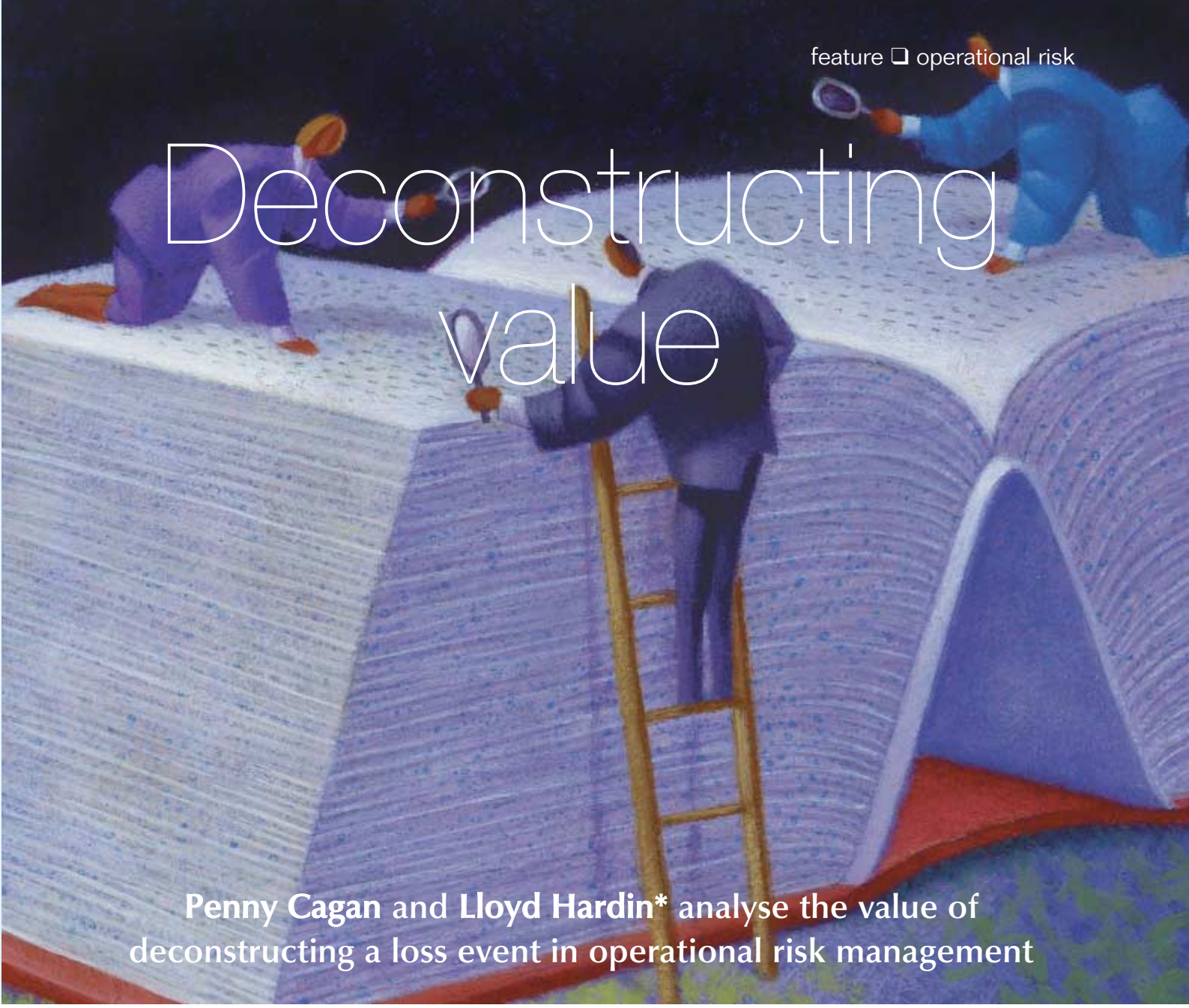

Deconstructing value

Penny Cagan and **Lloyd Hardin*** analyse the value of deconstructing a loss event in operational risk management

