Operational risks

As operational losses tend to arise suddenly, it is possible to envisage a scenario where the counterparties do not have time to reduce their exposures, which makes the risk of systemic effects particularly large. The general opinion is that operational risks have increased considerably in recent years, partly as a result of the rapid rate of change in terms of extensive restructuring, internationalisation, new operations and new technology. In Sweden, as in the rest of the world, the methods for measuring and analysing operational risks are as yet relatively undeveloped. Only a few individual banks have reached a stage where the operational risks are quantified and economic capital can be allocated to operational risks.

Risk management in the major banks both in Sweden and internationally is increasingly focussing on operational risks. Operational risks have always existed in banking. The difference now is that operational risks are viewed as a separate area and that the banks try to measure and analyse these risks, as well as manage them.

In addition to credit risks, operational risks can probably be sufficiently large to cause a bank serious problems, and thus threaten financial stability.

In addition to credit risks, operational risks can probably be sufficiently large to cause a bank serious problems, and thus threaten financial stability. The size of operational risks varies between the banks depending on business focus and strategy. Studies estimate that 15-25 per cent of the total financial risk in international banks' current operations relates to operational risks.[34]

A number of different factors have increased interest in this area:

Spectacular events:
A number of spectacular events in the financial sector incited large media interest during the second half of the 1990s. Most well known was the Barings Bank case in 1995, where an employee disregarded instructions, and by taking and concealing trading positions caused losses which, following liquidation of the 232 year-old bank, amounted to GBP 1.4 billion.[35]

34 Basel Committee on Banking Supervision 2000. Risk Management Group. Unpublished survey.

35 Adrian E. Tschoegl. 1999. The Key to Risk Management: Management. The Wharton School.

Changes in operations:
Changes in the banks' operations and new products have caused increased operational risks. In many banks, new business areas have grown considerably compared with more traditional banking operations (see Chapter 1). The current very rapid rate of change in the banking sector with extensive structural transformation, internationalisation and investments in new technology is in itself a source of increased operational risks, as adapting regulations, instructions and routines takes time. In 1998, operational losses of approximately USD 7.4 billion were reported in the mass media, which is almost double the 1995 figure.[36]

Allocation of risk capital:
By setting a required return in proportion to risk for different business areas, the bank can better control its operations, and thus improve profitability in the long term. In estimating and allocating economic capital internally in the banks, the ambition is to estimate as far as possible how much economic capital different business areas need, including capital to cover operational risks.

Authorities' attention:
The authorities' increased attention in this area has also contributed to the development of risk management in the banks. When the Basel Committee on Banking Supervision presented its draft proposals regarding new capital adequacy regulations in June 1999, it was proposed that the increasingly sophisticated capital adequacy requirements for credit and market risks should be supplemented by a capital requirement for "other risks", in which operational risks were included. This work is in progress in collaboration with the banking sector, and a consultative document is planned to be published in January 2001.

What are operational risks?

To date, there is no official definition of operational risk, but the following definition seems to be gaining ground in the financial sector: "*Operational risk is the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events*".[37]

In other words, the concept covers a large number of events, which can be divided into a number of risk categories. The more common include

- Deficiencies in internal control: internal theft, fraud and unauthorised activities, unclearly defined authority, weak corporate culture and management problems.

36 A study in autumn 1999 carried out by PriceWaterhouseCoopers, organised by the British Bankers Association, ISDA and Robert Morris Associates. 110 international financial institutions were consulted and 55 responded the majority of them banks.

37 This definition has been adopted by the Basel Committee.

- Process and transaction errors, technology and system errors.
- Legal, administrative and documentation errors.
- Crime: robbery and fraud.
- Loss of or damage to physical assets, e.g. in case of fire.

The first category has traditionally caused significant problems. In many cases, the bank management has lacked knowledge of the operational risks, or has failed to take them sufficiently seriously. When problems have come to light, management has reacted too slowly. Losses have often been preceded by management sending the wrong signals to their organisations, leading to a corporate culture where insufficient emphasis is placed on following regulations and instructions and implementing controls. It is also important to have a corporate climate where employees are not afraid to admit mistakes. Many of the major losses occurring in recent years have started off as minor mistakes that grew out of control when people tried to hide them.

The losses that may arise can be divided into *direct and indirect losses*. An example is a computer failure resulting in the bank's computer services not functioning. The direct losses in this case would be the costs of dealing with the computer failure, in the form of increased overtime costs and consulting costs or software costs. The indirect costs in this example would be the costs resulting from reduced confidence in the bank and the loss of income during the computer system's down time. Historically, banks have focused on direct costs, which is natural since these are easier to measure. It has, however, become increasingly clear that such an approach results in an underestimation of the risks, and consequently indirect losses should also be taken into account.

Some well-known examples of operational incidents and "near misses" in Sweden

Fraud
The most obvious operational risk, beside robbery, is fraud perpetrated by bank employees
Sparbanken Väst's Gothenburg office, where the regional manager was sentenced to prison as a result of large-scale fraud in connection with granting credit.

