques may assist firms in reducing their capital charges, allowing them to deploy their hard currency elsewhere, they remain

exposed to risks that can harm (if not destroy) their reputations, or severely impair their liquidity and ability to meet financial commitments.

Most risks to financial firms divide into expected losses (covered by reserve provisions), unexpected losses (covered by regulatory and economic capital), and catastrophic losses that must simply be prevented by internal controls, or transferred using insurance or ART instruments. The problem in devising rules for the capitalisation of operational risk is that as yet, it is quite unclear what proportion, and type, of operational risks fall into each category – and the boundaries keep moving as the industry changes.

To take a classic example, the management of Barings Bank were reportedly warned of the dangers of putting Nick Leeson in charge of both trading and settlement at a remote outpost with little additional oversight. They clearly felt that the operational risk involved was minor – but were proved dramatically wrong when it came to light in 1995 that Leeson

“The best measurement techniques and capital models in the world will not reduce operational risks unless used in co-ordination with inherently solid management processes”

had built up, and systematically concealed, a huge loss-making position. The operational risk had turned out to be catastrophic.

The most effective control over that risk would have been a change in organisational structure, not capitalisation. Today, a number of firms offer "rogue trader" insurance – which could be viewed as a

form of capitalisation against operational risk. However, it is unlikely that they would agree to provide cover to companies with internal controls as botched as Barings'. So operational risk management, in this case, is about internal controls, not about quantification and capitalisation.

More generally, it is important to consider quantification and capitalisation of operational risk as just one of many tools in the establishment of a viable programme. The reality is that all banks need to consider at least rudimentary approaches to operational risk capital, even where these do not lead to regulatory benefits; while operational risks are perhaps less tangible than market or credit risks, they have been responsible for some of the biggest losses in history (See table A, following page).

Three approaches

So what does Basle's consultation document say about operational risk? In the 1998 Accord, the Basle Committee made an implicit assumption that "all other risks" were included under the capital buffer related to credit risk. In its new recommendations, the committee proposes rather more accurate and complicated methods for calculating capital charges for credit risks, and has for the first time attempted to deal with operational risk as an entity in its own right.

It is important to note that it is presently unclear whether all of the national bank supervisors who applied the original 1988 Capital Accord will require all of their regulated institutions to meet the proposed BIS standards. The US Federal Reserve is still considering this issue and there has been recent conjecture that it may not require smaller banks to adhere to the newer capital requirements.

The mission for those banks that do eventually fall under the purview of the Basle guidelines is to quantify operational risk in order to set aside capital to cover

A. Top 10 Operational Risk Disasters

Source: IC Squared First

1. BANK OF CREDIT & COMMERCE**INTERNATIONAL, 1972-1992 (\$32 billion)**

In 1991, The Bank of Credit and Commerce International (BCCI), sustained a \$17 billion "black hole" loss in its accounts, while regulators from the Bank of England seized another \$15 million in assets after one of the most complicated webs of financial misdeeds ever recorded came to light. Evidence had allegedly surfaced that BCCI had a secret inner circle of operators, mostly in Pakistan where it was founded, who apparently financed drug running, money laundering, bribes, terrorism and other illegal activities.

Event trigger: Banking fraud**Contributing factors:** Improper management practices, failure to set proper limits**2. LONG-TERM CAPITAL MANAGEMENT, 1998 (\$4 billion)**

The significance of the events surrounding the collapse of Long-Term Capital Management and its subsequent loss of \$4.4 billion should not be underestimated. The breakdowns at LTCM include overexposures to leverage, sovereign, model, liquidity and volatility risks. The chain of events that led to the firm's demise began with Russia's announcement on August 17, 1998, that it was "restructuring" its debt, or lengthening the terms of the payout on short-term bonds. Wall Street, with a newly acquired suspicion of all sovereign instruments, witnessed a mass unwinding of credit risk positions. The effect on the market of LTCM's unwinding its position was so enormous that the Federal Reserve Bank, in a historic move, initiated a bailout of the hedge fund.

