CHAPTER 5

The Taxonomy of Operational Risk

5.1 THE CRITERIA OF CLASSIFICATION

The heterogeneity of operational risk makes it necessary to come up with a system for classifying it and identifying its components. Hubner, Laycock, and Peemoller (2003) argue that one important advance in the rapidly improving understanding of operational risk is that the disaggregation and classification of operational risk is being put on a more rational footing. All efforts to define, analyze, and interpret operational risk are based on endeavors to come up with collections of risk types and the losses associated with these risks. Disaggregation involves separating out the different components of a risk cluster into categories.

5.1.1 General principles

The classification of operational losses (resulting from exposure to operational risk) can be approached from three alternative angles: the causes of operational failure, the resulting loss events, and the legal and accounting forms of consequential losses (that is, cause, event, and effect as shown in Figure 4.5). An operational (loss) event is defined by Haubenstock (2004) as "an event due to failed or inadequate processes, people or systems, or exposure to external events that caused, or potentially could have caused, a material loss or adversely impacted stakeholders ". The phrase "potentially could have caused" refers to "near-misses". The effects, according to the BCBS, are the direct losses resulting from (i) write-down of assets, (ii) regulatory compliance penalties, (iii) legal payments/settlements, (iv) customer

I. A. Moosa, *Operational Risk Management*

restitution, (v) loss of recourse, and (vi) loss of physical assets. Out of these effects, the two that need explaining are customer restitution and loss of recourse (as the others are straightforward). Restitution refers to payments to third parties resulting from operational losses for which the firm is legally responsible. Loss of recourse refers to losses experienced when a third party does not meet its obligations to the firm, provided that the outcome is attributable to an operational event. Moreover, the causal relations between the three levels (causes, events, and effects) are complex and indeterminate.

At first sight, the BCBS's definition is more consistent with the first alternative: it purports to identify the ultimate sources of operational losses by pointing to four broad categories of causes (people, processes, systems, and external events). The problem is that these generic sources of operational risk cannot be linked in a straightforward manner to the general types of loss identified by the BCBS. However, event- and effect-based regulatory classifications also appear in various Basel papers including the Quantitative Impact Study 3. The logical reason for the three dimensions of cause, event, and effect is easy to understand. Every operational risk manager who wants to know how to reduce exposure needs causal disaggregation to identify areas where management actions will have the desired effect (avoiding the cause outright or reducing the influence of the causer on the frequency or severity of the resulting event). An event-based classification makes the operational risk manager's task easier, as losses can be considered to materialize in an event.

Peccia (2003) argues that what is needed is developing a framework for classifying the causes of operational risk, because the usual classification of the causes of operational risk as either system problems or poor controls is unsatisfactory, giving rise to the possibility of misclassification or double counting. A more appropriate schema, he suggests, is the classification of losses by the area of impact on the results, as the ultimate objectives is to explain the volatility of earnings arising from the direct impact of losses on the financial results. Another problem is that the causes and effects of operational events are still commonly confused. Operational risk types, such as human risk and system risk, constitute the cause (not the outcome) of risk, as the latter is the monetary consequence. Peccia concludes that a classification based on causes is prone to errors and misunderstanding.

5.1.2 The BCBS classification

The Basel Committee has proposed the categorization of operational risk into manageable units according to regulatory-specified business lines or functional units. This may not be satisfactory for banks because the structure of regulatory business lines for the standardized approach does not reflect the way in which banks are structured or managed. With the help of the industry, the BCBS developed a matrix of seven broad categories of loss events that are further broken down into sub-categories and related activity examples. This classification is similar to the typology of hazards used by the insurance industry. Table 5.1 shows a listing of operational loss events with definitions and examples. Here, it is possible to relate event types to departments. For example, litigation and settlements can be

Table 5.1 The BCBS taxonomy of operational loss events

Event	BCBS Definition	Sub-categories/Examples
Internal fraud (IF)	Losses due to acts of fraud involving at least one internal party.	• Account take-over and impersonation • Bribes and kickbacks • Forgery • Credit fraud • Insider trading (not on firm's account) • Malicious destruction and misappropriation of assets • Tax noncompliance • Theft • Extortion • Embezzlement • Robbery • Intentional mismarking of position • Unauthorized and unreported transactions
External fraud (EF)	Same as internal fraud except that it is carried out by an external party.	• Computer hacking • Theft of information • Forgery • Theft
Employment practices and workplace safety (EPWS)	Losses arising from violations of employment and health and safety laws.	• Discrimination • Compensation and termination issues • Health and safety issues General liability
Clients, products and business practices (CPBP)	Losses arising from failure to meet obligations to clients or from the design of a product.	• Disputes over advisory services • Violation of anti-monopoly rules and regulations • Improper trade • Insider trading on firm's account

(*Continued*)

Table 5.1 (*Continued*)

Event	BCBS Definition	Sub-categories/Examples
		• Market manipulation • Money laundering • Unlicensed activity • Product defects • Exceeding client exposure limits • Account churning Aggressive sales • Breach of privacy • Misuse of confidential information • Customer discloser violations
Damage to physical assets (DPA)	Losses arising from damage inflicted on physical assets by a natural disaster or another event.	• Terrorism • Vandalism • Natural disasters
Business disruption and system failures (BDST)	Losses arising from disruptions to or failures in systems, telecommunication and utilities.	• Hardware • Software • Telecommunications • Utility outage • Utility Disruption
Execution, delivery and process management (EDPM)	Losses arising from failed transaction processing with counter-parties such as vendors	• Incorrect client records • Negligent loss or damage of client assets • Unapproved access to accounts • Client permissions • Missing and incomplete legal documents • Failed mandatory reporting obligations • Inaccurate external reports Non-client counterparty disputes • Accounting errors • Collateral management failure • Data entry, maintenance or loading error • Delivery failure • Miscommunication • Missed deadlines • Vendor disputes

Source: BCBS (2004a)

related to the Legal Department, compensation claims can be related to Human Resources, system failures to IT, settlement failures to Treasury, and errors in the books to the Accounts Department.

An alternative classification structure is based on functional units but this is specific to an individual firm. For example, the term "legal department" can be expected to vary between firms according to their history and internal environment. In the same firm, the term may vary between countries in response to local requirements. Yet, there is clear added value in using this classification, as disaggregation empowers and encourages the functions to monitor and manage risk on a structural basis. Moreover, this approach emphasizes the role of the functional units as providers of proactive, rather than reactive, risk management support to the risk owners.

One problem with this classification is that some of the subcategories do not have precise meaning. Take, for example, "fraud", which does not have an exact legal or regulatory meaning. It is used as a generic term to designate a variety of forms of (mostly nonviolent) economic wrongdoing, whose commission constitutes a criminal offence and/or a civil wrong. Examples of fraud are theft, unauthorized withdrawal of money from ATMs, forgery of instruments, false accounting, fraudulent conveyance, and unauthorized trading. One should distinguish between three roles that a bank can play in fraud: perpetrator, vehicle, or victim. Tax fraud and money-laundering offences are common examples of economic crimes committed by banks. Fraud can be committed by banks and employees against clients and counterparties. In this sense, it is misleading to describe fraud as a risk faced by banks. Rather, the bank itself is the source of risk borne by outside parties (from the bank's perspective, it is legal risk). When the bank is a vehicle for fraud, it is not subject to the direct risk of loss, but reputational risk is present. There may be cases where the law reallocates financial risk, forcing banks to bear the loss and compensate the victims on the grounds of contributory negligence or some breach of conduct-of-business standards (for example, failure to cancel a reported stolen card on time, or not checking signatures). In cases where a bank is the victim or the vehicle, fraud can be internal or external. The BCCI, for example, was both the perpetrator (for example, money laundering) and the victim (fraudulent lending, theft, and other practices of its management).