"To deconstruct" something has come to mean a variety of things today but, often, it is used to connote a process that "tears down" or "destroys". The term, however, can also carry a meaning that suggests a process of analysis and dissection, for the purpose of creating or reconstructing something new. As financial institutions start on the path of devising and implementing a risk and control self-assessment programme, they often overlook the value of deconstructing a loss event, with the ultimate purpose of creating and reconstructing a scenario that can be used in a variety of ways. The characteristics of an external loss event can be isolated and analysed in a process that provides context and content for a robust operational risk self-assessment programme. The full value of external loss events – beyond applications to the modeling of fat tail events – is often overlooked.

In fact, external loss events are the raw materials of risk and can provide the structure for a variety of operational risk programmes and, in particular, the foundation for a risk and control self-assessment. We will provide an example in this article of how a case study from one loss database – OpVantage First (which stands for financial institutions risk scenario trends) – can be used as a starting point in the design of a self assessment programme. The same approach can be derived from any database of external events and case studies that is available within your institution. Our goal is to demonstrate how case studies contain the raw materials that each institution needs to deconstruct loss events and reconstruct loss scenarios.

There are multiple steps necessary when designing a self-assessment programme and the examination of a single loss event or a series of related events can assist with the defining and delineation of each step in the process. An operational risk self-assessment often follows these activities: the identification of what is being assessed, the selection of relevant loss events, identification of key control breakdowns, assessments of controls through guided questionnaires, the creation of linkages between risks and controls, assessment of risks and quantification of results and the creation of action plans to mitigate risks by enhancing or modifying the control environment (see Exhibit A on page 38). A loss event can provide both the context and the content for all these steps.

Large loss events

The loss event involving Bank of Credit and Commerce International (BCCI) that came to light in 1991 is one of the largest operational risk incidents that the financial industry has ever experienced. It is also the most complex event in the OpVantage

First database of operational risk loss events. (see Exhibit B opposite). Large events, such as BCCI, can provide a meaningful framework for a loss assessment exercise. Regulators, such as Bank for International Settlements (BIS), have been very clear in their recommendations that it is important to factor in these large events into an operational risk framework. If an institution looks only at its internal events, it is most likely only considering events of small or moderate size and not factoring into its review process unexpected or more earth-shattering losses.

The industry appears to be clear on the importance of including fat-tail events in quantification models but there has been notably less discussion on their role in qualitative endeavors. Self-assessments often rely on scenarios during workshops and interviews in order to account for the "worse case" scenarios. It is powerful when analysing fat-tail events to use real events, rather than constructing "made-up" scenarios. It is difficult for those that are being "assessed" or the participants in a workshop from the institution's front lines to argue that an event could "never happen" to them if it in fact happened to someone else. Real events (and being able to say "it happened to your competitor and it can happen here") are harder to challenge during the process of holding self-assessment workshops and building enterprise-wide support than made-up scenarios.

Exhibit A: self-assessment text box:

A self-assessment usually includes the following steps:

- ❑ Identify what is being assessed (geography, product type, business unit, governance unit)
- ❑ Select relevant loss event (from an external loss database, in-house research sources and news retrieval services)
- ❑ Identify key control breakdowns as a result of the loss event
- ❑ Assess controls through guided questionnaires
- ❑ Create linkages between risks and controls
- ❑ Assess risks and quantify results
- ❑ Create action plans to mitigate risks by enhancing/modifying controls.

BCCI background

BCCI is a complex case to analyse and, hence, provides rich material for a self-assessment. It was eventually uncovered that BCCI was heavily involved in money laundering and the financing of arms trafficking. Its clients included such notable figures as former Panamanian dictator, Manuel Noriega, as well as individuals that were involved in various drug and crime cartels. The regulatory probe that eventually exposed the bank's losses was brought about by its illegal control of several US banks, including First American Bankshares. The American bank was run by two Washington insiders, who allegedly acted as front men in order to cover up for the fact that a foreign bank owned a US-domiciled one, which was a violation of US bank regulations at the time. The revelation of First American Bankshares' suspect ownership structure led to an investigation of BCCI's other activities and the bank was ultimately shut down.

