Note

Managing Operational Risk

By A.V. Vedpuriswar

"Operational risk is a daily and continuous 24 X 7 X 365 process. A way of life. Not an event or a meeting at the end of the quarter. Each person and stakeholder at you organization or institution is responsible for it and should live each day embracing it[1]."

Introduction

Operational Risk Management has become increasingly important in recent years. Many of the big scams of the past two decades including Barings, have been due to the failure of Operational Risk Management. In an increasingly complex and volatile business environment, organizations are realizing the importance of robust systems, processes and controls to ensure that human errors and fraud do not occur. The management of operational risk has received added impetus thanks to regulators. The Sorbanes Oxley Act enacted in the US in 2002, after the collapse of Enron has put pressure on organizations to strengthen their approach towards operational risk management. The Act requires boards of directors to become much more involved with day-to-day operations. They must monitor internal controls to ensure that risks are being assessed and handled well. Meanwhile, Basle II has come up with detailed guidelines for identifying and measuring operational risk.

In this note, we try to understand the sources of operational risk, how it can be measured and the risk mitigation techniques which can be applied.

Understanding Operational Risk

Operational risk can be defined as the risk of loss due to inadequate or failed internal processes, people, systems or external events. Some operational risks directly affect the financial performance of the organization. Others do so by interacting with credit and market and other risks.

The nature of operational risk is somewhat different from that of market or credit risk. (See Exhibit 1.1). Banks make a conscious decision to take a certain amount of credit and market risk. Operational risk, by contrast, is a necessary part of doing business. More often than not, operational risks are "inherent" not "chosen." The only way to avoid operational risk is by exiting the business!

It is much more difficult to identify, quantify and manage operational risk than credit or market risk. Data on operational risk is not exhaustive. Most banks are still in the process of collecting data. Developing statistical models for operational risk is thus challenging.

---

[1] Operationalrisk.blogspot.com

Exhibit 7.1
Market, Credit & Operational Risks: A quick comparison[2]

Step	*Market Risk*	*Credit Risk*	*Operational Risk*
Risk categories	• Interest rate • Equity • Currency • Commodity	• Default • Downgrade	• Processes • People • Systems • External events
Risk factors	• Volatility • Correlations	• Default and recovery distributions • Correlation	• Loss frequency
Risk measurement	• Market VAR	• Credit VAR • Expected loss	• Operational VAR • Expected loss

Identifying operational risk

As mentioned earlier, operational risks are not consciously taken. But they invariably arise in the course of conducting business activities. The key challenge is often to identify and anticipate the various kinds of operational risk that may arise. The Basle committee has provided a useful framework in this regard.

Internal fraud: Examples include intentional misreporting of trading positions, employee theft, and insider trading on an employee's own account. This risk is considered *low frequency, high severity*.

External fraud: Examples include computer hacking, robbery and forgery. This risk is considered *high/medium frequency, low/medium severity*.

Employment practices and workplace safety: Examples include worker compensation claims and sexual discrimination claims. This risk is considered *low frequency, low severity*.

Clients, products, and business practices: Examples include fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account and money laundering. This risk is considered *low/medium frequency and high/medium severity*.

Damage to physical assets: Examples include earthquakes, fires and floods. This risk is considered *low frequency/low severity*.

[2] Draws from Philip Jorion's book "Value at Risk – The New Benchmark for Managing Financial Risk," *McGraw Hill*, 2007, p. 497.

Business disruption and system failures: Examples include hardware and software failures, telecommunication problems, and utility outages. This risk is considered *low frequency/low severity*.

Execution, delivery and process management: Examples include data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to clients' accounts. This risk is considered *high frequency, low severity*.

These seven distinct types of operational risk, as indicated above, vary in terms of frequency and severity. So they need to be handled differently.

- Low frequency, high severity risks can put the future of a firm at risk. These risks cannot be actively managed on a day-to-day basis. The expected losses cannot also be built into the product price.
- The high frequency low severity risks have high expected loss but low unexpected loss. These risks must be covered by the general provisions of the business. They can also be managed with suitable systems and processes.
- It is the medium frequency medium severity risks that are often the main focus of operational risk capital measurement.

Quantifying operational risk

The following tools, listed in order of increasing sophistication, can be used for assessing operational risk.

- *Critical self-assessment:* Each department submits a subjective evaluation of the sources of operational risk, along with expected frequency and costs.
- *Key risk indicators:* A centralized unit develops subjective risk forecasts through risk indicators, such as trading volume, number of mishandled transactions, staff turnover, and so on.
- *Formal quantification:* Operational risk managers prepare an objective distribution of operational risk losses from an event database.

