CHAPTER 7

Operational Risk

After reading this chapter you will be able to

- Understand the prevalence of operational risk
- Identify situations in which operational risk is likely to be an issue
- Evaluate opportunities to reduce operational risk

Operational exposures arise from the possibility of fraud, error, or system or procedural problems. Methods to manage operational risk include clear financial risk management policy, documentation of policies and procedures, adequate risk oversight, and segregation of duties. Employee compensation, education and training, holidays, and job rotation policies are also important. These issues are discussed in the following pages.

Financial risk management primarily deals with the risks that arise directly or indirectly as a result of financial markets. Analysis of previous significant losses suggests that losses often occur as a result of one or more major problems:

- Speculative trading
- Unauthorized trading
- Not hedging
- Overhedging

- Poor processes
- Inadequate division of duties
- Lack of oversight

Other contributors to risk include:

- Merger situations—risks may be hard to manage during implementation phase
- Risk across an organization, particularly if there are separate suborganizations

How Operational Risk Arises

Operational risk arises from the activities of an organization in three key areas: people, processes, and technology. Many large derivatives losses have been exacerbated by, or resulted from, operational failings that permitted losses to accumulate.

IN THE REAL WORLD

Risk and Oversight

"The risk management mechanism at the Daiwa Bank was not effectively functioning, and directors failed to meet their oversight responsibility."

Conclusions of a Japanese court in the largest shareholder lawsuit ever filed against individuals in Japan ordered Daiwa executives to pay $775 million in damages for failure to oversee a New York–based trader who engaged in unauthorized bond trading and hiding of $1.1 billion in losses.

Operational risk has traditionally been loosely defined and quantified. The ability to manage operational risk requires knowledge of processes, systems, and personnel and the ability to ensure that duties and procedures have been clearly established, documented, and followed. Many risks that an organization faces cross risk boundaries—for example, combining credit risk and operational risk.

Although operational risk is usually associated with treasury or trading operations, these risks and exposures also exist in other types of organizations. Operational losses do not always occur in organizations with large volumes or complex operations. The complexities of financial products, volatility of financial markets, combined with the operational intricacies of an organization, can produce risks that need to be managed carefully in all organizations.

For corporations, the decline in market value of the company as a result of an operational failure, such as might occur as a result of

IN THE REAL WORLD

Controlling Operational Risk

Although the business of financial institutions and nonfinancial institutions differs significantly, many of the operational risks they face are similar. In past interviews by the Bank for International Settlements of about 30 major banks, internal controls and the internal audit process were seen by virtually all as the primary means to control operational risk.

Source: Risk Management Subgroup of the Basel Committee on Banking Supervision, "Operational Risk Management," September 1998.

declines in a publicly traded company's share price, may be greater than the actual operational losses. The perception of operational weaknesses is particularly negative.

In some cases, operational risk may be partially offset by insurance designed to meet the needs of specific operational failures or breakdowns. It is presumed that insurance is an important part of any risk management strategy, though its discussion is beyond our scope. However, the discussion will focus on conditions within an organization that may reduce the likelihood of an operational issue, where possible.

TIPS & TECHNIQUES

Operational Controls

Some suggestions for implementing operational controls are:

- Involve management with oversight and adequate information.
- Implement appropriate policies and procedures, including limits, controls, and reporting requirements. These should be documented.
- Set up an independent risk management function to ensure that policies and limits are not violated and to provide oversight to management.
- Use internal audits to ensure activities are consistent with policies.
- Include an administrative or support function that can independently price and report on transactions, if no risk oversight function exists.

Error and Fraud

People are critical to the functioning of an organization, and from a risk management perspective, they often represent one of its most significant risks.

Transactions involve employee decisions and relationships. As a result, potential for error and fraud must always be guarded against. Due to the size and volume of treasury and finance transactions, the potential damage of a large error or fraud is serious. In addition, personnel may be subject to pressure to outperform or earn profits, which exacerbates the risk of a problem. The risk of errors or fraud as a result of one or more individuals falls into this arena.