Though BCCI's illegal involvement in US banking led to its investigation and exposure, the bulk of the bank's losses have been attributed to questionable loan practices. Throughout its history, BCCI made large loans to both individuals and companies, without requiring collateral or performing proper background checks. The bank covered up its accumulating losses from bad lending decisions by creating a matrix of false accounts that hid the losses for years. This fraudulent activity combined with large numbers of poorly performing trades to produce a total loss of $17 billion.

The BCCI case may never be fully understood. For the purpose of this analysis, money laundering is considered the primary trigger of the incident: the bank's untenable loan strategy and practice of hiding the massive losses that resulted through a series of overseas accounts, ultimately led to its downfall. We have used, in this article, money laundering and the bank's credit culture as the content and context for the design of a self-assessment process. (The full BBCI case is in Exhibit B)

Step 1 – establishing relevancy

When starting to design the self-assessment, the first step is to review relevant cases and establish relevancy within your own organisation. For instance, in the case of BCCI, you would first want to ask the following question: "Can money laundering happen, in any capacity, in our institution?" If the answer is yes, the case should be deconstructed so that the building blocks can be gathered before the impact or risk is assessed. If the answer is "no" you will want to continue your review of other external events until you find something more relevant or, perhaps, continue analysing the BCCI case for other issues that might present a greater risk to your own internal environment.

Exhibit B: BCCI case from OpVantage First Database

OpVantage First Operational Risk Database

Report for Loss Event 1971

Event description: BCCI

On 5 July, 1991, an incident that has been described as the biggest bank fraud in history – and which included elements of people, process and relationship risk – came to a head when regulators in seven countries raided and took control of branch offices of Bank of Credit and Commerce International (BCCI). Monetary losses from the scandal were huge, totaling $17 billion. This case developed over nearly two decades and encompassed an intricate international web of financial institutions and shell companies, which escaped full regulation, and were reportedly involved in a number of suspect transactions, in addition to legitimate banking activities. BCCI's scheme was so complex that, even a decade after the institution closed, its activities are not completely known.

BCCI was founded in 1972 by Agha Hasan Abedi, a Pakistani banker with Arab backing. The institution was chartered in Luxembourg but was headquartered in London and had branches and subsidiaries in 70 countries. This multi-national platform supported a conglomeration that became increasingly complex over time. BCCI's international nature helped the company avoid a large amount of regulation because no one country had full jurisdiction over the firm.

This point is pivotal to understanding why BCCI's problems were overlooked for so long by so many outside agencies. Although institutions such as the CIA and the Bank of England reportedly had some knowledge of BCCI's activities before the scandal broke, regulators worldwide were unable to take action against the bank because inadequate communication among agencies prevented the spread of vital information on its activities. Regulation was made even more difficult by the high-level government connections that BCCI's leaders cultivated. Although they may not have endorsed the bank's activities, various government players were often willing to overlook signs that could have exposed the scandal before 1991.

One such signal was the bank's involvement in money laundering and financing of arms trafficking. BCCI's presence in the Cayman Islands made it a useful route for tainted funds. Clients included such notable figures as former Panamanian dictator, Manuel Noriega, as well as individuals who were involved in various drug and crime cartels. American enforcement officials uncovered evidence of these transactions by 1983 but did not act on them until 1988. At that point, the US Custom's Service completed an undercover operation that led to the arrest of several BCCI figures, who were convicted of money laundering on 29 July, 1990. The bank itself pled guilty to the laundering charge and was fined $14m.