As mentioned earlier, a major challenge in quantifying operational risk is that data on the severity and frequency of historical losses are often not available. Internal historical data on high frequency risks is relatively easy to obtain but these risks are not the important ones from the point of view of measuring operational risk capital. It is the low frequency, high severity and medium frequency medium severity risks that are the most important risks to measure from a risk capital perspective. But there is little historical data available.

If frequency and severity are the two key issues, by inference, there are two distributions that are important in estimating potential operational risk losses. One is the loss frequency distribution and the other is the loss severity distribution.

The *loss frequency* is a measure of the number of loss events over a fixed interval of time. The *loss severity* is a measure of the size of the loss once it occurs. The *loss-distribution approach* (LDA) then combines these two variables into a distribution of total losses over the period considered. Often, it is assumed that these distributions are independent. But such an assumption can be unrealistic at times.

For loss frequency, the most commonly used distribution is the Poisson distribution. Under this distribution, losses happen randomly. The probability that "n" losses will occur in time T is $\frac{e^{-\lambda T}(\lambda T)^n}{\angle n}$. λ is the expected value of losses defined in such a way that during a short period of time, Δt, there is a probability $\lambda \Delta t$ of a loss occurring. In other words, λ is nothing but the average number of losses per unit time.

Loss severities can be tabulated from a combination of internal and relevant external data. The risk manager can measure the loss severity from historical observations and adjust it for inflation and some measure of current business activity. For loss severity, a lognormal probability distribution is often used. The parameters of this probability distribution are the mean and standard deviation of the logarithm of the loss.

The loss frequency distribution is combined with the loss severity distribution for each loss type and business line to determine a total loss distribution. Monte Carlo simulation is often used for this purpose.

For most banks, the historical data available internally to estimate loss severity and loss frequency distributions is limited. As a result of regulatory requirements, banks have started to collect data systematically in recent years, but it may be some time before a reasonable amount of historical data is available. As we saw earlier in the chapter on credit risk, data can be a problem even in the case of credit risk management. But, traditionally banks have done a much better job at documenting their credit risk losses than their operational risk losses. Moreover, in the case of credit risks, a bank can rely on a wealth of information published by credit-rating agencies to assess the probability of default and the expected loss given default. Similar data on operational risk does not exist. Moreover, banks may conceal a large operational risk loss from the market if they feel it will damage the reputation.

Operational risk failure at Deutsche Morgan Grenfell[3]

In September 1996, the investment bank Deutsche Morgan Grenfell (DGM) decided to suspend a star fund manager, Peter Young, in its asset management unit. DMG also halted trading on its three main European equity funds, worth some $2.2 billion.

Young had breached the limit of 10 percent that such funds could invest in unlisted securities. This limit had been imposed because of the difficulty of confirming market values for these securities. After a stellar performance in 1995, the funds managed by Young ranked last in their category in the first half of 1996.

Deutsche Bank, DMG's German owner agreed to compensate the shareholders in the funds. It set aside some $720 million to cover the total losses. The total cost was even higher as a result of the business lost due to the bank's tarnished reputation.

The loss frequency distribution should be estimated from the bank's own data as far as possible. For the loss severity distribution, regulators allow banks to use their own data along with external data. Part of the external data may come from the banks provided they are willing to share data among themselves. The remaining can be sourced from data vendors.

One way to deal with the problem of inadequate data is to use scenario analyses to supplement internal and external loss data. Managers can use their judgement to generate scenarios where large losses occur. The scenario analysis approach forces managers to start thinking proactively and creatively about potential adverse events. The main drawback of scenario analysis is that it requires a great deal of senior management time.

Scaling

Losses due to operational risk can be scaled up if we know the exponent for scaling. In general the exponent will lie between zero and 1. Thus if a division with revenue R_1 has incurred losses of 100, a division with revenue = R_2 will have losses of $\left(\frac{R_2}{R_1}\right)^K \times 100$; where k is the exponent.

Power Law

A simple but powerful tool for forecasting operational risk is the power law. This law states that the probability of a random variable *x* exceeding a value *V* is given by:

[3] Philippe Jorion, "Value at Risk: The New Benchmark for Managing Financial Risk," McGraw Hill, 2007.

p ($x > v$) = $K V^{-\alpha}$ where K is constant, α is the power law parameter.