In addition to fraud perpetrated within an organization, there is also the risk of fraud by those external to the organization. Although it is beyond the scope of this discussion, scams have involved fraudulent financial securities, financial institutions, and contractual agreements, among others.

Processes and Procedures

Processes and procedures help to ensure that an organization's polices are followed. Documentation of policies and procedures may reduce administrative time and provide tactical support to employees.

Risk arising from processes and procedures includes the risk of adverse consequences as the result of missing or ineffective processes, procedures, controls, or checks and balances. Often, these processes are designed to catch error or fraud. Process and procedural risk affects hedging and trading decisions, the oversight and risk control functions, how transactions are processed, and adherence to policies.

Technology and Systems

Technology and systems risks are operational risks that arise from financial instrument pricing and trading systems, reliance on technology,

IN THE REAL WORLD

Unauthorized Trading

One potentially significant result of operational exposure is unauthorized or excessive trading, and the potential resultant losses.

One leading Lloyds of London syndicate developed an *unauthorized trading* insurance policy for large financial institutions. The policy was designed to provide coverage in the event of losses from unauthorized, concealed, or false trading in excess of a predetermined limit, trading in unauthorized instruments, or trading with unauthorized counterparties.

payments systems, protection of data and networks, and access to files or data that can be fraudulently altered.

The existence of technology has eased many of the mundane functions associated with treasury, cash management, and trading, but it introduces new challenges with respect to risk management. To a certain extent, the degree of operational risk arising from technology depends on the processes conducted inhouse. A financial institution may have a very different set of technology and processes to support it than a municipal government, for example. However, there are some common areas of exposure.

Systems and networks should be evaluated in light of their vulnerability to sabotage, fraud, or error. A complex system that is understood by only one employee is a temptation to problems. The subject of risk in technology and systems security is relatively technical, and many aspects are best suited for discussion with an industry professional.

An organization using financial products should have the technological ability to analyze the risks inherent in those products and the

underlying exposure. If staff do not have access to appropriate technology, it will be difficult to manage the complexities of pricing and analysis of financial risk.

Operational Considerations

Operational risk encompasses people, processes, and technology, and its management requires consideration of operational issues. A few operational considerations may be useful:

- Maintain cash forecasts for various currencies and keep them current.
- Ensure employees have an opportunity for training and skills enhancement.
- Consider implementing job sharing or cross training to enhance team.
- Ensure adequate reporting to team, management, and board.
- Determine backups of both key data and employee roles.
- Maintain good relationships with financial institutions and other vendors.
- Ensure appropriate controls to guard against illegal activities, including money laundering.

Managing operational risk relies on the following tools:

- Contingent processing capability if the business relies on payment or other data processing
- Well-developed internal controls
- Use of internal audit
- Exception reporting for items that are missed, errors, or otherwise noteworthy

Different laws and regulations apply to different kinds of organizations around the world. Some of the following considerations may be addressed, or even restricted, by local laws and regulations, others not at all. This discussion is intentionally general in the sense that it presumes any operational issues will be undertaken within the more stringent laws and rules of either the local environment or the home country.

Internal Controls

Internal controls are perhaps the most important tools for managing operational risk. In fact, many large losses at banks can be attributed to internal control failures. The board of directors has final responsibility for ensuring that appropriate internal controls are implemented. Effectiveness of internal controls should periodically be tested and amended as necessary.

Appropriate division or segregation of duties among staff members is a key internal control. For example, confirmation should be separate from trading. Risk management reporting should be separate from trading. Separation may require an administrative or support function that can independently price and report on transactions when no formal risk oversight function exists. Other important control structures include approvals, reconciliations, and verifications.

One of an organization's greatest vulnerabilities comes from the potential for errors and fraud. If losses can be concealed, and an employee is tempted to do so because of pressure to generate profits or for other reasons, the organization is at tremendous risk, particularly since the largest losses are likely to be concealed with great effort.

The subject of internal control is complex and beyond the scope of this brief discussion. An adequate, effective audit program, monitoring, and a clear audit trail, in part derived from appropriate processes and reporting, is also critical. Liaison with professionals with audit, tax, and legal expertise is encouraged.