It may also be the case that some important subcategories are missing. For example, should employment practices and workplace safety have a category called "employee offensive odour". This is not a joke. In a recent article in *Financial Times*, Sanghera (2005) concluded after some research that "dealing with smelly employees in these days of windowless workplaces and cubicles may be one of the biggest management challenges of our time". Indeed, a message on *workplace.net* says "any one who has an offensive body odour and works with other people who find it offensive is breaching health and safety law guidelines". This issue may lead to termination problems and people failure, as the message says that body odor can cause "disruption in the workplace". Sanghera (2005) says explicitly that "barely a month passes without some smell-related dispute hitting the headlines", referring to the "worker from Portsmouth getting sacked because his bosses claim he is too pongy".

5.1.3 Classification according to causes (sources)

The classification of operational risk according to the cause (the sources of risk) is consistent with Mestchaian's (2003) suggested decomposition of the BCBS's definition of operational risk. Table 5.2 reports the risk sources, their categories and examples. For instance, external risk includes external fraud (such as external money laundering), natural disasters (such as floods), and non-natural disasters (such as arson). This classification goes beyond the BCBS categories.

Table 5.2 Operational risk by cause

Risk	Category	Examples
People Risk	Disclosure-related issues	• Concealing losses • Misuse of important information • Non-disclosure of sensitive issues
People Risk	Employment, health and safety	• Employee actions • Compensation disputes • Employee defection • Labor disputes • Strikes • Employee illness • Employee injury • Forced retirement • Promotions related disputes • Discrimination and harassment issues • Infliction of distress
People Risk	Internal fraud	• Embezzlement • Money laundering • Unauthorized fund transfers • Accounting fraud • Credit card fraud • Tax fraud
People Risk	Trading misdeeds	• Insider trading • Market manipulation • Improper pricing • Unauthorized trading

(*Continued*)

Table 5.2 (*Continued*)

Risk	Category	Examples
Process Risk	Errors and omissions	• Employee error • Inadequate quality control • Inadequate security • Inadequate supervision • Failure to file a proper report
Process Risk	Transaction and business process risk	• Inadequate account reconciliation • Inadequate transaction completion • Inadequate transaction execution • Inadequate transaction settlement • Lack of proper due diligence • Loss of critical information
Technology Risk	General technology problems	• New technology failure • Technology-related operational errors
Technology Risk	Hardware	• System failure • Outdated hardware
Technology Risk	Security	• Computer virus • Data security • Hacking
Technology Risk	Software	• Inadequate testing • System failure • Incompatible software
Technology Risk	Systems	• Inadequate systems • System maintenance
Technology Risk	Telecommunications	• Fax • Internet • E-mail • Telephone
External Risk	External fraud	• Burglary • External misrepresentation • External money laundering • Robbery
External Risk	Natural disasters	• Flooding • Hurricane • Blizzard • Earthquake
External Risk	Non-natural disasters	• Arson • Bomb threat • Explosion • Plane crashes • War

5.2 FREQUENCY AND SEVERITY OF LOSS EVENTS

Operational risk events can be divided into high-frequency, low-severity events (which occur regularly) and low-frequency, high-severity events (which are rare but produce huge losses if they occur). The low-frequency, high-severity risks (such as internal fraud, which could jeopardize the whole future of the firm) are risks associated with loss events that lie in the very upper tail of the total loss distribution. High-frequency, low-severity risks (such as credit card fraud and some human risks) have high expected loss but relatively low unexpected loss.

The BCBS (2002b) has produced results on the frequency and severity of each type of risk event for a typical bank with investment, commercial, and retail operations. These are reported in Table 5.3, showing that internal fraud is a low-frequency, high-severity risk event. These are the kinds of event that can bring a major bank to its knees (for example, the Barings case). It is also shown that external fraud is less severe than internal fraud although it is more frequent. Damage to physical assets, on the other hand, is a low-frequency, low-severity event and so is business disruption and system failure. Exactly the opposite to internal fraud is execution, delivery, and process management, which is a high-frequency, low-severity event.

The frequency and severity of operational loss events depend on and vary with the business line, as shown in Table 5.4. For example, internal fraud is a low-frequency, high-severity event in corporate finance, trading and sales, commercial banking, and asset management, but it is a low-frequency, medium-severity event in retail banking, payment and settlement, and in agency and custody. Execution, delivery, and process management is a low-frequency, low-severity event in corporate finance, but it is a high-frequency, low-severity event in trading and sales, retail banking, and in payment and settlement. It is also a medium-frequency, low-severity event in commercial banking, agency and custody, and asset management.

Table 5.3 Frequency and severity of operational risk events

Risk Event	Frequency	Severity
Internal fraud	L	H
External fraud	H/M	L/M
Employment practices and workplace safety	L	L
Clients, products, and business practices	L/M	H/M
Damage to physical assets	L	L
Business disruption and system failures	L	L
Execution, delivery, and process management	H	L

Table 5.4 Frequency (top) and severity (bottom) by business line and risk type

	Internal fraud	External fraud	Employment practices and workplace safety	Clients, products and business practices	Damage to physical assets	Business disruption and system failures	Execution, delivery and process management
Corporate Finance	L	L	L	L	L	L	L
	H	M	L	H	L	L	L
Trading & Sales	L	L	L	M	L	L	H
	H	L	L	M	L	L	L
Retail Banking	L	H	L	M	M	M	H
	M	L	L	M	L	L	L
Commercial Banking	L	M	L	M	L	L	M
	H	M	L	M	L	L	L
Payment & Settlement	L	L	L	L	L	L	H
	M	L	L	L	L	L	L
Agency & Custody	L	L	L	L	L	L	M
	M	L	L	M	L	L	L
Asset Management	L	L	L	L	L	L	M
	H	L	L	H	L	L	L
Retail Brokerage	L	L	L	L	L	M	M
	M	M	L	M	L	L	L

Based on the frequency of loss events, Pezier (2003a) classifies operational risk into nominal, ordinary, and exceptional risks. Nominal operational risk is the risk of repetitive losses (say, losses that may occur on average once a week or more frequently) associated with an ongoing activity such as settlement risk, minor external fraud (credit cards), or human error in transaction processing. Ordinary operational risk is the risk of less frequent (say, between once a week and once every generation) but larger losses, yet not life-threatening for the firm. Exceptional operational risk produces losses that have no more than a few percent chance of occurrence over a year, but those losses may be life-threatening.