Illustration

A bank with annual revenues of $2 billion has incurred a loss of $100 million on account of operational risk. What would be the losses for a bank with a similar business profile but with revenues of $6 billion? Assume the exponent for scaling losses is 0.23.

$$\text{Loss for Bank B} = \left(\frac{\text{Revenue of Bank B}}{\text{Revenue of Bank A}}\right)^{.23} \times \text{loss for Bank A}$$

$$= \left(\frac{6}{2}\right)^{.23} \times 100$$

$$= 3^{.23} \times 100$$

$$= \$128.75 \text{ million}$$

Illustration

There is a 90% probability that operational risk losses will not exceed $20 million. The power law parameter is given as .8. Find the probability of the losses exceeding:
(a) $40 million (b) $80 million (c) $200 million

The power law states : Prob ($x > v$) = $K v^{-\alpha}$
We are given that : .1 = $(K)(20)^{-.8}$
or K = 1.0986
Thus we get probability ($v > x$) = $1.0986x^{-.8}$
When x = 40, probability = $(1.0986)(40)^{-.8}$ = 5.74%
When x = 80, probability = $(1.0986)(80)^{-.8}$ = 3.30%
When x = 200, probability = $(1.0986)(200)^{-.8}$ = 1.58%

Illustration[4]

Consider the following distribution

Frequency Distribution		**Severity Distribution**	
Probability	*Frequency*	*Probability*	***Severity***
0.5	0	0.6	$2,000
0.3	1	0.3	$5,000
0.2	2	0.1	$100,000

The losses due to operational risk can be tabulated as follows:

[4] Adapted from Philippe Jorion's book "Value at Risk – The New Benchmark for Managing Financial Risk," *McGraw Hill*, 2007, pp. 499-500.

Tabulation of Loss Distribution

Number of Losses	*First Loss*	*Second Loss*	*Total Loss*	*Probability*
0	0	0	0	0.500
1	2,000	0	2,000	.3 x .6 = 0.180
1	5,000	0	5,000	.3 x .3 = 0.090
1	100,000	0	100,000	.3 x .1 = 0.030
2	2,000	2,000	4,000	.2 x .6 x .6 = 0.072
2	2,000	5,000	7,000	.2 x .6 x .3 =0.036
2	2,000	100,000	102,000	.2 x .6 x .1 =0.012
2	5,000	2,000	7,000	.2 x .3 x .6 =0.036
2	5,000	5,000	10,000	.2 x .3 x .3 =0.018
2	5,000	100,000	105,000	.2 x .3 x .1 =0.006
2	100,000	2,000	102,000	.2 x .1 x .6 =0.012
2	100,000	5,000	105,000	.2 x .1 x .3 =0.006
2	100,000	100,000	200,000	.2 x .1 x .1 =0.002

Loss Distribution approach

Basle II allows various ways of quantifying operational risk. One of them is the Loss Distribution Approach (LDA). The LDA consists of the following steps:

- Organizing and grouping loss data: Loss data are grouped according to business lines/event type. When enough data does not exist internally, data may have to be collected from outside.
- Weighting the data points: Equal weights are attached to all the data points, with three exceptions. Split losses are those that affect more than one business line. Old losses are given lower weight. External data and scenarios may have to be scaled to capture the biases involved.
- Frequency of loss distribution: This is usually done using the Poisson/Negative binomial/Binomial distribution. Internal data are usually preferred because they are more relevant.
- Severity distribution: In general, severity distributions are more difficult to construct, compared to frequency distributions. Recent internal loss data are often insufficient

to calibrate the tails of severity distributions. Extrapolating the values to values beyond those observed is a challenge. Sometimes, it may be better to model the body and the tail separately. Extrapolations can lead to the inclusion of extremely severe hypothetical losses and an overestimation of the needed capital reserve.

- The frequency and severity distribution are combined using Monte Carlo simulation.
- The capital requirements are determined, based on the estimates of expected, unexpected and stress losses.

The Basle framework

The Basle Committee has recommended some best practices in the area of operational risk.

- Board approval – The board of directors should approve and periodically review the Operational Risk Management framework.

- Independent internal audit – The board should subject the operational risk management framework to comprehensive and independent internal audit.

- Management implementation – Senior management should develop policies, processes and procedures for managing operational risk in the bank's important products, activities, processes and systems.

- Risk identification and assessment – Banks should identify and assess the operational risk inherent in all materials, products, activities, processes and systems.

- Risk monitoring and reporting – Operational risk profiles and material exposures to losses must be regularly monitored and reported to the senior management and the board of directors.

- Risk control and mitigation – Policies, processes and procedures must be put in place to control/mitigate material operational risks.

- Contingency and continuity planning – Contingency and continuity plans must be in place to cope with severe business disruption.

- Disclosure – Banks should make adequate disclosures to allow the markets to assess the approach of the bank towards managing operational risk.

Sarbanes Oxley Section 404

The linkages between Sarbanes Oxley and Operational Risk Management are often not fully appreciated. Section 404 of Sarbanes Oxley (SOX) pertains to the effectiveness of internal controls over financial reporting. Internal controls must provide reasonable assurance regarding the reliability of financial reporting. SOX 404 has been supplemented by the rules for auditors developed by the Public Company Accounting Oversight Board (PCAOB). These rules specify what auditors must do when performing an audit of internal control over financial reporting.