Event trigger: Model risk**Contributing factors:** Undertaking of excessive risks, general flaw in strategy**3. CENDANT CORPORATION, 1985-2000 (\$2.85 billion)**

In the largest and longest-running accounting fraud case in history, three former executives of Cendant Corporation pleaded guilty on in June 2000 to federal fraud charges. The related activities are conjectured to have occurred over a span of 12 years, during a period that saw the tiny Compu-U-Card company become CUC International, and ultimately, through a series of mergers, the Cendant Corporation. The executives who admitted to charges of doctoring the books and overstating revenues contend that it was part of the company's culture to do so. Funds were shifted from merger reserves in order to prop up earnings, and when the reserves were depleted due to bad investments, the company simply acquired additional targets. Cendant has agreed to a \$2.85 billion settlement of a class-action suit in the largest such settlement in history.

Event trigger: Relationship risk**Contributing factors:** Accounting fraud, employee misdeeds and practices, insufficient compliance measures and improper management practices**4. SUMITOMO CORPORATION, 1989-1999 (\$2.6 billion)**

Sumitomo's star copper trader, Yasuo Hamanaka lost \$2.6 billion over 10 years in unauthorised copper trading for Sumitomo Corp. He was found guilty of fraud, falsifying permission to trade above his limits and illegally accessing funds.

Event trigger: Unauthorised trading**Contributing factors:** Employee misdeeds, lack of dual control, failure to supervise employees**5. PRUDENTIAL INSURANCE COMPANY, 1982-1995 (\$2 billion)**

A class action suit by 10.7 million customers and affected policy holders complained that the company's agents had talked them into buying life insurance policies that they did not need. Prudential settled and returned an estimated \$2 billion to policyholders in the form of rebates and enhancements to existing policies.

Event trigger: High pressure sales tactics**Contributing factor:** Improper management practices**6. ORANGE COUNTY, 1991-1994 (\$1.6 billion)**

In December 1994 Orange County in Southern California announced publicly that its investment pool had suffered a \$1.6 billion loss. This was the largest investment loss ever registered by a municipality and led to its bankruptcy and the mass layoff of municipal employees. The loss has been blamed on the unsupervised investment activity of county treasurer Robert Citron, who had previously delivered returns that were 2 per cent higher than other municipal pools in the state of California, and was viewed as a "wizard" who obtained better-than-average returns in difficult market conditions. He placed a bet through the purchase of reverse repurchase agreements that interest rates would fall or stay low. The strategy worked until February 1994, when the Federal Reserve undertook a series of six interest-rate hikes that generated huge losses for the fund.

Event trigger: Market fluctuations**Contributing factors:** Failure to question above-market returns, insufficient compliance measures, undertaking of excessive risks**7. SHOWA SHELL SEKIYU 1989-1993, (\$1.5 billion)**

In a people risk situation, Showa Shell Sekiyu KK, a major oil refiner in Japan, faced losses of 165 billion yen from forward currency transactions. The company's treasury department, expecting the US dollar to rise against the yen, began buying forward dollars on futures markets at around 145 yen. Unfortunately, the dollar decreased to 120 yen in 1993, causing huge exchange losses for the firm. From 1989 until 1993, the treasury department, hoping to recoup as yet unrealised losses, expanded its forward buying position in excess of the amount allowed by internal company rules. To conceal these losses, the department rolled over the settlement of its positions, which increased the amount of unrealised losses because the yen continued to rise in value relative to the US dollar.

Event trigger: Unauthorised trading**Contributing factors:** undertaking of excessive risks, employee action**8. PRUDENTIAL SECURITIES INC, 1981-1990 (\$1.4 billion)**

Prudential Securities settled charges of securities fraud with state and federal regulators in 1994. The settlement stemmed from charges of improper management practices, sales misrepresentation, and an executive management structure that promoted profits above all else. It also damaged the reputation of its parent insurance company,

which had managed to survive for more than 100 years without serious scandal. The problems are blamed on an aggressive incentive structure that encouraged Prudential's brokers to sell limited partnerships without regard to whether they were appropriate for their clients. In October 1993 Prudential Securities settled civil charges with the SEC, the National Association of Securities Dealers, and 48 state securities regulators. Prudential initially paid out \$371 million under the pact, which included a \$330 million settlement fund for investors and a \$4 million fine. In 1995 the firm pleaded guilty to securities fraud and was placed on three-year probation. The settlement also allowed investors who did not participate in the earlier class-action suit to press charges, and opened the firm to future additional losses. The firm ultimately added another \$300 million to the \$300 million restitution fund that was put into place.