Examples of exceptional risk events are reported in Table 5.5. The majority of the institutions listed in the table went bankrupt, were taken over, or they

Table 5.5 Examples of exceptional operational loss events

Year	Company	Cause of Loss
1991	Salomon Brothers (U.S.)	Treasury bond primary market manipulation
1993	Bank of Commerce and Credit International (BCCI) (Luxembourg)	Illegal activities (drugs, arms)
1994	Kidder Peabody (U.S.)	Management Incompetence
1995	Barings Bank (U.K.)	Rogue trading and management incompetence
1995	Diawa Securities (Japan)	Involvement with gangsters
1996	Bankers Trust (U.S.)	Selling products that clients did not fully understand
1997	Morgan Grenfell (U.K.)	Unauthorized investment in illiquid assets
1997	NatWest Markets (U.K.)	Mispricing of derivatives
1998	Long-Term Capital Management (U.S.)	Lack of transparency, conflict of interest, model bias and uncontrolled leverage
2000	Equitable Life Assurance Society (U.K.)	Non-respect of guaranteed annuity contracts
2001	Cantor Fitzgerald and Others (U.S.)	Terrorist attack on World Trade Center
2002	Allied Irish Bank (U.S.)	Rogue trading
2002	Merrill Lynch (U.S.)	Biased analyst recommendations
2003	Central Bank of Iraq (Iraq)	External fraud (by the former President)
2004	Yukos Oil Company (Russia)	Internal fraud
2005	Central Bank of Brazil (Brazil)	External fraud (a brilliantly-executed bank robbery)
2006	Royal Bank of Scotland (U.K.)	External fraud

were forced to merge as a consequence of their losses (hence the characteristic of life-threatening loss events). These were all consequences of deliberate actions and not mere accidents. In most cases, these actions were unethical, illegal, or criminal. They were not necessarily initiated by senior management but they were at least allowed to endure by management incompetence and/or negligence. The root problem is individual or corporate greed. These loss events have been widely publicized and used as case studies.

Sometimes, of course, it may not be clear whether the failure of a firm is due to operational risk only or a multiplicity of risks (recall the discussion in Chapter 4 on distinguishing operational loss events from market and credit loss events). Take, for instance, the case of the most publicized hedge fund failures during the period 1994–2002, which are shown in Figure 5.1. These failures brought total losses of $12.8 billion caused by a variety of factors, as shown in Table 5.6. As we can see, the failure of the ten hedge funds is attributed to more than operational risk, but it is the diversity of operational risk that makes it appear more prominently in Table 5.6. In a Capco Research (2002) paper, these failures were attributed mostly (50 percent) to operational risk, followed by investment risk (38 percent) then business risk (6 percent) and multiple risks (6 percent). Presumably investment risk here means market risk and credit risk. Although one tends to think that market risk would be more important

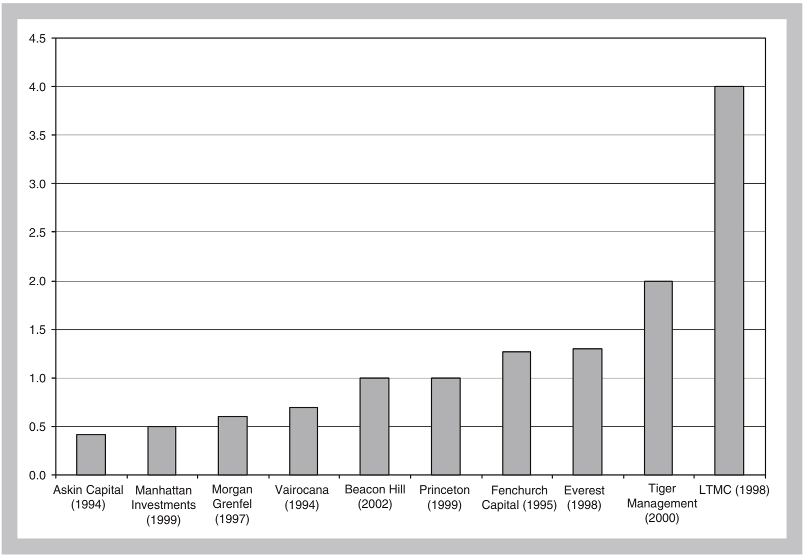

Figure 5.1 Losses incurred in the ten most publicized hedge fund failures ($billion)

Table 5.6 The risk factors responsible for hedge fund failures

Market Risk Factors	Credit Risk Factors	Operational Risk Factors
• Trading losses • Directional bets • Highly complex portfolios • Unfavorable market • conditions • High and uncontrolled leverage	• Post-Russian debt-default shock	• Weakness in the risk management systems • Misrepresentation of fund performance • Unauthorized holdings of unlisted securities • Pricing irregularities • Lack of liquidity • Conflict of interest • Collusion with a prime broker • Absence of adequate risk management system for new strategies • Lack of transparency to prime broker • Model bias in the risk management process

than operational risk in the case of hedge funds, this is obviously not the case here. Thus, the prominence of operational risk in Table 5.6 is not only due to its diversity but also to the fact that the failures are attributed mostly to operational risk.

5.3 A CLOSE LOOK AT OPERATIONAL LOSS FIGURES

To get a feel of the frequency and severity of operational loss events, we examine the loss data reported in BCBS (2003c) as a result of the 2002 data collection exercise. The BCBS asked participating banks to provide information on operational losses in 2001. A total of 89 banks participated in this exercise, reporting the number of loss events and the amounts involved (in millions of euros). The reported losses were classified by business lines and event types according to the BCBS's classification, but some reported losses were unclassified. As far as the number of losses is concerned, a total of 47,269 events were reported, 43 percent of which were events of external fraud (Figure 5.2) and more than 60 percent were in retail banking (Figure 5.3). As far as the loss amount is concerned, the total amount lost was EUR7.8 billion, 29 percent of which came under execution, delivery, and process management (Figure 5.4) and 290 percent was under retail banking and commercial banking (Figure 5.5). In terms of business line/event type combinations, the most frequent losses occurred

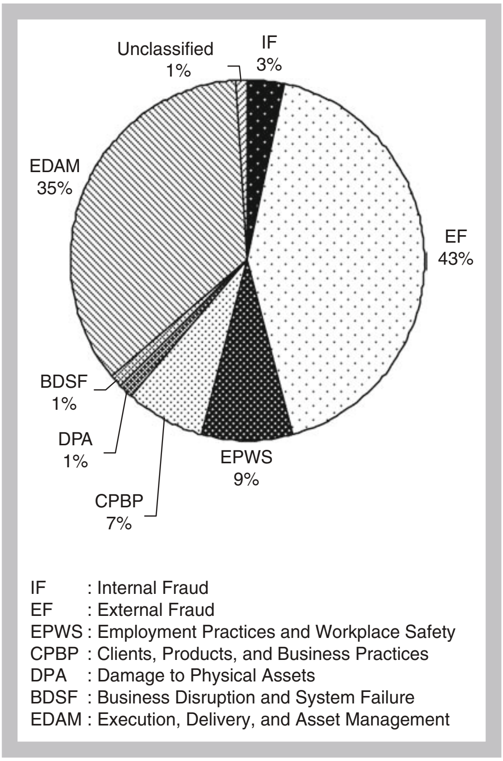

Figure 5.2 Number of losses by event type (the BCBS (2003c) data)

in external fraud in retail banking, whereas the largest loss amounts occurred in damage to physical assets in commercial banking.

Switching now to the concepts of frequency and severity, the frequency is the number of loss events, whereas average severity can be calculated by dividing the total loss incurred under a certain loss event type or business line by the corresponding number of losses. Figures 5.6 and 5.7 report the severity of losses by event type and business line, respectively.