As Nick Bolton and Judson Berkey[5] mention, it would seem at first sight as though there is nothing specific in SOX about operational risk. But the connection is that control failures can lead to material financial misstatements. A single assessment process serving both Basel II and SOX 404 needs can help integrate the risk management process and achieve efficiencies. UBS, the global Zurich based bank has embraced such a philosophy. The UBS operational risk framework is built around the following:

- Clear definition of roles and responsibilities
- Control objectives
- Explanatory notes to control objectives
- Control standards
- Quality metrics / key risk indicators

Sound Practices for the management and supervision of operational risk

Developing an Appropriate Risk Management Environment

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation. Senior management should develop policies, processes and procedures for

[5] "Aligning Basel II Operational Risk & Sarbanes Oxley 404 projects," in "Operational Risk: Practical approaches to Implementation," ed Ellen Davis, Risk Books, 2005.

managing operational risk in all of the bank's material products, activities, processes and systems.

Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control
Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is assessed.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile, in light of their overall risk appetite and profile.

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

Role of Supervisors
Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Role of Disclosure
Principle 10: Banks should make sufficient public disclosure with regard to operational risk management.

Ref : Basle II Approach Paper, www.bis.org

Operational Risk Capital
Under Basle II, banks have three alternatives for determining operational risk regulatory capital. The simplest approach is the *basic indicator approach.* In this approach,

operational risk capital is set equal to 15% of annual gross income over the previous three years. Gross income is defined as net interest income plus non interest income[6].

In the *standardized approach,* the bank's activities are divided into eight business lines (See Exhibit 7.2).

Exhibit 7.2

Business Line	***Beta***
▪ Corporate finance,	18%
▪ Trading and sales,	18%
▪ Retail banking,	12%
▪ Commercial banking,	15%
▪ Payment and settlement,	18%
▪ Agency services,	15%
▪ Asset management,	12%
▪ Retail brokerage.	12%

The average gross income over the last three years for each business line is multiplied by a "beta factor" for that business line and the result summed to determine the total capital.

In the *Advanced measurement approach*, the regulatory capital requirement is calculated by the bank internally, using various qualitative and quantitative criteria. Banks must measure the operational risk capital requirement for each risk type in each of the eight lines of business. Each of the seven types of risk (see earlier part of the chapter) is mapped to these eight business lines to arrive at 56 separate estimates of operational risk capital.

Systems and processes

Effective management of operational risk calls for sound systems and processes that enable managers to know what risks are being taken, measure them and assess whether they are within prescribed limits. These systems should impose the necessary checks and balances and facilitate corrective action, where necessary.

Take the example of JP Morgan Chase, the global bank. JPMC has strengthened the Audit Department and risk assessment throughout the firm, enhanced data quality and controls, and also strengthened permanent standing committees that review new clients, new products and all reputational issues. Since 2011, the total headcount directly associated with controls has gone up from 24,000 people to 43,000 people, and the total annual controls spend has gone from $6 billion to approximately $9 billion annually. JPMC actually spends far more on controls if the time and effort expended by

[6] Net interest income is the excess of income earned on loans over interest paid on deposits and other instruments that are used to fund the loans.

front-office personnel, committees and reviews, as well as certain technology and operations functions are also included.

The various scams and disasters in recent times have made it clear that top management cannot let treasurers and other managers operate freely without being questioned when they are taking major financial decisions. Good management control systems help in defining performance standards, measuring actual performance and taking corrective action on a regular basis. By evaluating, monitoring and controlling the various sub-units, an organisation can ensure that there is optimal risk taking.

Systems and processes must be regularly monitored to ensure that they are working properly. Auditing should be undertaken periodically to check the robustness of the systems, procedures and controls. Auditing can also help to set standards and assess the effectiveness and efficiency of the system in meeting these standards. This way, managers can identify the scope for improvement, besides understanding how systems and processes are currently working.

A comprehensive audit must ideally review all the processes associated with measuring, reporting and managing operational risk. It must verify the independence and effectiveness of the risk management function and check the adequacy of the documentation. Audits should be held regularly to take into account changes in the circumstances and to monitor progress. The frequency of audits would depend on how integral it is to the company's strategy, the time and expenditure involved, etc. Audits can be performed in various ways – surveys, questionnaires, focus groups.

By themselves, audits cannot mobilize people into action. Audits can only come up with recommendations. Indeed, in some of the classic failures like Barings, audit recommendations were not implemented. The way senior managers enforce audit recommendations is hence key to sound operational risk management.

A key pillar of Basle II is market discipline which is facilitated by detailed and honest disclosures. The Satyam scam of 2008 has raised major concerns about the quality of disclosures in emerging markets and the role of auditors who certify these disclosures. Many high profile and respected companies in India seem to be resorting to "aggressive" accounting. The independence of auditors, who certify the financial statements is being widely questioned. After all, they are appointed by and paid for by clients.