Compensation of Personnel

An organization that does not wish to speculate on financial market movements should not motivate its employees to speculate. However, even when employee compensation is based on something other than correct market forecasts, there may be subtle or implicit messages that accurate market forecasts are a definition of good performance. All managers should be able to identify opportunities to encourage the behavior that is warranted under the circumstances.

An appropriate compensation structure for finance personnel should suit the risk tolerance of the organization. Performance for bonuses should be considered carefully. Compensation is an important signal of performance expectations, particularly in the treasury department, where the process of mark-to-market is ongoing.

Finance personnel who are compensated with a profit-derived bonus are more likely to be motivated to take risks in pursuit of enhancement of the organization's (and their own) bottom line. Staff should know what is expected of them, and their compensation should reflect these expectations. An industrial company that does not wish to speculate in financial markets will want compensation based on something other than correct market bets.

Likelihood of fraud increases with employees in serious financial difficulty or with addictions such as gambling or drugs. Prospective employees should be screened carefully to the extent permissible by law to avoid potential problems.

Management Involvement

Management oversight and accountability is extremely important. Involvement of key management, as well as internal and external audit professionals, can also offer guidance in the area of controls. Management must have an appropriate level of knowledge about orga-

nizational risks to develop policies and acceptable strategies and monitor compliance.

In addition, deficiencies highlighted by audit or review should be corrected immediately, and feedback should ensure that problems have been corrected.

Conflicts of Interest

Management should be aware of the potential for conflicts of interest. If staff are influenced to transact business with certain institutions, these influences may have an impact on the independence of decisions made by staff. Although most finance professionals are familiar with issues of conflict, senior management should communicate exactly what is expected of treasury and finance personnel. This is especially true with respect to professional relationships with others in the business.

Both actual and perceived conflicts of interest should be considered. For example, employees have been encouraged to do business with a financial institution in exchange for preferential treatment for themselves or family members. This puts the organization's welfare in conflict with that of the employee and does not put the interests of stakeholders first. Some organizations prohibit personal transactions with dealers and financial institutions that do business with the organization to reduce potential for conflict.

Staff Training and Skills

Knowledgeable, well-rounded staff are an asset to any organization. Employees should be provided with opportunities for training and skills enhancement. This may require a dedicated training budget or allocation, as well as management support for training.

Employees should be encouraged to learn about other financial activities of the organization. Cross training is an opportunity to broaden

employee skills and enhance a team, facilitate succession planning, avoid reliance on one or two key individuals, and ensure that other employees can step in quickly in the event of a sudden departure. Employee rotation may also make it harder for employees to cover up inappropriate actions, thus potentially reducing the likelihood of fraud, intentional misinformation, or unauthorized transactions.

The hiring of financial personnel needs to be considered in the light of professional duties. Emphasis on specialization of finance personnel means that a financial manager has access to new, highly specialized personnel, but they need to fit into the organization's culture objectives, particularly with respect to risk management attitudes.

Financial Institution and Vendor Relationships

Maintenance of good relationships with financial institutions and other vendors is important. Good relationships with an appropriate number of financial institutions or dealers, with at least one backup, should be maintained. Overreliance on, or a majority of transactions with, one institution or individual representative should be questioned.

Relationship maintenance includes ensuring that correct documentation is provided when a new employee joins who is responsible for transactions. A list of authorized dealing personnel should be provided to counterparties on at least an annual basis and whenever a change occurs. Financial institutions should be informed in writing when key employees have left the organization. This helps to avoid opportunities for errors, embarrassment, or intentional misrepresentation.

Monitoring Exposures

An important operational activity is to monitor exposures. It is important to keep up to date with market or regulatory changes that might affect a currency's convertibility or liquidity, especially for emerging-market currencies.

In addition, maintain an understanding of counterparty issues and monitor counterparty viability, as well as agency ratings. Exposure to high-quality counterparties is preferable, though not a guarantee of loss prevention.

Organizations using exchange-traded contracts such as futures must ensure that margin can be administered by someone else, in the event of a margin call, if key personnel are unavailable.

Exposure assessment is discussed in more detail in Chapter 9.