Unauthorised trading
Insufficient internal control can enable unauthorised trading to have consequences that can lead to major losses in an individual institution/organisation
(i) City of Stockholm option trading in the 1980s
(ii) A stockbroker at Nordbanken who carried out unauthorised trading over a long period of time

Technical breakdowns
Disruptions in technical systems can lead to both direct and indirect costs
(i) SEB's Internet bank that failed to manage the large amount of orders on one occasion.
(ii) Breakdowns that have occurred at stock exchanges and clearing institutes (OM, BGC and the RIX system)

Assessment of operational risks

The banks' risk management previously focused mainly on market and credit risk. Over the past years, the banks have increasingly adapted their organisations and also appointed policy and reporting officers responsible for operational risks. The primary responsibility for the management of operational risks often lies with the respective business unit, since these have the best ability to monitor the risks in the operations. The overall policy and reporting responsibility is concentrated centrally in the banks, in a similar way to the management of market and credit risks. The bank management always has the ultimate responsibility for implementing the strategy for management of operational risks determined by the board of directors.

The traditional starting point for management of operational risks has been to rely entirely on internal audit, staff ethics and the bank's culture. There is currently no generally accepted method of identifying, reporting and measuring operational risks. However, a number of different techniques and processes aimed at controlling these risks have arisen recently.

- Self-assessment, where the different business areas assess the risks on the basis of centrally prepared checklists.
- Risk mapping, where procedures and product flows are reviewed to identify which types of risks may arise and where they may arise.
- Identification of prioritised risks. An assessment is made of the probability of an event leading to a loss (high-low), and the amount of the loss should the event occur (high-low). Action programmes are being introduced for risks having the combination high probability and high loss.
- Identification of risk indicators. Indicators can be determined at different levels and can be of very different natures. High staff turnover can, for example, in some cases be considered to increase the risk of human errors and mistakes. It can also lead to a weaker corporate culture, making internal control more difficult. The indicators are monitored and reported continuously, and measures can be put in place if developments are considered disquieting.
- Escalation triggers. If the risk control department considers that the risk indicators have reached disquieting levels or that there are deficiencies in the risk management of a business, for example deficient assignment of responsibilities, the business area can be allocated a higher internal capital requirement until the problem is solved. As there is a required return on the internal capital, there is a stronger incentive to solve the problem quickly.
- Development of loss event databases. Losses resulting from operational risks are reported in a structured way. The loss data is used to monitor developments and to estimate, using statistical methods, the probability of various losses, e.g. in case of computer failures. This can then be used to assess the amount of capital which should be allocated for these risks. Also the reporting of *near misses*, i.e. events which could have led to a loss but did not do so due to sheer luck or to the problem being identified and dealt with in time. An increased frequency of this type of incident gives an indication of increased operational exposure.

Operational risks are, as has been seen, a very broad concept. A bank's different business lines, such as asset management, corporate finance and securities trading, are exposed to different degrees and to different risk types. One approach is to try to identify a few indicators of exposure per business line. These indicators are normally expressed as a value, volume or number. In the securities trading business line, it is reasonable, e.g., to assume that there is a correlation between volume of trades and operational losses. In the asset management business line, it may instead be more reasonable to monitor the value of assets under management and the value of transactions, while the volume of new deals may be useful information for assessing the operational risks in the corporate finance business line. In many cases, the identification of indicators is based on intuition, since the banks still have too little internal loss data to carry out a reliable statistical analysis.

Only a very few banks have gone as far as to quantify the operational risks and to allocate economic capital to these risks.

The banks are in a phase where they are trying out different methods and combinations of methods. According to an international study carried out in 1999, self-assessment was the most common method, even though 71 per cent used or planned to use all the above techniques in the near future.[38] However, there is a trend towards attempts to develop more risk-based, "bottom-up" methods based on actual loss data from internal and external loss event databases. In Sweden, as in the rest of the world, this process has just begun. Only a very few banks have gone as far as to quantify the operational risks and to allocate economic capital to these risks.

Notably, operational risks are also affected by organisational culture and management attitudes. Improvements in quantitative methods alone will not solve all problems, but can provide important support in identifying and evaluating the risks.

Regardless of which method the bank chooses to use, it is important to be able to detect the operational errors that arise and react to them. As the banks have already experienced, rapid action can drastically reduce the size of the loss.

Measurement problems

One of the banks' aims in attempting to measure operational risks is to assess the amount of buffer capital needed by the bank to protect itself against operational losses. The capital serves to protect the bank against unforseen events that might jeopardise the bank's continued existence. Losses expected by the bank should be covered by the bank's earnings through the pricing of the bank's services. This can be done by budgeting for losses known by the bank to occur with a certain frequency, such as credit card misuse.[39]

Since the interest in reporting operational losses in a structured way has arisen recently, there is no structured historical data to refer to. In addition, the operational losses that are relevant from a capital perspective, exhibit low probability and great magnitude, therefore few events are reported. In certain areas of operational risk, longer data series may be available. This normally applies to the computer department, where detailed statistics are often available, e.g., on computer failures and interference in computer systems. Significant data problems arise in the development of *internal loss databases*. Unambiguous and exclusive definitions, which apply to the whole bank, are important, particularly for direct and indirect losses. For example, it is not unusual in case of robbery to re-