Money laundering

Money laundering has become a top priority for large banks. If this risk is not properly controlled, it can severely damage the reputation of the bank. Advances in technology are coming in handy here. Take the case of JP Morgan Chase. JPMC has deployed a new anti-money laundering (AML) system, Mantas, a monitoring platform for all global

payment transactions. Mantas utilizes sophisticated algorithms that improve with experience. JPMC reviews electronically $105 trillion of gross payments each month. On an average, 55,000 transactions are reviewed by humans after algorithms identify any single transaction as a potential issue. Following this effort, JPMC stopped doing business with 18,000 customers in 2015. JPMC is required to file suspicious activity reports (SAR) with the government on any suspicious activity. Last year, the bank filed 180,000 SARs. JPMC exited or restricted approximately 500 foreign correspondent banking relationships and tens of thousands of client relationships to simplify the business and to reduce AML risk.

Data privacy and Cybersecurity

In today's digital world, cybersecurity has become a major concern. Many banks are paying a lot of attention to cyber risk. Take the example of UBS. The bank continues to invest significantly in dedicated security programs to strengthen its cyber defense. For UBS cyber risk includes data theft committed increasingly by criminal organizations, disruption of service, such as distributed denial of service attacks, and cyber fraud, often through business email compromise and phishing attacks. UBS has recently appointed a Head of Cyber Risk in order to effectively address the challenges posed by cyber risk. The role focuses on the enterprise governance for cyber-related activities, and includes regular assessments of cyber threat intelligence, analysis of the effectiveness of the bank's controls, and progress on improving cyber defense capability. The bank's cyber response framework, comprises "Analyze," "Protect," "Detect" and "Respond / Recover" capabilities. The cyber response framework also includes assessments of the capabilities of the bank's vendors.

Another global bank, JP Morgan Chase has a huge amount of data about customers because of underwriting, credit card transactions and other activities. The bank uses this data to help serve customers better. JPMC has elaborate measures in place to protect customers and their data. Customers usually agree to allow outside parties to have access to their bank accounts and their bank account information. Customers do this with payment companies, aggregators, financial planners and others. Based on experience, JPMC feels that third parties collect far more information than they need in order to do their job. Many third parties also sell or trade information in a way customers may not understand. The third parties, quite often, are doing so for their own benefit, not for the customer's benefit. Often this is being done on a daily basis for years after the customer signed up for the services, which they may no longer be using. JPMC has begun to ask third parties to limit themselves to what they need in order to serve the customer and to let the customer know exactly what information is being used and why and how. In the future, instead of giving a third party unlimited access to information in any bank account, JPMC hopes to build systems that allow the bank to "push" information and only that information agreed to by the customer to a specific third party.

Conclusion

Operational risks abound in today's business environment. The whole process of measuring, managing, and allocating operational risk is still in its infancy. As time goes by and data is accumulated, more precise procedures are likely to emerge. Operational risk capital allocation aims at ensuring that business units become more sensitive to the need for managing operational risk.

Case Illustration: The Collapse of Barings

Introduction

The collapse of Barings Bank in 1995 was one of the most astounding events ever in the history of investment banking. Barings went broke when it could not meet the huge obligations piled up by its trader Nick Leeson. At the time of its bankruptcy, Barings had huge outstanding futures positions of $27 billion on Japanese equity and interest rates; $7 billion on the Nikkei 225 equity contract and $20 billion on Japanese government bond and euro yen contracts. The risk taken by Leeson was huge when we consider that Barings' capital was only about $615 million. Leeson was particularly aggressive after the Kobe earthquake on January 17, 1995. His bet was that the Nikkei would continue to trade in the range 19,000 - 20,000. Unfortunately for him, the Nikkei started falling after the Kobe earthquake. Leeson made some desperate moves and single handedly tried to reverse the sentiments on the Osaka Stock Exchange but this had little impact. Barings' total losses exceeded $1 billion. The bank went into receivership in February, 1995.

Background Note

Barings Bank, founded in London by Francis Baring in 1763, was the first merchant bank in the world. It provided finance and advice to its clients and also traded on its own account. When it was set up, Barings operated in the London-based commodities markets, selling and buying wood, wool, copper and diamonds. During the Napoleonic wars, the bank helped the British treasury by supplying gold ingots to Britain's allies.

In 1818, Barings' influence was such that the French prime minister of the day, the Duc de Richelieu, declared, "Barings has become the sixth great power in Europe, after England, France, Austria, Prussia and Russia." It was a party to nearly all the major deals at that time.