BCCI's use by cartels was just one facet of a much larger event. The regulatory probe that exposed the bank's losses was brought about by its illegal control of several US banks, particularly First American Bankshares. This regional bank was based in Washington, DC, and ostensibly run by two high profile Washington insiders, Clark Clifford and Robert Altman. Because US regulators would not permit BCCI to buy US financial institutions, the bank used Clifford and Altman as front men, to hide its involvement. When this scheme was exposed in 1991, the revelation triggered an investigation that exposed many of the bank's other illegal activities and, ultimately, brought the firm down. In the wake of the scandal, First American was sold, in part, to First Union Corp, and another BCCI acquisition, National Bank of Georgia, was sold to South Trust Corp. Also associated with BCCI were Independence Bank, in California; CenTrust, a Miami-based thrift; and Capcom Financial Services, a trading company through which BCCI reportedly lost hundreds of millions of dollars. These three institutions eventually folded.

Though BCCI's illegal involvement in US banking led to its investigation and exposure, the problem that created the bulk of the firm's losses was fraud, particularly questionable loan practices and record-keeping. Throughout its history, BCCI made large loans to both individuals and companies and did not properly secure them. When these loans went bad, the bank had no legal recourse and was forced to absorb the losses. This "strategy", which ran counter to common sense and all principles of good lending, racked up huge losses for BCCI. The firm covered this problem by creating a matrix of false accounts that hid the losses for years. This fraudulent activity combined with large numbers of poorly performing trades to produce a total loss of $17bn.

When BCCI's problems were uncovered in the 1991 probe, regulators in seven countries moved quickly to take over the bank's branches. On 5 July, offices in the UK, US, France, Spain, Switzerland, Luxembourg and the Cayman Islands were seized and the bank's business activities were frozen. BCCI's assets were ultimately liquidated and a pool was established to reimburse depositors who had lost their funds when the bank shut down.

The BCCI case may never be fully understood. For the purpose of this analysis, money laundering, a subset of the external risk category, is considered the primary trigger of the incident: the bank's untenable loan strategy and practice of hiding the massive losses that resulted through a series of overseas accounts, were the problems that ultimately led to its downfall. These were compounded, though, by many other elements, including a bad trading strategy that created further losses. This factor brought in an element of market risk, which falls into the category of process risk. The case also involved several types of relationship risk, including BCCI's numerous regulatory violations and legal liabilities and its negligence in protecting the interests of depositors who were not wealthy or well-connected. Other contributory factors included omissions on the part of regulators, who should have taken action against BCCI long before 1991 and organisational gaps, which confounded outsiders who tried to sort out the tangle of the bank's subsidiaries.

While volumes could be written based on the existing knowledge of BCCI's activities, there are still shadowed areas that may never be illuminated. The extent of the bank's involvement in cartel activity, for example, is impossible to quantify accurately and the intricate connections among the people and companies associated with BCCI defy understanding. Add in the myriad triggers and contributory factors, and the $17bn price tag, and the BCCI saga is – so far – the biggest bank fraud in history.

A deconstruction of the BCCI case would be relevant to a number of business units, geographic locations and governance issues. For the purposes of this article, let us consider a cash management unit of a large bank. A search of the First database by "cash management services" would turn up 112 events, the largest of which is the BCCI case. The next step would be to read through and dissect the BCCI case and to identify the primary control breakdowns.

For the purposes of simplicity, we have analysed one event. However, there are many more events listed in the First database for cash management (see Exhibit D opposite). Often there are patterns that emerge among a series of events or commonalities that are not always apparent from a single event. Single events can also be challenged as a "one-off" incident that could "never happen here". However, when you examine a series of events, often the same control failings occur again and again – such as lack of supervision, failure to question above-market returns and failure to establish dual controls.

It is more difficult to challenge the relevancy of the self-assessment exercise when a pattern is demonstrated among a group of events. For instance, many of the events in the First database include the control breakdown: "failure to report transactions". This is one of the control failings evident in the Allied Irish/Allfirst and Barings unauthorised trading events. Items that are initially overlooked, like "failure to question above market returns" become powerful risk indicators in their own right (for instance, the percentage above or below the average return can be used to track operational risk problems) when they are shown to reoccur in a number of similar events.