Event trigger: Sale misrepresentation**Contributing factors:** Insufficient compliance measures, undertaking of excessive risks, improper management practices**9. DREXEL BURNHAM LAMBERT, 1988-1993 (\$1.3 billion)**

On September 29, 1993, a \$1.3 billion "global" settlement went into effect for all claims pending against Michael Milken and more than 200 present and former officers and directors of Drexel Burnham Lambert and other entities related to the firm. Drexel's problems began in 1988, when former employees filed a class action suit charging the company with fraud, breach of duty and negligence in connection with employee purchases of the firm's common stock, which was not publicly traded. The suit attempted to recover losses sustained by the stock's purchasers when the value of shares was substantially reduced. The company's problems were compounded in 1989, when three employees charged Drexel's top managers with breach of contract and violation of their fiduciary duties.

Event trigger: Misappropriating funds**Contributing factors:** Weak crisis management, management inaction, improper management practices**10. DAIWA BANK, 1983-1995 (\$1.1 billion)**

On September 26, 1995, Daiwa Bank announced that it had lost \$1.1 billion since 1983 due to unauthorised trading. Toshihide Iguchi, an employee with the bank's New York branch since 1976, was in charge of both securities trading and the custody department, and used these positions to carry out and cover up his alleged scheme. He continued to do so until July 17, 1995, when he wrote a confession letter telling bank officials about his unauthorised trading losses, which had reached \$1.1 billion. Four days later, he sent a second note to management detailing ways to cover up the incident. Daiwa acknowledged the letters and informed Japanese officials of the loss on August 8. They waited until September 15 to pass the information on to American regulators, and publicised the loss 11 days later. When Daiwa confessed to covering up the scandal, the Fed revoked its US charter.

Event trigger: Unauthorised trading**Contributing factors:** Employee misdeeds, lack of dual control, lack of proper segregation of duties ■

future losses. The expectation is that around 20 per cent of all bank capital will be allocated to operational risk, but individual banks may hold more or less than this proportion according to the sophistication of their operational risk management. In the spirit of the discussion above, the discretionary element of regulation means that capital discounts will only be given to banks that can both demonstrate their ability to measure operational risks, and also their ability to control and manage them.

The Basle Committee is recommending an "evolutionary approach" to the quantification of operational risk capital. In essence, it specifies three approaches, based on the supposition that the appropriate capital charge for a typical bank will diminish as it takes progressive steps to address operational risk. This essentially allows banks to make increasingly large discounts to their regulatory capital as they make demonstrable progress towards a well-managed and properly controlled operating environment. Given that banks today vary widely in their preparedness, different banks will start at different points on the scale.

The crudest approach, known as the single indicator approach, is designed for less sophisticated (and usually smaller) banks. This method allocates risk capital based on a single indicator of operational risk, the default being gross revenue. It is unclear if gross revenue is a relevant indicator for operational risk. The single indicator approach is considered the easiest to implement, because it specifies a single number across the organisation based on a well-known quantity: in order to satisfy this approach, banks will not have to do anything! However, all other things being equal, it will likely result in higher capital charges than the other two approaches, and the hope is that banks will try to reduce these by moving up the evolutionary ladder – that is, by demonstrably

improving their management of operational risk.

The second approach, the standardised approach, is the one the Basle Committee recommends that larger and more international banks use for the time being. It is also the approach that middle-tier banks should target in order to reduce their capital charges. While the single indicator approach is a crude, across-the-board measure, the standardised approach is based on information gathered from individual business units. It is suggested in the consultative paper that this approach

“No more than a handful of banks would qualify for the internal measurement approach, largely because of lack of appropriate data”

best reflects the actual level of risk within a complicated organisation with a variety of business activities, but without invoking complex and still controversial mathematical models.

The standardised approach is inevitably more complicated than the single indicator approach. The basic principle is that banks will have to map their own business units into a standard set of business units defined by the regulator. Each of these standard units is associated with a particular financial indicator – for example, the amount of assets under management for an asset management business – and the associated capital charge is defined by the level of these indicators.