In 1890, the rapidly growing bank made massive losses in Argentina and had to be bailed out by the Bank of England. In the 19th century, Barings spread across the globe, creating a global network that remained its main source of competitive advantage until the 1990s. By the beginning of the 20th century, Barings had become the British royal family's banker and received five separate peerages as rewards for its services to banking. In 1995, the star of Barings with 55 offices in 25 countries, was clearly on the ascendant.

Nick Leeson and the Singapore Operations

Nick Leeson started his career as a settlement clerk in 1985, with one of England's prominent bankers, Coutts & Company. In June 1987, Leeson joined Morgan Stanley as a trainee in the Settlement Division for Futures and Options. He quickly realized that dealers held the most remunerative jobs. Driven by ambition, Leeson resigned from Morgan Stanley and joined Barings in July 1989 again as a clerk in the Settlement Division for Futures and Options. He was transferred to Jakarta where he streamlined

the settlement of bearer bonds and reduced Barings' exposure from £100 million to £10 million. By the time he returned to London in 1991, he had grown in stature and was looking for more challenging assignments.

Barings had acquired a seat on the Singapore International Monetary Exchange (SIMEX) but had not activated it. The Barings subsidiary in Singapore bought and sold shares, researched the local markets and offered fund management and banking facilities. But it was not able to deal in futures. As all the requested transactions were routed through another trader, Barings could not charge commission. Leeson felt Barings should activate the seat to take advantage of the growing business and expressed his willingness to be involved in the Singapore operations.

Soon after arriving in Singapore, Leeson passed an examination conducted by SIMEX and started his trading activities. Shortly thereafter, Leeson was named General Manager and head trader of the local branch. Initially, Leeson dealt only in arbitrage trades[7] based on the Nikkei index, where the profit margins were small.

At first, SIMEX was a very small exchange, handling only 4,000 trades a day. Most of the big dealers dealt in the Nikkei index at the much bigger Osaka exchange in Japan. During the summer of 1992, the Osaka exchange imposed stringent regulations on futures and options dealers. The dealers were asked to pay much higher margins on which no interest was paid and a minimum commission was also stipulated. As a result of these restrictions, many dealers shifted to the SIMEX. The number of trades increased from 4,000 to 20,000 a day. Leeson captured a large share of this increase in trading volumes.

Leeson's modus operandi

Barings booked trading errors in a separate computerised account known as the 'error account'. Essentially, error accounts accommodated trades that could not be settled immediately. (In securities trading jargon, these are called breaks). A compliance officer normally investigated the trade and examined how it affected the firm's market risk and profit and loss. When Leeson had started the operations, he had an error account numbered '99905', where all the errors were booked before they were transferred to London. After receiving instructions from London, Leeson started a new error account, which was numbered '88888'. Leeson conducted a number of unauthorised trades using this account and asked a colleague to remove this account from the daily reports which Barings Singapore sent to London.

- Between 1992 and 1995, the Barings management had little idea of Leeson's true profit and loss performance. The details of account 88888 were never reported to Treasury officials in the London headquarters.

[7] Arbitrage trades take advantage of the price differential of an instrument or a commodity in two markets. They involve buying in a lower-priced market and selling in the higher-priced one.

- In September 1992, the London headquarters set up an error account 99002. Instead of shifting to this account, Leeson kept error account 88888 active to hide his trading losses and unauthorised trades.

- Leeson made it look as though he was maintaining a flat book exposure. Actually, he maintained huge long and short positions which carried risk way beyond he was authorized to take or for that matter, even Barings as a bank could afford to take. Leeson was allowed to make unhedged trades on up to 200 Nikkei 225 futures, 100 Japanese Government Bonds and 500 euroyen futures contracts. Leeson's positions greatly exceeded these authorized limits. Leeson also engaged in the uanuthorised sale of Nikkei 225 put and call options. He did this to earn premiums that could be used to meet margin calls.

- Initially, Leeson's proprietary trading involved arbitrage in Nikkei-225 stock index futures and 10-year Japanese Government Bond (JGB) futures between the SIMEX and the Osaka Securities Exchanges (OSE). However, Leeson soon embarked upon a much riskier trading strategy. He began placing bets on the direction of price movements on the Tokyo stock exchange. Initially, Leeson was very successful. His reported trading profits, were spectacular and accounted for a significant share of Barings' total profits. The bank's senior management regarded Leeson as a star performer and did not think it necessary to drill deeper into his activities.

- Far from making profits, Leeson was in reality making losses. Leeson needed funds to meet his margin calls and support the losses that were piling up. But he succeeded in persuading the London office to release funds. From 1992 till the collapse of Barings, Leeson was able to get funds to meet margin calls on unauthorized trades with little security whatsoever.

- Leeson used his position running the back office to hide the true picture from his bosses. In September 1992, he debited a Barings receivable account at Citibank Singapore and credited the funds to error account 88888. This transfer helped Leeson to hide his trading losses. Lesson also forged a fax from the London based risk manager to the effect that the error account 88888 had an insignificant balance.