Step 2 – identifying control breakdowns
Once the primary control breakdowns are analysed, the next step is to target the ones that are most relevant to your own institution. A review of the BCCI case in the First database includes the following control breakdowns: inadequate due diligence, failure to set proper limits, failure to report transactions, improper management practices and lack of supervision. A set of best practices documents is available for each of the control issues, either from regulatory agencies, industry associations or in-house sources including compliance, audit and legal.

For control issues involving "due diligence" there are numerous best practice and 'know-your-client' documents available from international and national bank regulators. For instance, BIS published a document entitled "Customer Due Diligence for Banks" in October 2001. This document delineates a thorough list of best practices associated with due diligence. These procedures include such items as assuring that the identify of all intermediaries acting on behalf of account holders is known and the source of all client funds is clearly identified. (see Exhibit C).

Step 3 – accessing control failures
Now that we have identified our business activity (cash management), identified a relevant loss event (BCCI) and analysed the loss event for relevant control failings (lack of due diligence), we can use the best practices we have identified for the controls as a basis for a guided questionnaire. For instance, the BIS document on due diligence practices recommends that banking institutions have clearly articulated statements of know-your-client policies and procedures. This can easily become a question that is included in a self-assessment questionnaire: "Have you received a clearly articulated statement of know-your-client policies and procedures in the last year?" Values can be attributed to each answer on the questionnaire and an overall score can

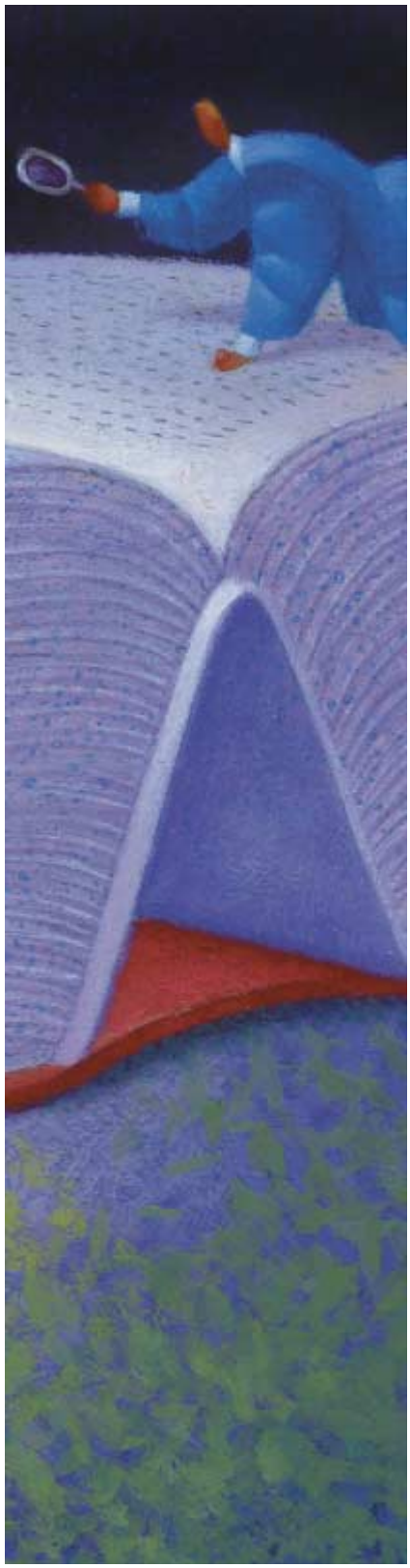

Exhibit C: Due Diligence – best practices

(source: BIS, Customer Due Diligence for Banks, October 2001, www.bis.org)

- ❑ Accounts should not be opened and approved until identity of customer is established, including the identity of intermediaries who are acting on behalf of clients
- ❑ High risk clients should be identified based on background, country of origin, public profile, linked accounts, business activities
- ❑ Source of client funds should be clearly identified
- ❑ Know-your-client procedures and policies should be distributed to all account managers and relevant persons
- ❑ Regular client identity reviews should be performed
- ❑ All new accounts should be reviewed and approved by at least one person other than account manager
- ❑ If the identity of a client can not be confirmed, the account should be closed and monies returned.

ultimately be generated for the purposes of a self-assessment, quantification or a scorecard.