The operational loss events reported in Table 5.4 encompass mostly financial institutions. But all entities are exposed to operational risk in the course of their daily business, and for this reason, it may be useful to examine some operational risk events that span a wide variety of entities. Appendix 5.1 contains a table showing 62 randomly selected operational loss events that took place between 1984 and 2006. The reported operational losses were incurred by banks (including central banks), non-bank financial institutions, and firms operating in various sectors (manufacturing, utilities, transportation, food, mining, and entertainment), as well as universities, cities, and

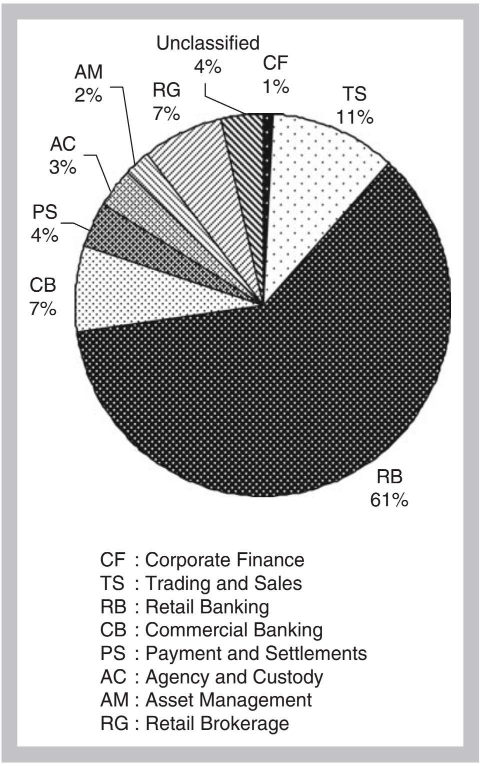

Figure 5.3 Number of losses by business line (the BCBS (2003c) data)

government entities. Because the BCBS's classification of operational loss events covers banks only, a large number of loss events appear as unclassified. The losses reported in the table range between the $9499 dollar incurred by the Yorkshire Building Society (as a result of an alleged sex discrimination case) and the $95 billion incurred by New York City as a result of the 9/11 terrorist attacks.

Table 5.7 shows a classification of the 62 events by type and business line, providing information on the number of events, the mean and the median values of the loss incurred, as well as the smallest and largest loss in each case. By event type, the most serious events (measured by the mean value of the loss) are damage to physical assets and internal fraud, with the former appearing more important because of the losses incurred by New York City as a result of the 9/11 attacks. By business line, the unclassified business lines are the ones where the big losses were incurred, this is mainly due to the fact that these losses were incurred by non-financial firms and other entities, which are not covered by the business line classification

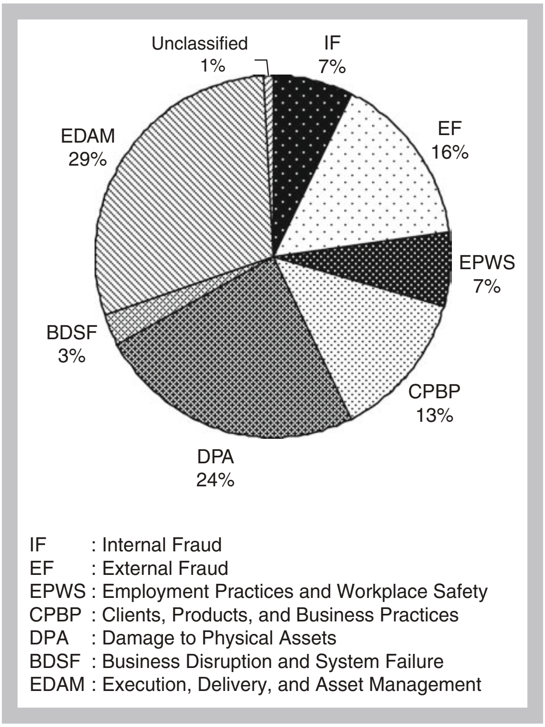

Figure 5.4 Loss amount by event type (the BCBS (2003c) data)

of the BCBS. Naturally, the judgment changes if we consider the median loss as opposed to the mean loss: in this case, for example, external fraud appears to be more serious than internal fraud. In terms of the number of events (frequency), events related to clients, products, and business practices are the most frequent followed by internal fraud.

Table 5.8 shows a two-way classification of the same loss events by type and business line. If we exclude the events recognised by the unclassified business lines, we can see that the most common combination are loss events related to clients, products and business practices in corporate finance followed by internal fraud in commercial banking. While these tables provide some interesting information, one has to be careful about deriving some overall conclusions from a relatively small sample of events.

Finally, Appendix 5.2 presents a brief description of loss events organized by event type and business line as reported by the media. This is just a drop in the ocean compared to the universe of operational loss events. Operational losses are indeed more frequent than what one may believe, which is definitely the impression one gets by examining operational loss databases.

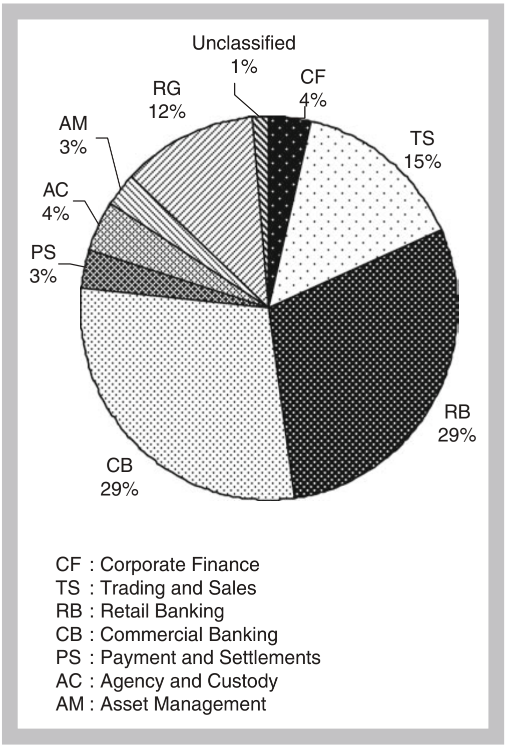

Figure 5.5 Loss amount by business line (the BCBS (2003c) data)

5.4 EXTERNAL OPERATIONAL LOSS DATABASES

In this section we deal with external databases as opposed to internal databases of individual firms (which we will deal with in the following section). External databases may take two forms. The first, such as the British Bankers Association's (BBA) database the global operational loss database (GOLD), is a contributory scheme where members contribute their own loss data in return for access to the loss data of other members, ending up with an industry-pooled database. The second type are the public databases that record publicly released loss events, including the databases of vendors such as OpRisk Analytics and OpVantage through the OpRisk Global Data and OpVar database, which are parts of the SAS Institute, Inc and a division of Fitch Risk Management, respectively. These vendors collect data from public sources, such as newspaper reports, court filings, and Securities and Exchange Commission (SEC) filings. As well as classifying losses by the Basel business line and causal type, the databases also include descriptive information on each loss event. A description of the GOLD database can be found on the BBA's website (www.bba.org.uk).