This approach thus goes some way towards reflecting the makeup of an individual institution's business, making it a

better measure than the one-size-fits-all approach based on gross revenue. Banks aiming to take this approach will have good reason to start thinking about their business lines' operational risks and how they might be best managed, but will not have to go through the laborious and complicated exercise of collecting and evaluating internal loss data required under the last, and most sophisticated, approach.

This approach, the internal measurement approach, is reserved for banks with the most sophisticated risk management controls and programmes in place. This approach breaks down the idea of indicators still further, by introducing the concept of risk types. A bank will need to provide an exposure indicator for each risk type (tied to individual business units) based on internal loss data, and the probability of a loss event occurring. This allows banks to move the capital charge for operational risk most closely into line with the actual economic risks of their business, in a way that reflects both their track record and their current operating environment.

No more than a handful of banks would qualify for this approach today, largely because of the lack of appropriate data. The Basle Committee recognises that banks will move toward this approach as they start collecting internal loss data, and that this will be a step-by-step process. Among the tasks that need to be undertaken are the establishment of industry standards for loss data and the collection of a "critical mass" of loss data by pooling internal loss information from a number of institutions.

For the moment, then, the vast majority of banks will be most interested in the standardised approach – either aspiring to it, in the case of smaller organisations, or ensuring compliance with it, in the case of medium-sized and larger institutions. The standardised approach is in any case a

natural precursor to the internal measurement approach, so even banks aiming higher will find it useful to work through the requirements of the standardised approach.

Please refer to Box B for a discussion of the business line approach. Interested readers are encouraged to respond to the Basle Committee with their views before the May 31 consultation date: in this area, more than most such regulatory consultations, it is particularly important that a diversity of views be heard.

Getting started

Assuming that an appealing form of the

standardised approach is eventually implemented, where does that leave banks? It is likely that many will fall into the first tier in the beginning and be hit with the highest capital charges. It is also possible that many moderately sophisticated banks will be able to move quite quickly into the second tier once they have demonstrated they have the proper controls in place. In order to qualify for this stage, the banks will have to demonstrate the establishment of an operational risk management and control process, and a strategy for mapping an individual bank's business lines into the standardised formula.

The BIS suggests the adoption of numerous "qualitative" items in a bank's quest to manage its operational risks. These items include:

- the establishment of a risk reporting system;
- the need to establish an independent operational risk management and control process (which usually involves either a risk management, internal audit or financial operations function); and
- the need to identify those historical loss events that are appropriate for an individual institution and its business units (which involves the use of an external loss database).

B. The Business Line Controversy

THE BASLE COMMITTEE'S consultation document includes a table, intended for use under the standardised approach, which stipulates a set of business lines along with appropriate loss types and exposure indicators.

This table is presented as an example of how business units might be mapped. The Basle Committee is advocating that a continuum be maintained between the standardised and internal measurement approaches, and the same business unit categories used for each.

What differs in the latter approach is that a broad set of exposure indicators are additionally assigned to each business unit. For instance, the volume of new deals might be an exposure indicator for investment banking, and volume of transactions might be the appropriate indicator for commercial banking. It is then recommended, under the internal measurement approach, that using a combination of business line/loss type, the banks calculate the probability of loss events. The committee has invited comment on the exposure indicators (or risk indicators) and the loss types.

The business line approach has sparked a great deal of controversy within the industry, with some labelling it "woefully inadequate" for the task at hand. A key objection is that it is entirely predicated upon the application of a single, standardised set of theoretical business units to real-life businesses that may vary widely in their activities, operating environments and risks. And, the thinking goes, no matter how comprehensive the standard framework is – and the structure suggested by the Basle Committee is on the meagre side – there will never be a set of

business units that adequately reflects those of all real organisations. Banks fear the prospect of having to rearrange their organisational structures and business lines to qualify for the standardised approach.

And even if a business line approach were adopted, the one presently being put forward by the BIS is at least problematic in its current incarnation. For instance, the recommended structure for investment banking does not adequately reflect the structure of these business units in many organisations. Trading & sales is more closely aligned with money management functions in some organisations than it is with investment banking. In other organisations, there is a clear division down the middle between investment banking and capital markets.