38 See footnote 36.

39 With regard to operational exposures, it is still difficult to estimate expected and unexpected losses, due to inadequate data series. There is no explicit pricing of operational risks, and there is little possibility for allocating untaxed reserves for these in most countries.

port the sum stolen as an operational loss, while consequential costs, such as staff on sick leave and repairs to the premises, are reported as personnel and material costs respectively. Attention is thus not paid to the operational loss as a whole. In addition, there is the potential loss of income for the days the bank was closed as a result of the robbery. The boundary between operational risk and other types of risk can also be inconsistent. In many cases, a loss is reported as a credit loss, despite the fact that the real cause was deficient internal instructions or inadequate documentation, and thus strictly speaking the loss ought to have been classed as an operational loss. A lower limit is often also set for the losses to be reported.

The banks discuss and work in various groupings for the international exchange of internal data and the development of *common databases*. The objective is to obtain an adequate volume of data to carry out statistically reliable analyses.[40] Detailed definitions and reporting instructions are, of course, also important in this context. External databases, often containing major losses reported in the media, are already used to some extent today, mainly for the purpose of comparison with competitors, and for drawing up various types of worst case scenarios.

Risk reduction

With regard to other risks, such as interest rate risk, the bank can normally increase its anticipated income by raising the risk level. The bank's anticipated income does not normally increase, however, if operational risk is increased. The bank thus has an explicit interest, in most cases, in trying to limit operational risks. However, reducing operational risk involves expenses, e.g., for staff, systems, and controls. The better operational risks have been identified and quantified, the easier it is to create an understanding of the risks to which the bank is exposed, and to determine which risks the bank is prepared to take and what it is prepared to pay for risk reduction.

The better operational risks have been identified and quantified, the easier it is to create an understanding of the risks to which the bank is exposed, and to determine which risks the bank is prepared to take and what it is prepared to pay for risk reduction.

The banks already use traditional insurance solutions for certain types of operational risks, such as fire and theft. As a rule, these risks are reinsured on the international reinsurance market. Products for other types of operational risks, such as unauthorised securities trading, are being developed. Insurance solutions can fulfil a function, since each individual bank cannot be expected to hold

40 Consortia for common databases, in which the various individual banks' internal loss data is compiled, are currently in a start-up phase. Apart from the British Bankers Association, these databases are provided mainly by various consultancies. Incidents are to be reported to the databases according to detailed instructions. All information is anonymous and the data is to be made available to the participants.

sufficient buffer capital to manage major losses. Different insurers could, however, manage even major bank losses through a diversified portfolio containing such diverse risks as bank failures, nuclear accidents and natural disasters. A number of questions remain to be solved, however, with regard to these new insurance products.

- Operational risks can be difficult to define and quantify, and it can thus be difficult to clearly determine what is actually covered by the insurance.
- Insurance contracts normally contain clauses on disclosure requirements. This means that insurance compensation may not be payable or may be reduced, if the insurer considers that the insured has withheld information on risk exposure. With regard to losses resulting from deficient staff ethics or competence, which are considered an important part of operational exposure, the question of the bank's duty of disclosure to the insurer can be difficult.
- Loss investigations in case of operational losses are often difficult and take a long time. The period between the loss and payment can be significant and place a strain on the bank's liquidity.
- An additional risk is that the amount is so high that the insurer cannot pay, and that the operational risk is thus replaced by a counterparty risk. When the sums insured are large, it is important that the reinsurance structure is transparent.

From a societal point of view, it is also feared that *moral hazard* problems can arise, that is that insurance policies against operational risks reduce the bank's incentive to improve its internal risk management. This can be counteracted by the insurers placing higher demands on the banks' risk management, as well as through the structure of the insurance. Significant excesses, a ceiling on possible compensation and "reinstatement" requirements in case of loss counteract moral hazard.

Systemic risk

Even though quantification attempts encounter many difficulties, systematic measures to identify operational risks increase the bank's awareness of where the really significant risks lie. Operational risks also differ from credit and market risks in that they are normally not correlated between different institutions. Market crashes and economic shocks can affect many banks simultaneously and in a relatively similar way, while, e.g., computer failures or fraud probably affect one bank at a time. This means that systemic risks resulting from operational risks can be expected to be less serious than other systemic risks. The bankruptcy of an individual bank could have serious repercussions on other banks in the system, irrespective of whether the bankruptcy is caused by fraud or bad loans.

From a systemic point of view, it is therefore important that the banks spread their risks, and do not allow such large individual exposures even to other well-reputed banks that a bankruptcy would threaten their own bank's survival.

The Barings Bank case showed that high losses resulting from operational risks can, in principle, be revealed overnight even in a well-reputed bank. In the case of such a rapid course of events, the counterparties do not have the same opportunity of reducing their exposures, as they have in the case of a slower deterioration in a counterparty's credit worthiness. From a systemic point of view, it is therefore important that the banks spread their risks, and do not allow such large individual exposures even to other well-reputed banks that a bankruptcy would threaten their own bank's survival.