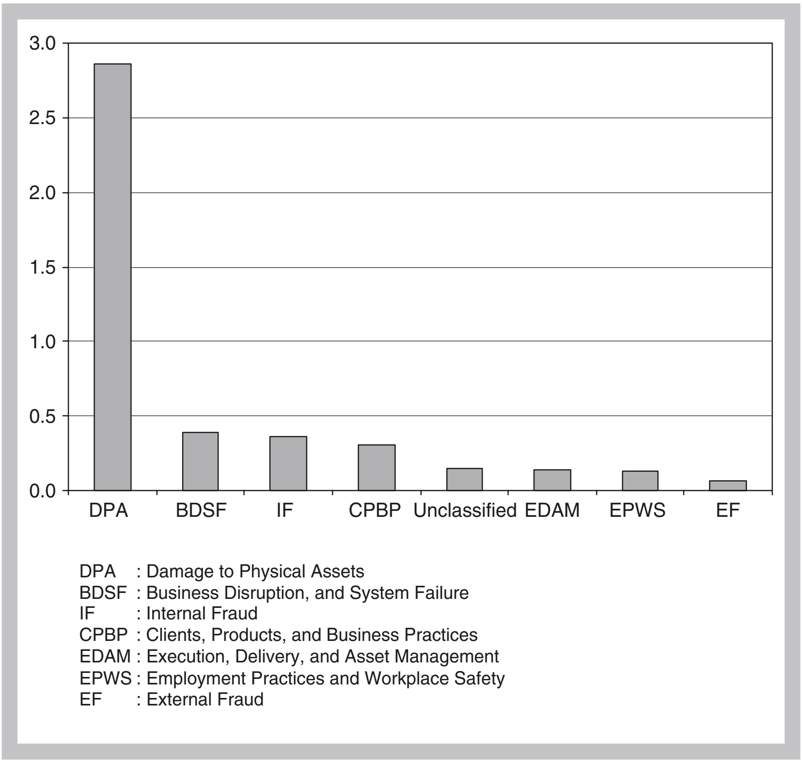

Figure 5.6 Severity by event type

Imeson (2006a) describes GOLD and similar databases by pointing out that these databases allow firms to consider the following questions: (i) What are typical loss events? (ii) Could loss circumstances occur in my firm? (iii) Would we see similar loss amounts? (iv) Which operational risks are subject to the highest losses? (v) How do loss events impact on the business? (vi) Which business areas suffer most losses? (vii) Are my controls or risk indicators appropriate? and (viii) Is reputational risk associated with loss events?

Baud, Frachot, and Roncalli (2002) identify two differences between the public databases and the industry-pooled databases, the first of which is the threshold for the recorded losses, as the threshold is expected to be much higher in the case of public databases than in the industry-pooled database. The second difference is the level of confidence one can place on the information provided by the database. For example, nothing ensures that the threshold declared by an industry-pooled database is the actual threshold, as banks are not necessarily prepared to uncover all losses above this threshold even though they pretend to do so.

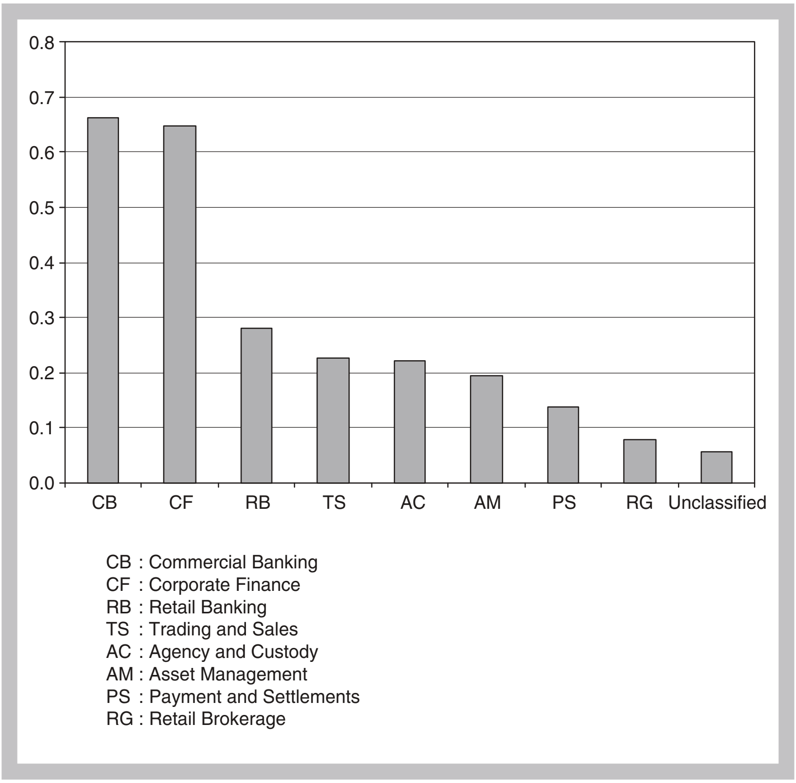

Figure 5.7 Severity by business line

An operational loss database must include, as a minimum, information on (i) the business line recognizing the loss; (ii) the unit in the business line recognizing the loss; and (iii) the function/process within the unit recognizing the loss. The information provided on each loss event include: (i) the firm incurring the loss; (ii) the amount; (iii) the start, end, and settlement dates; (iv) the type of entity incurring the loss; (v) the event type; and (vi) the business line. Also reported is a description of the event. Most of the information is obtained from the media.

Cagan (2001) argues that collecting data according to less optimal standards can misinform the decision-making process. Therefore, she recommends the following criteria for proper data collection:

- Data must be collected according to the reasons for (sources of) the losses.
- Data records should include contributory factors (such as the lack of controls), although these factors may not be the cause. This is because

Table 5.7 Loss events (million dollars) by event type and business line (62 events)

	Number	Mean	Median	Minimum	Maximum
Event Type					
Internal fraud	15	677.0	9.1	0.38	9,300.0
External fraud	5	225.0	50.4	0.15	1,000.0
Employment Practices and Workplace safety	7	17.2	1.2	0.95	100.0
Clients, products and business practices	22	72.9	8.3	0.44	925.0
Damage to physical assets	9	10,700.0	41.3	1.0	95,000.0
Business disruption and system failures	1	175.0	175.0	175.0	175.0
Execution, delivery and process management	3	48.5	20.0	0.75	125.0
Business Line					
Corporate Finance	9	138.0	20.0	0.9	925.0
Trading & Sales					
Retail Banking	2	7.5	7.5	0.01	15.0
Commercial Banking	9	189.0	50.4	0.28	1,000.0
Payment & Settlement	1	88.0	88.0	88.0	88.0
Agency & Custody					
Asset Management	3	14.1	7.3	1.3	33.6
Retail Brokerage					
Unclassified	38	2.8	9.5	0.1	95,000.0

the contributory factors may intensify the severity of the loss. It was Leeson's activities that brought the demise of Barings, but inadequate supervision contributed to the severity of the loss. With adequate supervision, it is likely that his activities would have been put to an end at an earlier stage and a lower level of losses.

Table 5.8 Classification by event type and business line (million dollars)

	Internal fraud	External fraud	Emp practices and workplace safety	Clients, products, and business practices	Damage to physical assets	Business disruption and system failures	Execution, delivery, and process management
Corporate Finance							
Number	1			7			1
Mean	127.5			156.2			20.0
Trading & Sales							
Number							
Mean							
Retail Banking							
Number			1		1		
Mean			0.1		15.0		
Commercial Banking							
Number	6	3					
Mean	96.5	37.4					
Payment & Settlement							
Number	1						
Mean	88.0						
Agency & Custody							
Asset Management							
Number	2			1			
Mean	20.5			1.3			
Retail Brokerage							
Unclassified							
Number	5	2	6	14	8	1	2
Mean	1,887.4	3.3	20.1	98.0	12,035.0	174.6	62.7

- Each data record should include the type of loss incurred or the loss effect for the purpose of proper risk quantification.
- Loss events should be tracked over their life cycles, as they are often not one-time events. This is why a database may show dates for the beginning, end, and settlement of loss events.
- The scaling of data should be based on asset size "buckets" to avoid revealing the identity of the firm enduring operational loss.