And while it is suggested that corporate finance be lumped into the same category as municipal finance, government finance and merchant banking, the risks associated with these categories are very different. Should corporate finance include transaction work, such as mergers and acquisitions? This type of business activity, including merchant banking that often encompasses private equity and leveraged buyout activities, can, in the real world, incur an entirely different class of risks to offering advice on restructuring.

The same difficulties hold true for other recommended business lines. It is assumed, for example, that "private banking" can be lumped in with "retail banking", but these categories and their inherent risks are entirely disparate. For instance, private banking, especially in an entrepreneurial culture, can be associated with

huge risks, particularly with international clients. And this brings up another concern: how do you make allowances for the risks associated with different geographic areas? Does a private banking unit that solely does business with US clients hold the same risk as one focused on Latin America?

One alternative would be for the BIS to undertake a product line approach rather than a business line approach. This would be a more flexible way of establishing standards that would be workable for a larger population of banks, and does not assume that every bank looks alike. For instance, if the BIS were to adopt this approach, it would be much easier to extrapolate the loss data and apply the lessons learned from one relatively standardised product type to another, rather than trying to leap from one idiosyncratic business unit to another.

It is not yet too late, however, for this to change. The Basle Committee has requested commentary through May 31, 2001, and has said that it will work with the industry to refine the framework.

This is the time for risk officers, senior executives, chief financial officers and others associated with the banking industry to take a look at their own institutions' business line structures and determine if what is being recommended is workable.

The committee needs to hear a diversity of opinion from all sectors of the banking community. If this is not forthcoming, banks may in practice have to choose between the "one-size-fits-all" single indicator approach and a "many-sizes-fit-few" standardised approach. ■

None of the above items are overly exotic or difficult to implement – they can involve home-grown or external remedies in each case. What is important to understand is the stress on a rigorous control environment. To reiterate: operational risk quantification is not the same thing as operational risk best practice. For all the discussions on business lines and product types, the important thing from both a business and regulatory perspective is to get started. And getting started does not have to be an expensive or grand gesture, and need not necessarily involve elaborate software or theoretical models.

A widely circulated report published last year by Meridien Research breaks the operational risk management process down into four components (the quotations are from Basle's consultative document):

■ **Identification:** "Banks must have in place a sound process to identify in a consistent manner over time the events used to construct a loss database and to be able to identify which historical loss experiences are appropriate for the institution and representative of their current and future business activities."

■ **Tracking:** "Banks must develop rigorous conditions under which internal data would be supplemented with external data, as well as a process for ensuring relevance of this data for their business environment."

■ **Measurement:** "As part of their validation process, scenario analysis and stress testing would help banks in their ability to gauge if the operational environment is accurately reflected in data aggregation and parameter estimates."

■ **Management:** "One growing mitigation technique is the use of insurance to cover certain operational risk exposures. During discussion with the industry, the committee found that firms were using, or were considering using, insurance policies to mitigate operational risk."

Some of these might look formidable challenges for the average bank. The good news is that only the first, identification, is required by the standardised approach. The others are only required under the internal measurement approach. It has been suggested that it takes banks two to three years to move from stage to stage. This means that there is no time like the present to get started.

Risk identification

Risk identification is a good place to start for a bank that wants to qualify for the regulatory capital discounts allowed by the

“Risk identification is a good place to start for a bank that wants to qualify for the regulatory capital discounts allowed by the standardised approach”

standardised approach. One of the most efficient ways to identify key operational risks is the use of risk profiling workshops that gather individuals to talk about "what keeps them up at night". This qualitative scenario building (as opposed to the quantitative scenario building mentioned above) provides a quick way to get started on an operational risk programme – certainly quicker than the year or two that it will take to amass any meaningful amount of internal loss data.

This involves a multidisciplinary team approach that brings together employees and management within an organisation for guided sessions on what they perceive to be risks within that organisation. The approach here is predicated upon the assumption that there is a knowledge and

wisdom base within all organisations that can provide powerful feedback for the purposes of mapping risks. The process will not only increase the overall level of risk awareness throughout the organisation but has proven to be an effective communication tool for the purposes of change (and hence operational risk) management.