The BIS due diligence document also includes a discussion of proper account management procedures, such as the signing off on new accounts by a senior manager (who is not the account manager). This requirement for dual control of an account can also become a basis for an item on the questionnaire: "Have you reviewed the identity of all new client accounts during the past year?" Again, the answer to this question can be tracked and quantified as one of the inputs from the self-assessment process.

Step 4 – reconstructing the event

Now that we have deconstructed the event and identified the relevant control and risk factors, we can start to "reconstruct" a scenario for the identified business. We have now identified the relevant risks and asked the right questions and have the necessary content and context, to analyse the risk of money laundering for our identified business, which in this case is cash management. Through discussions, review of existing loss data and modeling techniques, we are prepared to arrive at a potential risk scenario for the possibility of a catastrophic money laundering event happening in our own institution. We now know what could happen and we know why it might happen.

Once we have identified the what and why that is embedded within the events, we need to establish a prioritised mapping of what risk issues we need to address immediately and what risks we are willing to live with. This prioritisation is often accomplished through group dialogues and in self-assessment workshops where the overall needs and resources of an entire business unit, or the organisation itself, are debated and ultimately, ranked. Other methods of establishing this prioritisation include interviews and questionnaires. Regardless of how we arrive at the prioritsation, we are now ready to fix the why.

Step 5 – action plans and risk indicators

The common thread through the entire process of identifying risks and controls, and creating questionnaires, has been the external BCCI loss event. All the content we have extracted from the one loss event can now be applied to the creation, assignment and monitoring of action plans and, ultimately, the fixing of the why. For instance, one possible action plan for a problem with the cash management business unit may be the requirement that the head of the department work with appropriate representatives from the compliance and legal departments in the drafting and dissemination of a know-your-client policy document, which has to be signed by every employee who interacts with clients. An additional action plan might call for the prioritising of account reviews by country or public profile of client.

Risk indicators can function as a "barometer" for the risk management process that runs alongside a variety of efforts as a method for ascertaining the control environment. Again, the dissection of a loss event can provide inputs in the design and monitoring of risk indicators.

The BCCI thread that we have been using as a "pull through" for a hypothetical self-assessment of a cash management division can be used in the design of risk indicators. The control breakdowns that were identified for BCCI and tracked to best practices, and questionnaires, can also become inputs for risk indicators. For instance, in the case of due diligence, the following risk indicators might be relevant: amount of times per year client identities of existing accounts are reviewed, percentage of accounts closed due to inability to confirm client identity, and percentage of accounts that are not signed off on by senior non-client banking supervisors. Threshold levels can be established for each of the risk indicators. The optimal levels are established through the use of expert opinion and predictive modeling techniques.

Conclusion

In essence, what we are suggesting is that loss events become the necessary "common language" in the self-assessment process. When they are dissected they become the vocabulary that allows for a common structure to be created through identification, control assessment and reporting. Although post-mortems of large events have occurred for years in financial institutions, we are advocating a more structured and analytical approach. The deconstructing of loss events creates a basis for identifying relevant risks and considering the unexpected or the catastrophic incidents that might threaten an organisation. The reconstructing of loss events leads to the creation of relevant scenarios that answer four important questions:

- ❑ What happened in this event?
- ❑ Why did it happen?
- ❑ Can it happen here?
- ❑ What can I do about it?

Ultimately, the entire process is not dissimilar to that of analysing a work of literature, where the information gleaned from "between the lines" often informs upon and deepens the work itself. In the case of external loss events, the true lessons learned can often be found in the margins of the text and become a profound source of content and context in the design of a self-assessment programme. ❑

** **Penny Cagan** and **Lloyd Hardin** work for OpVantage at Fitch Risk in New York*

Exhibit D: OpVantage First Database