Thrilwell (2003) describes how an operational loss database should be constructed and run with reference to the BBA's GOLD, where members of the BBA pool their operational loss data. The main driving force behind the willingness of banks to take part in this venture is their desire to benchmark their performance against their peers. In his analysis, Thirlwell talks about some general issues pertaining to the construction of an operational loss database, including confidentiality, anonymity, trust between participants, consistency, and flexibility/evolution. On the general issues he suggests the following:

1. The key factor in developing a database is confidentiality between the providers and the holder of the data.
2. Anonymity means that there are no clues that could trace a loss back to a particular participant unless the event is publicized in the media.
3. Trust is a fundamental factor if the participants are to report their loss events.
4. Consistency means that those reporting loss events should place similar losses in the same categories (that is, consistency in classification).
5. The database must be structured in such a way as to be easy to modify, should the need arise (for example, the emergence of new kinds of risk).

Thirlwell (2003) also talks about what he calls specific issues that include (i) operational loss versus operations loss; (ii) the classification of losses; (iii) the distinction between hard losses, soft losses, and near misses; (iv) the choice between cause/event and impact/event; (v) the reporting threshold; and (vi) scaling. On these issues he makes the following points:

1. Operational risk covers a far broader category of risk than simply operations risk (hence the distinction between operational risk and operations risk).
2. For the purpose of constructing a database, it is best to identify generic causes of losses since they can apply to a number of business activities.

3. Soft losses, contingent losses, and near misses are excluded from the database because they are difficult to quantify.
4. The database should identify the number or size of the events that give rise to a loss, then the cause is identified by a narrative field.
5. Establishing a threshold for reporting is determined by two factors: the purpose of the database and the cost/benefit balance.
6. One bank's minor event is another bank's catastrophe, which requires some scaling factor, such as assets, transaction volume, income, expenses, etc.

While operational risk databases are a useful means of providing information, Thirlwell (2003) identifies some of their limitations, including the following:

1. The data are not independently audited.
2. The database does not provide information on the quality of controls in the reporting banks.
3. The choice of the reporting threshold affects the quantity of data reported.
4. There are some data reporting problems, including the double counting of operational risk, credit risk, and market risk, as well as some legal and other reasons that prevent reporting.

5.5 INTERNAL OPERATIONAL LOSS DATABASES

The Basel II Accord places significant emphasis on the construction of internal loss databases for the purpose of measuring and managing operational risk. The BCBS (2003a) stipulates that data on operational losses is a tool that can be used for validating risk estimates, being a component of risk reporting and a key input in any AMA model of operational risk. Cagan (2001) argues that internal databases resemble external databases in the sense that both need to be supported by a well-defined body of data standards, but they differ in the type of losses they cover. While internal databases record the high-frequency, low-severity losses that characterize daily operations, external databases tend to cover the low-frequency, high-severity losses.

Haubenstock (2004) argues that collecting operational loss data is more beneficial to the underlying bank than just the satisfaction of the regulatory requirements, including the very act of collecting the data and the calculation of regulatory capital. It is indeed a component of the risk management framework (see Chapter 8), which is implemented for the ultimate objective of reducing both the frequency and severity of operational losses. More specifically, Haubenstock (2004) lists the following advantages of operational loss data collection:

- Increasing awareness of operational risk and its potential harm to the firm.
- Quantifying exposure, which helps efforts to focus resources on risk mitigation where it is needed.
- Analysis of the causes of events, which can be conducive to the improvement of controls.
- Evaluating the self-assessment process, because actual loss events can be used as a quality check over self-assessment. For example, a department that endures 100 operational loss events with an average severity of $50,000 cannot (without proper justification) make the prediction that it will only endure five loss events with an average severity of $10,000 over the following year.

An important question that crops up in any endeavor to construct an operational loss database is what constitutes an operational loss event (that is, what to record and what to leave out). According to the Basel II Accord, only direct losses are to be recorded, which encompass categories ranging from the write-down of assets to the loss of physical assets. The justification for this restriction is that these effects are objective and can be measured directly and consistently. Just like the choice of the definition of operational risk, this choice is rather narrow for a pragmatic reason, to facilitate the measurement of operational risk and hence regulatory capital. However, Haubenstock (2004) argues that firms should define their own data collection policies, which may mean going beyond Basel II. As a matter of fact, some external databases go beyond the Basel II recommendations by recording events that are not recognized by the Accord for the purpose of calculating regulatory capital. Why? Because the collection of operational loss data has more benefits than the mere regulatory compliance, and because (as we will see in Chapter 8) it is an integral part of the operational risk management framework. Likewise, Cagan (2001) argues that although it makes sense to adopt a definition for quantifying capital that excludes items that cannot be easily calculated, it is important to collect softer and less quantifiable losses for the sake of qualitative analysis.

In addition to the direct losses identified by Basel II, Haubenstock (2004) recommends that firms should collect data on near misses, which are events where some type of failure occurred without incurring financial loss, and indirect losses (or associated costs), which include items like business interruption, forgone income, loss of reputation, and poor quality. He also recommends the inclusion of strategic or business risk events. We have already seen that the exclusion of business risk from the definition of operational risk is a controversial issue, which Haubenstock (2004) capitalizes upon in his defense of the inclusion of business risk. For example, he takes the difficulty of attributing the following costs to either operational risk or business risk to mean that the line between operational risk and strategic risk is not clear at all: pulling out of a country, a failed product introduction, restructuring costs after layoff and excess real estate capacity due to inaccurate estimation.

Another important issue is the determination of the loss threshold, which is the amount below which the underlying loss event will not be recorded. The answer is simply that the choice of a threshold is a matter of costs and benefits, which means that it should vary across firms and activities. Some guidance can be obtained from the external databases. For example, the Riskdata Exchange Association, the American Bankers Association, and the BBA use thresholds of $25,000, $10,000, and $50,000, respectively. Roehr (2002) argues that the threshold, which is necessary to make the task of data collection manageable and cost effective, may change over time, depending on the business line and event type. He also argues that thresholds are likely to be much higher in external than in internal databases.

In addition to these issues, other related issues are confidentiality of the data and the mechanics of the collection process, including roles and responsibilities. We will have more to say about the modes of operational loss data collection in Chapter 8, so we close this chapter by saying a few words about confidentiality. In general, operational losses and events are regarded as very sensitive information, which means that there should be some standard for disclosure within and outside the firm. Firms, therefore, design their own confidentiality and data access restriction policies with the objective of striking a balance between security and transparency.

APPENDIX 5.1 SELECTED OPERATIONAL LOSS EVENTS

Table 5A1.1 contains 62 randomly selected operational loss events organized chronologically, spanning the period 1984–2006. The table reports the settlement date (when the case is closed), the name of the entity incurring the loss, the loss amount in million US dollars, the business line and event type. When no specific business line appears (–), this means that it is unclassified by the BCBS. This is because the BCBS classification is designed for banks only, whereas this table reports loss events endured by a variety of entities, including cities and universities. The source of information is various media outlets.