- Leeson sold straddles on the Nikkei 225, hoping that the Nikkei index would be trading in the range 19000-19500. The money he collected as premium could be booked as profits when the options expired worthless. But following the Kobe earthquake of January 17, 1995, the Nikkei dropped to 18,950. As the Nikkei fell, Leeson lost money on the put options. Leeson responded by buying March 1995 futures contracts. On January 23, the Nikkei dropped to 17,950. The long positions and the puts both began to register heavy losses. Though Leeson had started off by arbitraging between prices on the same futures contracts in Osaka and Singapore, by the time Barings collapsed, he was long on both these exchanges. Not surprisingly, during January and February 1995, Barings made huge losses.

The Crisis

Just a few months after he had begun trading, Leeson had accumulated a loss of £2 million. The loss remained hidden and unchanged until October 1993. Then it began to rise sharply. Leeson lost another £21 million in 1993 and £185 million in 1994. Total cumulative losses at the end of 1994 stood at £208 million. That amount was slightly larger than the £205 million profit (before accounting for taxes and for £102 million in scheduled bonuses) reported by the Barings Group as a whole. After the Kobe earthquake, the Nikkei crashed making Leeson's open position worse. By February 1995, Barings had gone into receivership. Leeson tried to escape but was later jailed. Barings was taken over by the Dutch group, ING.

Once the Singapore and Osaka exchanges understood that Barings would not be able to meet its margin calls, they took control of all the bank's open positions. The Nikkei index fell precipitiously when market participants learnt that the exchanges would be liquidating such large positions. The situation became more complicated when SIMEX announced that it would double the margin requirements on its Nikkei stock index futures contract from February 28. Several clearing members feared that their margin money might be used to pay for Barings' losses and threatened to withhold payment of the additional margin. To complicate matters further, regulators in Japan and Singapore were slow to inform market participants of the steps they were taking, to ensure the financial integrity of the exchange clearing houses. This lack of communication aggravated the fears of market participants. Later, following an assurance given by Monetary Authority of Singapore, SIMEX's margin calls were met and a potential crisis was avoided.

This was not the end of the matter for Barings' customers. Barings was one of the largest clearing members on SIMEX. It handled clearing and settlement for 16 U.S. firms and held approximately $480 million in margin funds on their behalf when it went bankrupt. U.S. futures exchanges typically arranged for the immediate transfer of all customer accounts of a financially troubled clearing member to other firms. Laws in the U.S. facilitated such transfers because they provided for strict segregation of customer accounts. This prevented the creditors of a broker or clearing member firm from attaching the assets of customers. But Japanese laws contained no such provisions. And this was not well known before the collapse of Barings. Although laws in Singapore recognized the segregation of accounts, SIMEX had never before dealt with the insolvency of a clearing member firm. Since most of Barings' customer accounts had been booked through Barings Securities in London, SIMEX did not have detailed information on individual customer positions. It had records pertaining to only a single aggregated account for Barings Securities. Moreover, the information that Leeson had provided to the exchange, was largely incorrect. So the task of sorting out the positions of individual customers became extremely difficult.

During the next week, Barings' U.S. customers scrambled to reproduce documentation of their transactions with the bank and supplied this information to SIMEX and The Osaka Exchange. This information enabled the exchanges to identify customer positions. At the same time, Barings' bankruptcy administrator in London asked the exchanges to block access to all Barings' margin deposits. The administrator also raised questions about the U.K. laws on the segregation of customer accounts.

It was not until ING took over Barings on March 9 that the bank's customers were assured of access to their funds. Even then, access was delayed in many cases. Some major clients waited for more than three weeks before their funds were returned.

The Bank of England Report on Barings

Following the Barings failure, the Bank of England identified various lessons from the disaster.

- *Management teams have a duty to understand fully the businesses they manage.* Top management at Barings did not have a good understanding of Leeson's business though it was creating huge profits for the bank.
- *Responsibility for each business activity must be clearly established.* Barings was using a "matrix" reporting system (by region and product) that left ambiguities in the reporting lines for Nick Leeson.
- *Clear segregation of duties is fundamental to any effective risk control system.* Leeson had control over both the front and back offices. The Barings affair demonstrated a compelling need for independent risk management.

Source: Philippe Jorion, "Value at Risk – The new benchmark for managing financial risk," McGraw Hill, 2007.

Concluding Notes

Looking back, it is clear that the Barings management failed to institute adequate managerial, financial and operational control systems. Checks and balances failed at lower as well as senior levels resulting in Leeson's free run. On paper, Leeson had many supervisors but no one really exercised any control.