Communication and Reporting

Appropriate and adequate reporting to team, management, and the board is important, as is a feedback loop that enables report recipients to ask questions and offer suggestions for improvement. Reporting should include both exposures and risk management activities.

Reporting and communications mechanisms should ensure that management and the board receives regular risk reports containing communication about risk exceptions, deviations from policy, reports about deficiencies, unusual losses, or anything else that would permit management and the board to better assess exposures and risk.

Reporting should be adequate to ensure adherence to risk management policies and limits and deviation from policy. Information should be available based on different criteria and detail, although this, in part, depends on the systems being used to produce the reports.

Forecasts and Reconciliations

Cash forecasts have a variety of purposes. First and foremost, they are used to manage an organization's liquidity and obligations. Forecasts and reconciliation of actual transactions to forecasted transactions also assist in the important identification of errors and certain fraudulent items.

From a risk management perspective, cash forecasts should be developed and maintained for the various currencies in which an organization has cash flows. A gap or mismatch between cash inflows and cash outflows for a particular currency provides information about gaps where funding is required or to assess foreign currency exposure. A forecast will assist in determining whether a gap is a timing issue or an exposure issue.

Not only does a cash forecast assist in highlighting areas of market exposure, but it also assists in liquidity management. Liquidity management ensures that an organization is adequately solvent to meet its immediate and short-term obligations. Reminder systems or other automated tools should be used to ensure that cashflows are properly anticipated and that key payment dates are met. Other date-sensitive issues, such as option expiry dates, should also be tracked closely.

Reconciliations should include analysis of brokerage fees or commissions that may provide clues about trading volumes or unauthorized trading.

Risk Oversight

Typically, treasury activities are overseen by one or more members of senior management, and ultimately, by the board of directors. The board should have a good understanding of the financial risks faced by the firm, provide leadership in the development of policies to measure and manage those risks, and ensure that management executes the plans quickly and effectively. The risk oversight function should be an independent function with reporting responsibility to top-level senior management and the board of directors, with a level of skills appropriate to the position. Issues of risk policy, including risk oversight, are discussed in Chapter 8.

Marking to Market

Marking to market involves repricing financial instruments, and sometimes the underlying exposures the instruments manage. It is an important risk management process. Large accumulated gains and losses should be monitored and assessed for potential follow-up action.

When marking to market, it is important to include all determinants of market value. For example, certain derivative products might be difficult to liquidate quickly, and a liquidity impact (premium or discount) may be appropriate. Nontraded transactions with a counterparty whose credit quality has declined substantially since the transaction was initiated might also require a pricing assessment of liquidity.

Marking to market should include the use of industry-standard pricing models. One reason for access to pricing models is to ensure that the organization is receiving competitive pricing on its transactions.

Pricing models should be documented and periodically evaluated against an external source, so that discrepancies between those used internally and those used by external market participants can be determined. It is also useful to check that internal mark-to-market prices would be comparable to those calculated using the documented pricing models. If pricing can be manipulated internally, it increases opportunity for loss.

Exchange-traded financial instruments can be valued using a real-time data vendor, since these instruments are standardized, and market prices for various contracts may be observed directly. Prices for actively traded money market and fixed income securities, and some over-the-counter derivatives, can also be found on several major data vendors.

Periodic pricing or mark-to-market should be undertaken by individuals other than the traders involved in the transactions, preferably from within the risk oversight or management function. This may require individuals other than those executing transactions to become

familiar with, and have access to, pricing software and real-time data. Prices should not be supplied by those responsible for undertaking the transactions (e.g., traders).

Policies

Management and board members require an understanding of risks for the development of policies. Stated policies on financial risk, exposures, and limits assist in the management of financial risk. Policies should include acceptable instruments and strategies. Limits should encompass the amount of exposure the firm has defined as acceptable risk and loss limits associated with it, and the limits on various types of transactions.

Policy issues include:

- Existence of policies
- Adherence to policies
- Periodic review of policies

Policies are developed by management, and significant policies are approved and reviewed by the board. Policies should be periodically reviewed for any necessary changes or updates. Management should be capable of ensuring adherence to risk management policy through oversight and reporting.