Table 5A1.1 Selected operational loss events reported by the media

Settlement Date	Firm	Loss (US$ million)	Business Line	Event Type
23/05/1984	Nestle S.A.	41.3	–	Damage to Physical Assets
01/05/1988	Nissan Motor Company	4.9	–	Clients, Products, and Business Practices
12/07/1989	Walt Disney Company	100.0	–	Employment Practices and Workplace Safety
01/10/1990	Eastman Kodak	92.5	Corporate Finance	Clients, Products, and Business Practices
01/02/1991	Mobil Oil Company	1.0	–	Clients, Products, and Business Practices
20/12/1991	Apple Computers	19.8	–	Clients, Products, and Business Practices
01/01/1992	Kuwait Oil Tankers Company	100.0	–	Internal Fraud
01/02/1992	Motorola Inc.	15.1	–	Clients, Products, and Business Practices
01/02/1992	Xerox Corp.	2.5	–	Clients, Products, and Business Practices
22/07/1992	Midland Bank	6.0	Commercial Banking	Internal Fraud
01/10/1992	Caterpillar Inc.	15.7	–	Employment Practices and Workplace Safety
20/05/1993	Nippon Steel	127.5	Corporate Finance	Internal Fraud
01/07/1993	Louisiana Interstate Gas Company	35.0	–	Clients, Products, and Business Practices
01/09/1993	Yamaichi Securities Co.	96.0	–	Clients, Products, and Business Practices
28/10/1993	Land Bank of Taiwan	4.0	Commercial Banking	Internal Fraud

(*Continued*)

Table 5A1.1 (*Continued*)

Settlement Date	Firm	Loss (US$ million)	Business Line	Event Type
01/01/1994	British Gas	1.2	–	Employment Practices and Workplace Safety
01/01/1994	Sao Paulo State Electricity Company	1.0	–	Damage to Physical Assets
01/02/1994	Air France	131.5	–	Damage to Physical Assets
01/02/1994	US Airways	8.1	–	Damage to Physical Assets
01/10/1994	Stanford University	3.2	–	Internal Fraud
01/01/1995	Lockheed Martin Corporation	24.8	–	Internal Fraud
10/03/1995	Kraft Foods Inc.	75.3	Corporate Finance	Clients, Products and Business Practices
01/12/1995	University of Wisconsin	3.5	–	Damage to Physical Assets
01/01/1996	Coca-Cola	2.0	–	Clients, Products, and Business Practices
01/01/1996	University of California at Berkley	1.0	–	Employment Practices and Workplace Safety
01/01/1996	Yorkshire Building Society	0.01	Retail Banking	Employment Practices and Workplace Safety
08/03/1996	Nike Inc.	15.0	–	Clients, Products, and Business Practices
31/12/1996	Bangkok Bank of Commerce	88.0	Payment and Settlement	Internal Fraud
01/02/1997	Toyota Motor Corporation	200.0	–	Damage to Physical Assets
01/01/1998	National Mortgage Bank of Greece	4.0	–	Clients, Products and Business Practices
01/01/1998	PepsiCo Inc.	2.4	–	Clients, Products, and Business Practices
17/02/2000	Singapore Airlines	9.1	–	Internal Fraud
15/06/2000	Amsterdam Stock Exchange	65.0	Corporate Finance	Clients, Products, and Business Practices
11/09/2001	New York City	95,000.0	–	Damage to Physical Assets
11/09/2001	Zurich Financial Services Group	900.0	–	Damage to Physical Assets

(*Continued*)

Table 5A1.1 (*Continued*)

Settlement Date	Firm	Loss (US$ million)	Business Line	Event Type
31/12/2001	Agricultural Development Bank of China	1.7	Commercial Banking	Internal Fraud
11/02/2002	British Airways	6.5	–	External Fraud
31/10/2002	Municipal Credit Union of New York City	15.0	Retail Banking	Damage to Physical Assets
19/03/2003	Central Bank of Iraq	1,000.0	Commercial Banking	External Fraud
25/03/2003	Commerzbank	33.6	Asset Management	Internal Fraud
01/04/2003	Yale University	0.15	–	External Fraud
31/05/2003	UK Inland Revenue	174.6	–	Business Disruption and System Failure
28/08/2003	Central Bank of Sweden	0.1	–	Employment Practices and Workplace Safety
19/03/2004	Bank of India	82.2	Commercial Banking	Internal Fraud
05/07/2004	Merchant Bank of Central Africa	19.0	Corporate Finance	Clients, Products, and Business Practices
06/09/2004	New Zealand Stock Exchange	0.44	–	Clients, Products, and Business Practices
20/10/2004	KPMG International	10.0	–	Clients, Products, and Business Practices
20/12/2004	Yukos Oil Company	9,300.0	–	Internal Fraud
31/12/2004	Bank of China	485.0	Commercial Banking	Internal Fraud
12/04/2005	New York Stock Exchange	20.0	Corporate Finance	Execution, Delivery, and Asset Management
10/05/2005	Banca Nazionale del Lavoro	1.3	Asset Management	Clients, Products, and Business Practices
18/05/2005	Morgan Stanley	1.6	Corporate Finance	Clients, Products, and Business Practices
08/08/2005	Central Bank of Brazil	70.0	Commercial Banking	External Fraud
29/08/2005	Lloyds of London	300.0	–	Clients, Products, and Business Practices
03/09/2005	State Bank of India	0.3	Commercial Banking	Internal Fraud
24/01/2006	Lloyds of London	124.6	–	Execution, Delivery, and Asset Management

(*Continued*)

Table 5A1.1 (*Continued*)

Settlement Date	Firm	Loss (US$ million)	Business Line	Event Type
15/03/2006	Commonwealth Bank of Australia	7.3	Asset Management	Internal Fraud
25/04/2006	British Petroleum	2.4	–	Employment Practices and Workplace Safety
12/07/2006	Bank of America	0.75	–	Execution, Delivery, and Asset Management
24/07/2006	Credit Suisse First Boston	6.7	Corporate Finance	Clients, Products, and Business Practices
24/07/2006	Lehman Brothers	0.88	Corporate Finance	Clients, Products, and Business Practices
02/08/2006	Royal Bank of Scotland	50.4	Commercial Banking	External Fraud

APPENDIX 5.2 A DESCRIPTION OF SOME OPERATIONAL LOSS EVENTS BY TYPE AND BUSINESS LINE

Tables 5A2.1 and 5A2.2 contain a brief description of selected loss events, as reported by the media, classified by event type and business line, respectively.

Table 5A2.1 A description of some operational loss events by type

Event Type	Company	Description of Event
Internal Fraud (Robbery)	Westpac Banking Corporation (Australia)	A senior bank customer relations manager stole more than AUD3.5 million between February 2003 and December 2004 from 15 customers' accounts. He was arrested in July 2006 and charged with obtaining money by deception and several counts of signature forgery.
Internal Fraud (Tax Evasion)	GlaxoSmithKline plc (U.S.A.)	In September 2006, a settlement was reached between the company and the U.S. Internal Revenue Service, whereby the Company agreed to pay $3.4 billion to settle a dispute over the taxation dealings between the British parent company and its U.S. subsidiary over the period 1989-2005.
Internal Fraud (Robbery)	JP Morgan Chase & Co (U.S.A.)	At a hearing in a U.S. federal court held on 21 August 2006, a former mailroom employee pleaded guilty to the theft of some $100 million in corporate cheques from a lock-box facility in New York.