Barings broke a very important rule of any trading operation i.e., separation of the dealing desk and the back office. The back office, which recorded, confirmed and settled trades transacted by the front office, should have provided the necessary checks to prevent unauthorised trading, fraud and embezzlement. But by putting himself in charge of the back office, Leeson relayed false information to Barings' London headquarters. Market risk reports submitted by Leeson were later found to be manipulated and inaccurate. Before the crisis, an internal audit team had concluded that Leeson's dual responsibility for both the front and back office was an excessive concentration of powers. It had recommended that Leeson be relieved of four

responsibilities, back office supervision, cheque signing, signing SIMEX reconciliations and bank reconciliations. This recommendation was not implemented.

Barings' senior management did not invest adequate time and effort in understanding the use of derivatives. While they were very enthusiastic and happy about the substantial trading profits earned by the Singapore office, they did not make any serious effort to analyse the way profits had been booked. Investigations later revealed that Leeson had conducted unauthorised trades almost from the time he started trading in Singapore. He made losses on many of these trades.

One of the techniques used by Leeson to deceive his bosses in the UK was cross trade, a transaction in which the same member of the exchange was both buyer and seller. If a member had matching buy and sell orders from two different customer accounts for the same contract and at the same price, he could execute the transaction by matching the two client accounts. However, he could do this only after declaring the bid and offer price in the pit. Also, a cross trade had to be done at the market price. Leeson, did not follow these guidelines. He broke down the total number of contracts into several different trades and changed the trade prices to manipulate profits. Leeson also recorded some fictitious transactions to jack up profits. Leeson also did not separate the proprietary and client trades.

Meanwhile, Barings also did not have a system to reconcile the funds Leeson requested from time to time with his reported positions. By 1995, Leeson had requested and received almost $1.2 billion. The management continued to fund Leeson's activities, thinking they were paying margins on hedged positions. Actually, losses were being incurred on outright positions on the Tokyo stock market. There was no system in place to reconcile the funds, Leeson had requested for his reported positions and the clients' positions. Only later did the management realize that Barings was exposed to significant market risk due to the naked positions.

References:

- Kennett A Froot, David S Scharfstein and Jeremy C Stein, "A framework for risk management," *Harvard Business Review*, November-December 1994, pp. 91-102.
- Marcus Eliason, "Shares plummet in Asia as some Barings operations suffered trading," *The Associated Press*, February 26, 1995.
- Dirk Beveridge, "Futures gambling busts British investment bank," *The Associated Press*, February 26, 1995.
- "Government freezes Barings assets in Seoul," *Associated Press*, February 26, 1995.
- Andrian Hamitton and Mark Gould, "Merchant bank faces collapse," *The Guardian*, February 26, 1995, p. 1.
- "Act now to prevent another Barings," *The Times of London,* February 26, 1995.
- Andrew Lorenz and Frank Kane, "Barings seeks rescue buyer; Barings bank collapse", *The Times of London,* February 26, 1995.
- Tim Rayment, "History repeats itself at Barings; Barings Bank Collapse," *The Times of London,* February 26, 1995.
- Andrew Lorenz and David Smith, "Queen's bank near collapse in £400 million loss; Barings Bank collapse," *The Times of London,* February 26, 1995.
- "A fallen star," *The Economist,* March 4, 1995, pp. 19-21.
- Barry Hillenbrand, "Losing one's Barings," *Time*, October 16, 1995, p. 47.
- Barry Hillenbrand, "The Barings Collapse: Spreading the blame," *Time*, October 30, 1995, p. 68.
- Frank Gibney Jr. "Leeson's last deal," *Time*, December 11, 1995, p. 24.
- Robert Simons, "How Risky is your company?" *Harvard Business Review*, May-June 1999, pp. 85-94.
- "Sound Practices for the Management and Supervision of Operational Risk," Risk Management Group of the Basel Committee on Banking Supervision, February 2003. www.bis.org
- Patrick de Fontnouvelle, Virginia DeJesus-Rueff , John Jordan & Eric Rosengren, "Capital and Risk: New Evidence on Implications of Large Operational Losses," Federal Reserve Bank of Boston, September 2003.
- David M Weiss, "After the trade is made – Processing securities transactions," *Penguin,* 2006.
- John C Hull, "Options, Futures and Other Derivatives," Prentice Hall, 2006
- John C Hull, "Risk Management and Financial Institutions," Pearson Education, 2007.
- Philippe Jorion, "Financial Risk Manager Handbook," John Wiley & Sons, 2007.
- Philippe Jorion, "Value at Risk: The New Benchmark for Managing Financial Risk," McGraw Hill, 2007.
- Jeffry M. Netter and Annette B. Poulsen, "Operational Risk in Financial Service Providers and the Proposed Basel Capital Accord: An Overview," Working Paper, Department of Banking and Finance Terry College of Business, University of Georgia. Athens.