Another approach, which is less dynamic than risk profiling, is self-assessment. This approach, however, is a second-best tool for risk identification if an organisation lacks access to risk profiling techniques. The goal is to identify risks, and there is no one who can do this better than the people who work on the front lines, in the business units. They are the people who sweat over the "near misses" and the people who gripe among themselves around the water cooler about problems that just never seem to get addressed by senior management.

The results of self-assessment can require some skill and common sense to analyse, since individuals may have all manner of conflicting incentives when it comes to disclosing risks. However, it can be as simple to carry out as sending questionnaires to employees and asking them to identify and/or rank risks that they perceive to be the most intrinsic and/or dangerous to their business units. Some approaches assign grades to each answer and monitor how they waver over time. This can be used as a first step in the process of identifying risk indicators for later internal data gathering efforts.

How does it work? Say a significant percentage of employees in your computer systems department rank "aging hardware" as a key risk in keeping a mission-critical system or service running. It is then possible to extract a risk indicator from this item – age of hardware – and a threshold value: two years. You can then ask your systems department to start tracking the age of all their in-house computers; when

the average age surpasses the threshold of two years, you may have an indication that it is time to buy new machines.

Is this investigation of an apparently abstruse risk worth it? Maybe, if the cost and effort involved in gathering the information is less than the exposure to future systems crashes and associated downtime and remediation efforts. And the information cost may be quite low, if you exploit existing sources of knowledge.

If you are wondering how to determine the optimal age for computer hardware, the easiest approach is to ask your in-house experts – your team of highly qualified technologists, whose inventory records will probably also contain more information than anyone would ever want on the age of equipment. But you need also to remember that their risk ranking may be self-serving. Technologists like shiny new hardware, so you may want to balance their response with some common sense weighting factor: maybe an extra six months over their suggested thresholds?

The next steps involve tracking the risks, reporting them and building the virtuous loop that feeds the "lessons learned" back to the business units, in the hope that misses and near-misses can be avoided in the future. And these next steps can be as simple as the hardware example above. If you start identifying your risks systematically, either through the collection of internal loss data, guided profiling workshops, or self-assessment questionnaires, you are almost there.

The first of these steps is to identify possible losses within an organisation by undertaking an extensive mapping of its product or business lines. If loss data exists in-house it is possible to rank these losses by product type, and compare them to external losses gleaned from external databases or in-house research efforts. If internal loss data is not available, then it is possible to create a ranking by polling front line managers

“There are many methods for tracking operational risks. Loss data and risk indicators can be tracked using commercial software products’

about which products are most risky (judged by, say, volatility in revenue or whatever indicator is most relevant) together with external loss data.

External loss data can be a very powerful indicator of where problems lie. For instance, if your firm is about to introduce a new product, it makes sense to research the type of losses that other firms have experienced with similar products in the past. It is remarkable how patterns emerge when a series of loss events is examined – patterns that are difficult to make out on a day-to-day basis, or from the historical experience of a single institution.

By comparing external loss data (either by business or product line) to what exists within your own firm, and benchmarking it against what you have learned from your self-assessment or risk profiling exercises, you are well on your way to qualifying for the standardised approach of the BIS recommendations. Equally importantly, however, you are also on the way to having a more complete picture of the hazards that lie within your organisation.

There are many methods for tracking your operational risks. Loss data and risk indicators can be tracked using commercial software products, or simply entered and monitored in spreadsheets. (However, the larger the amount of data collected, the more precarious it becomes to work in a spreadsheet.) The next step is to estab-

lish a template and structure for the reporting and escalation process of these indicators. Some of the products on the market allow the data to be represented as "heat maps" or other graphical representations of your risk indicators, allowing indicators that are approaching the outside boundaries of the desired threshold to be spotted quickly. The groundwork done in identifying and scoping risks should then allow an intelligent and concerted effort to constrain the risk before it becomes a problem.

Conclusion

We've seen that it is not too difficult to start building an operational risk framework that would qualify for some regulatory relief under the proposed revision of the Basle Capital Accord. No doubt both discussions and efforts made in these areas will accelerate as the proposal comes closer to becoming a reality.