(*Continued*)

Table 5A2.1 (*Continued*)

Event Type	Company	Description of Event
Internal Fraud (Credit Fraud)	Agricultural Bank of China (China)	In June 2006, China's Audit Office announced that it had discovered cases of criminal activity and fraudulent loans worth 51.5 billion yuan ($6.45 billion) at the Agricultural Bank of China.
Internal Fraud (Credit Fraud)	Universal Corporation (U.S.A.)	In September 2006, a California court ordered Universal Corporation to pay two of its employees $25 million in compensation for retaliation against them after they had reported fraudulent insurance claims.
Internal Fraud (Credit Fraud)	ANZ (Australia)	In June 2006 charges were brought against a former employee of the ANZ following an investigation by the Australian Securities and Investment Commission into unauthorized loans totaling AUD14.5 million.
External Fraud (Robbery)	Shanghai City Pension Fund (China)	A 33 year old Shanghai tycoon was arrested in October 2006 following an investigation of his role in the disappearance of 3.2 billion yuan ($400 million) from the Shanghai City Pension Fund.
Internal Fraud (Robbery)	Kuwait Oil Tankers Company (Kuwait)	In March 1992, two of four former executives of the Kuwait Oil Tankers Company were accused of embezzling $100 million from the state-owned company in the 1980s and during the 1990-91 Gulf crisis (war).
External Fraud (Forgery)	Macquarie Bank Limited (Australia)	In June 2006, four people were charged over Macquarie Bank's loss of about $4.5 million in margin loans obtained from the bank by them on behalf of investors.
BDSF (Hardware Failure)	Sony Corporation (Japan)	In August 2006, Apple Computer and Dell Inc recalled a total of 5.9 million notebook-computer batteries made by Sony, which can overheat and cause fire hazard. The loss amount was estimated at $225 million.
BDSF (Software)	Anthem Inc (U.S.A.)	In November 2005, the state government of Kentucky ordered Anthem Inc to refund $23.7 million to customers who were overcharged for Medicare Supplement coverage as well as fining it $2 million. The company stated that the faulty numbers resulted from a computer processing error.
BDSF (Software)	National Australia Bank (Australia)	In November 2004, the National Australia Bank announced that it had written off AUD409 million in impaired software.

(*Continued*)

Table 5A2.1 (*Continued*)

Event Type	Company	Description of Event
BDSF (Software)	ING Groep NV (Netherlands)	In June 2005, the ING Groep NV announced that it would compensate some 500,000 customers who were provided with incorrect calculations for personal insurance policies at a cost of 65 million euros.
BDSF (Systems)	JPMorgan Chase & Co (U.S.A.)	In 1998, Chase Manhattan Bank identified inaccuracies in its bond recording system, but nothing was done about it until it merged with JP Morgan in 2000. As a result, the bank lost $46.8 million as the glitch in the system caused funds to be transferred to bondholders who were not entitled to them.
EDPM (Data entry or maintenance errors)	Universal Health Care Services Inc. (U.S.A.)	In August 2006, Universal Health Care Service Inc announced that a U.S. government glitch caused a hold up of members' promised refunds, thus costing the company $3 million.
EDPM (Failed reporting obligation)	Morgan Stanley (U.S.A.)	In September 2006, the National Association of Securities Dealers fined Morgan Stanley $2.9 million for a variety of trading and trade-reporting violations over the period 1999-2006.
EDPM (Inaccurate reporting)	Banesto (Spain)	In April 2001, a court case between Carlisle Ventures and Banesto was settled when the latter paid the former $13.5 million in compensation for false reporting. According to Carlisle, Banesto portrayed itself as being in a better financial position than it was in reality.
EDPM (system misoperation)	Royal Bank of Canada (Canada)	In December 2005, the Royal Bank of Canada announced that it would refund CAD25 million to customers who were paid simple rather than compound interest as a result of a calculation error.
EPWS (Discrimination)	FedEx Corporation (U.S.A.)	In June 2006, a court awarded two Lebanese-American drivers $61 million in damages for suffering from racial discrimination by their supervisor.
EPWS (Loss of staff)	Benfield Group (U.K.)	In October 2006, the Benfield Group (a reinsurance brokerage firm) declared that its results would be sharply worse than expected due to the departure of key staff members. The firm also declared that it would spend some GBP10 million to retain the remaining staff.
EPWS (Termination Issues)	Microsoft Corp. (U.S.A.)	In October 2005, Microsoft paid $97 million to settle a lawsuit to compensate workers who were employed and paid by temporary agencies while they worked for Microsoft for long periods.

(*Continued*)

Table 5A2.1 (*Continued*)

Event Type	Company	Description of Event
EPWS (Termination Issues)	Commertzbank (U.K.)	In November 2000, Commerzbank reached a GBP5 million settlement with the former chairman of a company that Commerzbank had acquired. He was dismissed over a dispute over the valuation of certain assets.
EPWS (Discrimination)	Merrill Lynch and Company (U.K.)	In July 2004, a former employee of Merrill Lynch received a GBP550,000 compensation from the employer following comments about her physique and sex life at a Christmas lunch.
DPA (Natural Disasters)	Murphy Oil Corporation (U.S.A.)	In August 2005, Hurricane Katrina resulted in a major leak in Murphy's oil refinery in Louisiana, spilling over 85,000 barrels of oil. The company had to pay $330 million in compensation to the residents of St Bernard Parish in New Orleans.
DPA (Natural Disasters)	Allianz AG (Germany)	In July 2002, Allianz AG declared losses of 550 million euros as a result of severe flooding in Europe that summer.
CPBP (Guideline Violation)	FleetBoston Financial Corporation (U.S.A.)	In October 2006, FleetBoston Financial Corporation agreed to pay $19.75 million for failure to prevent the collapse of Enron Corporation.
CPBP (Money Laundering)	Bank of America	In September 2006, Bank of America agreed to pay $7.5 million to settle a money-laundering case involving $3 billion from South America.
CPBP (Market Practices)	Deutsche Bank Group (U.S.A.)	In September 2006, Deutsche Asset Management, a U.S. arm of Deutsche Bank, agreed to pay $19.3 million in settlement after failure to disclose conflict of interest.

Table 5A2.2 A description of some operational loss events by business line

Business Line	Company	Description of Event
Corporate Finance	JPMorgan Chase & Co (U.S.A.)	In September 2006, the New York Stock Exchange fined JPMorgan Chase $400,000 for violation of short-selling rules.
Corporate Finance	General Electric Co. (U.S.A.)	In August 2006, General Electric paid Canatxx Energy Ventures $136.1 million in damages for breaching a contract pertaining to a joint industrial project.

(*Continued*)

Table 5A2.2 (*Continued*)

Business Line	Company	Description of Event
Corporate Finance	Canadian Imperial Bank of Commerce (U.S.A.)	In July 2006, the Canadian Imperial Bank of Commerce agreed to pay $16.5 million as its share of the settlement over a case involving the underwriting of securities prior to the bankruptcy of Global Crossing in January 2002.
Corporate Finance	Grand Tobidabo (Spain)	In 1994 the former president of Grand Tibidabo was arrested for misappropriating $1 billion pesetas from a government-guaranteed loan to the company received from Chase Manhattan Bank.
Commercial Banking	Bank Islam Malaysia (Malaysia)	In 2005, Bank Islam Malaysia recorded losses of 480 million ringgit due to higher provisions for nonperforming loans made on operations conducted by the bank's offshore unit in Labuan.
Commercial Banking	ABN Amro Bank (U.K.)	In March 1999, ABN Amro declared losses of $30 million due to fraud related to letters of credit.
Retail Banking	Wells Fargo & Co. (U.S.A.)	In October 2006, Wells Fargo & Co. reached a $12.8 million settlement in an overtime pay lawsuit with employees.
Retail Banking	Visa International (U.S.A.)	In July 2006, Visa agreed to pay $100 million as its share of a settlement regarding fees charged to cardholders for foreign currency denominated transactions.
Retail Banking	ANZ (New Zealand)	In March 2006, the ANZ pleaded guilty to 45 charges of breaching the new Zealand Fair Trading Act by failing to disclose fees charged for overseas currency transactions on its credit cards.
Payment and Settlement	Credit Lyonnais (Belgium)	In March 1997, a former employee of Credit Lyonnais Belgium was arrested for embezzling BEF3.5 billion from the bank's offices in Ghent.
Agency Services	Dresdner Bank (U.K.)	In July 2004, Dresdner Bank was told by a London court that it must repay EUR49.2 million to the Saudi Arabia Monetary Agency.