System Considerations

Operational risk arises from technology and systems. Managing this risk often involves control of access to networks and trading systems, particularly third-party systems that support both real-time data and transactions, control of access to locations where technology or networks can be accessed, and employee use of hard-to-break passwords and log-in/log-out rules. Data should be protected through onsite and offsite data backups, with availability of a remote location in the event of a physical evacuation.

The ability to conduct transactions from real-time vendor systems is a source of exposure. Often these systems are presumed by management to be interactive price retrieval data systems, but some permit messaging and trading. Therefore, they should not be accessible by disgruntled former employees or unauthorized individuals such as consultants, visitors, or other employees. Internal and external systems should support multiple access and authority levels. Some employees may be permitted to change or modify records, others can enter new records, and some employees can only read records. Reports should be protected against an employee modifying report parameters, such as those used for exception reports, through the use of report-writing tools. The integration of systems or software to manage cashflows, market risk, and credit risk is useful.

Spreadsheets are widely used in both financial and nonfinancial organizations, but reliance on them, combined with lack of controls, can create operational exposure. Significant losses have resulted from erroneous calculations contained in spreadsheets. Creating an inventory of spreadsheets and their uses, complexity, and potential for error or misuse may help to highlight areas of risk.

Systems should provide timeliness, accuracy, security and integrity, consistency, completeness, and relevance in the provision of data to the organization and its stakeholders. As technology is a fairly complex area, the guidance of professionals in this area is highly recommended.

Professional Assistance

Professional assistance on a variety of financial risk management topics is available from many sources. Financial institutions are able to discuss the characteristics of products and the strategies for using them. As vendors of such products, their intention is usually to match their customers' needs with appropriate hedging products. Since they sell products, their perspective is naturally biased toward those products.

TIPS & TECHNIQUES

Exchange Resources

Exchanges spend significant resources in the education of financial market participants, offering educational materials, courses, and seminars for market participants. Generally, these resources involve listed derivatives and how they are used for hedging or trading. Information specific to the contracts they offer, as well as primers on product mechanics and hedging, can be helpful in understanding the basics of a specific market.

Many consulting firms have practices in risk management, due mainly to strength gained in other areas such as in corporate finance. Consulting firms offer highly skilled professionals in a number of areas who are available on a contractual or project basis. These are most often reached through referrals from other professionals. It is important to ensure which professionals will be working on a particular project and whether the firm is also a provider or vendor of risk management products such as technology.

Risk management associations and organizations provide education, and in some cases certification, ranging from introductory to highly specific. Some of these organizations are listed in the Appendix.

A small number of independent firms manage functions such as currency and interest rate risk on behalf of clients. These overlay managers are compensated in the form of fees. Money managers also use outsourcing when there is insufficient staff expertise to manage specialized risks.

Special Issues in Managing Operational Risk

Trading and Leverage

Special risks exist in organizations where trading, with or without the use of leverage, is involved. Since trading organizations such as dealers and commercial banks use large numbers of dealers and capital, the risks are naturally greater for an operational failure. It is critical to manage these risks proactively.

Trading can be purely speculative, or it can be a form of trading that optimizes business flows. The nature of trading is similar to a continuum, with pure trading at one end and complete hedging at the other end. An organization's position on the continuum depends to a certain degree on the organizational view of risk versus return. These topics are discussed in more detail in Chapter 8.

IN THE REAL WORLD

Notable Quote

"Of the series of great derivatives disasters in the middle of the 1990s, only one, that of Metallgesellschaft (loss $1.5 billion), has been caused by the mishandling of bona fide hedging transactions.

"The others—Barings (loss £850 million), Orange County (loss $1.7 billion), and Sumitomo (loss $2.6 billion)—have been the result of unhedged and unauthorized speculation."

Source: Edward Chancellor, writing in *Devil Take the Hindmost* (New York: Plume Publishing, 1999), pp. 248–249. Copyright Edward Chancellor.