The one prerequisite that we have not discussed thus far is management buy-in. Like all risk management, but perhaps even more so, operational risk management requires cross-disciplinary teamwork, a willingness to challenge long-established business orthodoxies, and an environment in which people can speak freely about the risks that worry them. None of this is likely to happen unless a firm's management buys into the need for operational risk management. If they don't, a bank might as well place itself within tier one and accept the highest possible capital charge!

For example, a firm's employees are an underutilised source of risk management knowledge; their collective experience and imagination makes up a repository of institutional wisdom that is rarely tapped in a focused manner. In order for self-assessment or guided workshop strategies to tap that wisdom, however, an organisation needs to foster a culture of open communication and knowledge management.

Employees need to feel comfortable reporting near-misses to their supervisors and discussing "lessons learned" in an effort to avoid future mishaps. They also need a structure to report problems, and there needs to be a mechanism to collect their concerns and issues and translate them into meaningful indicators.

Someone within an organisation – in audit, risk management, financial management or executive management – will need to have the necessary independence to move freely among the business units and collect the data. If a structure is not put into place where problems are reported and escalated up to the appropriate individuals, then the process is a waste of effort and energy.

There is argument among industry professionals whether the operational risk management process should be driven from the bottom up (which makes sense in terms of data collection, but perhaps not in terms of business management) or the top down. Regardless of the approach, the entire process needs to be sanctioned and supported by senior management.

In conclusion, getting started usually does not involve more than the decision to "get started" and the beginnings of a dialogue within your organisation with the most senior managers possible on how to manage your operational risks. Operational risk tends to be an iterative exercise – once you take one small step you gain additional knowledge to take the next step, and that knowledge informs how you take the step after that. It is truly an evolutionary process, and one that requires a dedicated effort to establish a culture that knows how to utilise knowledge within your organisations. If you are unsure how to take this step, then you will want to turn to experts for assistance, but by all means, get started! ■

Penny Cagan is head of research at Zurich IC Squared

Key Resources on Operational Risk

Mastering Risk, *Financial Times*, www.ftmastering.com, 10 Tuesday installments, starting on April 25, 2000, and ending on June 27, 2000. This is one of the most extensive discussions of risk management ever published in the general business press. Topics include a history of risk management, decision tree analysis, value-at-risk, product liability, bribery, systemic risk, e-commerce risk, and an introduction to crisis management.

Operational Risk and Financial Institutions, Risk Publications, 1998. Brings together essays by a number of risk professionals. Includes both introductory and more in-depth discussions of operational risk. Topics include trends, measurement and management, retail banking applications, processing errors, securities fraud and model risk. The charts – covering a variety of topics including descriptions of the large loss events – are especially worth investigating.

Operational Risk: A Special Report, *Risk* magazine insert, November 2000. Includes state-of-the-art discussions by most of the prominent thinkers in the industry on operational risk methodology, systems, programmes and solutions.

Operational Risk, March 2000. A special issue published by *Risk Professional* magazine. Includes several key operational risk articles.

Operational Risk: The Next Frontier, December 1999. This study is based on a series of interviews with 55 global financial institutions located in North America, Europe, and Asia, and includes a discussion of operational risk, management structures, senior management reporting, operational risk capital, insurance strategies, and tools. An executive summary and table of contents is available at the British Bankers Association site: www.bba.org.uk/html/1154.html. The report concludes with an observation of seven major trends, including an industry-wide acceptance of operational risk management as a core competency.

Time for a New Look at Operational Risk, February 2000. Meridien Research. Includes an overview of operational risk, an appraisal of available vendor solutions and case studies. www.meridien-research.com.

International Association of Financial Engineers, www.iafe.org. The IAFE has established an operational risk committee.

Bank for International Settlements (BIS), www.bis.org. This site provides access to most BIS studies, documents, news releases, initiatives, documentation, and best practices guidelines.

Global Association of Risk Professionals (GARP), www.garp.com. Includes access to GARP documents, and discussions. Also includes a link to MORE (Multinational operational risk exchange): www.morexchange.org, the loss database GARP is developing with NetRisk (www.netrisk.com).

Excerpted from IC² Bibliography on Operational Risk Resources