Merger and Acquisitions

Merger and acquisition situations present specific operational risks that need to be managed, not only during the often-lengthy transition phase but also after the transition is completed. The additional risks arise from the fact that it is more difficult to manage risk across an organization that might be geographically distant and involve various systems. In addition, different business cultures and practices may need to be taken into account, along with potentially different legal and regulatory environments.

Centralization

Many large multinational corporations and financial institutions have centralized trading, risk management, or treasury operations. These operations manage regional, or in some cases worldwide, exposures by netting hedging and liquidity requirements among members of the group.

Centralization has certain advantages, including the potential to reduce transaction costs associated with hedging. It may allow smaller group members access to skilled professionals in the operational center. However, the biggest consideration in centralization is risk, which arises through reduced control in key operational areas and through more reliance on reporting and quantitative measures. Strong operational controls and effective reporting become particularly important in centralized organizations.

Industry Recommendations

Group of 31: Core Principles

The Group of 31: Core Principles for Managing Multinational Financial Exchange Risk arose from a 1998 study of foreign exchange risk management multinational corporations sponsored by General Motors and

undertaken by Greenwich Treasury Advisors LLC.[i] The study surveyed 31 large multinational corporations with foreign exchange exposure arising from business activities—13 American, 2 Japanese, and 13 European companies with average sales of U.S.$50 billion. A follow-up study looked at the activities of an additional 33 U.S. multinational corporations with average sales of U.S.$11 billion.

Twelve core principles for managing foreign exchange exposure were used by a majority of firms. The core principles include fundamental principles, trading-volume-related principles, and principles related to risk-appetite.

Although they specifically reflect foreign exchange exposure management, the principles may also be helpful in the management of other financial risks.

Fundamental Principles

1. *Document foreign exchange policy*. Document a foreign exchange policy approved by senior management or the board of directors. Critical policy elements include hedging objectives, hedgeable exposures, hedging time horizon, authorized foreign exchange derivatives, the extent to which positions can be managed upon views of future foreign exchange rates, compensation for foreign exchange trader performance, and hedging performance measures.
2. *Hire well-qualified, experienced personnel*. Have a sufficient number of qualified, experienced personnel to properly execute the company's foreign exchange policy.
3. *Centralize foreign exchange trading and risk management*. Centralize the foreign exchange trading and risk management with the parent treasury, which may be assisted by foreign hedging centers reporting to parent treasury.

4. *Adopt uniform foreign exchange accounting procedures*. Require uniform foreign exchange accounting procedures, uniform exchange rates for book purposes, and multicurrency general ledgers for all foreign exchange transactions. Monthly, reconcile the parent treasury's foreign exchange hedging results to the group's consolidated generally accepted accounting principles (GAAP) foreign exchange results.

5. *Manage foreign exchange forecast error.* If anticipated foreign exchange exposures are being hedged, manage the forecast error and take steps to minimize it to the greatest extent possible.

6. *Measure hedging performance*. Use several performance measures to fully evaluate historic hedging effectiveness. Evaluate current hedging performance by frequently marking to market both the outstanding hedges and the underlying exposures.

Trading-Volume-Related Principles

7. *Segregate the back office function*. Segregate back office operations such as confirmations and settlements from trading. If trading volume is sufficient, use nostro accounts and net settle.

8. *Manage counterparty risk*. Have credit rating standards and evaluate counterparty risk at least quarterly. Measure credit exposure using market valuations, not notional amounts, against assigned counterparty credit limits. Use ISDA or other kinds of master agreements with at least major counterparties.

9. *Buy derivatives competitively*. Execute the foreign exchange policy by competitively buying foreign exchange derivatives with appropriate trading controls.

Risk-Appetite-Related Principles

10. *Use pricing models and systems*. Have in-house pricing models for all derivatives used. Use automated systems to track, manage, and value the derivatives traded and the underlying business exposures being hedged.

11. *Measure foreign exchange risk*. Understand the full nature of the foreign exchange risks being managed with a combination of risk measures such as value-at-risk, sensitivity analysis, and stress testing.

12. *Oversee treasury's risk management*. Independently oversee treasury's risk management with a risk committee to review and approve treasury's risk-taking activities and strategies, exposure and counterparty credit limits, and exceptions to corporate foreign exchange policy. Depending on the level of foreign exchange risks being managed, have either a part-time or a dedicated function to review treasury's compliance with approved risk management policies and procedures.

Group of 30 Recommendations[ii]

A seminal report by the *Group of 30* more than a decade ago addressed how both dealers and end-user organizations could better control the risks associated with the use of derivatives. It remains a classic set of fundamental risk management principles and may be useful to decision makers involved in risk management. The relevant recommendations of the Group of 30 are:

1. *The role of senior management*. Dealers and end users should use derivatives in a manner consistent with the overall risk management and capital policies approved by their boards of directors. These policies should be reviewed as business and market circumstances change. Policies governing derivatives use should be clearly

defined, including the purposes for which these transactions are to be undertaken. Senior management should approve procedures and controls to implement these policies, and management at all levels should enforce them.

2. *Marking to market*. Dealers should mark their derivatives positions to market, on at least a daily basis, for risk management purposes.

3. *Market valuation methods*. Derivatives portfolios of dealers should be valued based on mid-market levels less specific adjustments, or on appropriate bid or offer levels. Mid-market valuation adjustments should allow for expected future costs such as unearned credit spread, close-out costs, investing and funding costs, and administrative costs.

4. *Identifying revenue sources*. Dealers should measure the components of revenue regularly and in sufficient detail to understand the sources of risk.

5. *Measuring market risk*. Dealers should use a consistent measure to calculate daily the market risk of their derivatives positions and compare it to market risk limits.
   - Market risk is best measured as *value at risk* using probability analysis based on a common confidence interval (e.g., two standard deviations) and time horizon (e.g., a one-day exposure).
   - Components of market risk that should be considered across the term structure include absolute price or rate change (delta); convexity (gamma); volatility (vega); time decay (theta); basis or correlation; and discount rate (rho).

6. *Stress simulations*. Dealers should regularly perform simulations to determine how their portfolios would perform under stress conditions.

7. *Investing and funding forecasts*. Dealers should periodically forecast the cash investing and funding requirements arising from their derivatives portfolios.

8. *Independent market risk management*. Dealers should have a market risk management function, with clear independence and authority, to ensure that the following responsibilities are carried out:

- Development of risk limit policies and monitoring of transactions and positions for adherence to these policies (See recommendation 5.)
- Design of stress scenarios to measure the impact of market conditions, however improbable, that might cause market gaps, volatility swings, or disruptions of major relationships, or might reduce liquidity in the face of unfavorable market linkages, concentrated market making, or credit exhaustion (See recommendation 6.)
- Design of revenue reports quantifying the contribution of various risk components, and of market risk measures such as the value at risk (See recommendations 4 and 5.)
- Monitoring of variance between the actual volatility of portfolio value and that predicted by the measure of market risk
- Review and approval of pricing models and valuation systems used by front- and back-office personnel, and the development of reconciliation procedures if different systems are used

9. *Practices by end users*. As appropriate to the nature, size, and complexity of their derivatives activities, end users should adopt the same valuation and market risk management practices that are recommended for dealers. Specifically, they should consider regularly marking to market their derivatives transactions for risk manage-

ment purposes; periodically forecasting the cash investing and funding requirements arising from their derivatives transactions; and establishing a clearly independent and authoritative function to design and assure adherence to prudent risk limits.

10. *Measuring credit exposure*. Dealers and end users should measure credit exposure on derivatives in two ways:

- *Current exposure* is the replacement cost of derivatives transactions—that is, their market value.
- *Potential exposure* is an estimate of the future replacement cost of derivatives transactions. It should be calculated using probability analysis based on broad confidence intervals (e.g., two standard deviations) over the remaining terms of the transactions.

11. *Aggregating credit exposures*. Credit exposures on derivatives, and all other credit exposures to a counterparty, should be aggregated taking into consideration enforceable netting arrangements. Credit exposures should be calculated regularly and compared to credit limits.

12. *Independent credit risk management*. Dealers and end users should have a credit risk management function with clear independence and authority, and with analytical capabilities in derivatives, responsible for the following:

- Approving credit exposure measurement standards
- Setting credit limits and monitoring their use
- Reviewing credits and concentrations of credit risk
- Reviewing and monitoring risk reduction arrangements

13. *Master agreements*. Dealers and end users are encouraged to use one master agreement as widely as possible with each counterparty to document existing and future derivatives transactions, including

foreign exchange forwards and options. Master agreements should provide for payments netting and closes out netting, using a full two-way payments approach.

14. *Credit enhancement*. Dealers and end users should assess both the benefits and costs of credit enhancement and related risk-reduction arrangements. Where it is proposed that credit downgrades would trigger early termination or collateral requirements, participants should carefully consider their own capacity and that of their counterparties to meet the potentially substantial funding needs that might result.

15. *Promoting enforceability*. Dealers and end users should work together on a continuing basis to identify and recommend solutions for issues of legal enforceability, both within and across jurisdictions, as activities evolve and new types of transactions are developed.

16. *Professional expertise*. Dealers and end users must ensure that their derivatives activities are undertaken by professionals in sufficient number and with the appropriate experience, skill levels, and degrees of specialization. These professionals include specialists who transact and manage the risks involved, their supervisors, and those responsible for processing, reporting, controlling, and auditing the activities.

17. *Systems*. Dealers and end users must ensure that adequate systems for data capture, processing, settlement, and management reporting are in place so that derivatives transactions are conducted in an orderly and efficient manner in compliance with management policies. Dealers should have risk management systems that measure the risks incurred in their derivatives activities, including market and credit risks. End users should have risk management systems that measure the risks incurred in their derivatives activities based on their nature, size, and complexity.

18. *Authority*. Management of dealers and end users should designate who is authorized to commit their institutions to derivatives transactions.

19. *Accounting practices*. International harmonization of accounting standards for derivatives is desirable. Pending the adoption of harmonized standards, the following accounting policies are recommended:

- Dealers should account for derivatives transactions by marking them to market, taking changes in value to income each period.
- End users should account for derivatives used to manage risks so as to achieve a consistency of income recognition treatment between those instruments and the risks being managed. Thus, if the risk being managed is accounted for at cost (or, in the case of an anticipatory hedge, not yet recognized), changes in the value of a qualifying risk management instrument should be deferred until a gain or loss is recognized on the risk being managed. Or, if the risk being managed is marked to market with changes in value being taken to income, a qualifying risk management instrument should be treated in a comparable fashion.
- End users should account for derivatives not qualifying for risk management treatment on a mark-to-market basis.
- Amounts due to and from counterparties should only be offset when there is a legal right to set off or when enforceable netting arrangements are in place.

Where local regulations prevent adoption of these practices, disclosure along these lines is nevertheless recommended.

20. *Disclosures*. Financial statements of dealers and end users should contain sufficient information about their use of derivatives to provide an understanding of the purposes for which transactions are undertaken, the extent of the transactions, the degree of risk involved, and how the transactions have been accounted for. Pending the adoption of harmonized accounting standards, the following disclosures are recommended:

- Information about management's attitude to financial risks, how instruments are used, and how risks are monitored and controlled
- Accounting policies
- Analysis of positions at the balance sheet date
- Analysis of the credit risk inherent in those positions
- For dealers only, additional information about the extent of their activities in financial instruments

Summary

- Operational risk arises from the possibility of error, fraud, or a gap in procedures or systems. It is one of the most prevalent risks that organizations face.
- Operational risks are exacerbated in situations where additional risks exist, such as during mergers or acquisitions, trading environments, or geographically diverse organizations.
- Management of people, processes such as reporting and controls, and an assessment of the technological risks an organization faces may be useful in identifying and managing operational risk.

Notes

i *Group of 31: Core Principles for Managing Multinational Financial Exchange Risk,* The Group of 31/Greenwich Treasury Advisors LLC. Copyright 1999 by Greenwich Treasury Advisors LLC. Reproduced with permission.

ii *Group of 30 Global Derivatives Study Group; Derivatives: Practices and Principles,* Washington, DC, July 1993. Copyright protected. Reproduced with permission.