Risk Management Analytics

Operational Risk Modelling

Model risk

- Modeling is a critical component in the risk management of an organization. Models help quantify risk and other exposures as well as potential losses. However, models can be complex and are subject to **model risk**, which includes input errors, errors in assumptions, and errors in interpretation.

Model risk

- ***Model Complexity***

  When quantifying the risk of simple financial instruments such as stocks and bonds, model risk is less of a concern. These simple instruments exhibit less volatility in price and sensitivities relative to complex financial instruments so, therefore, their market values tend to be good indicators of asset values.

Model risk

- However, model risk is a significantly more important consideration when quantifying the risk exposures of complex financial instruments, including instruments with embedded options, exotic over-the-counter (OTC) derivatives, synthetic credit derivatives, and many structured products. For these complex instruments, markets are often illiquid and do not provide sufficient price discovery mechanisms, which puts greater emphasis on models to value instruments, typically through a mark-to-model valuation approach.

Model risk

- Losses from model errors can be due to errors in assumptions, carelessness, fraud, or intentional mistakes that undervalue risk or overvalue profit. The six common model errors are as follows:

  1. *Assuming constant volatility*. One of the most common errors in modeling is the assumption that the distribution of asset price and risk is constant. The 2007–2009 financial crisis showed just how incorrect this assumption can be, when market volatilities not predicted by models increased significantly over a short period of time.

Model risk

- 2. *Assuming a normal distribution of returns*. Market participants frequently make the simplifying assumption in their models that asset returns are normally distributed. Practice has shown, however, that returns typically do not follow a normal distribution, because distributions in fact have fat tails (i.e., unexpected large outliers)

Model risk

- *3. Underestimating the number of risk factors*. Many models assume a single risk factor. A single risk factor may produce accurate prices and hedge ratios for simple products such as a callable bond. For more complex products, including many exotic derivatives (e.g., Bermuda options), models need to incorporate multiple risk factors.

Model risk

- *4. Assuming perfect capital markets*. Models are generally derived with the assumption that capital markets behave perfectly. Consider a delta hedge strategy that requires active rebalancing based on the assumption that the underlying asset position is continuously adjusted in response to changes in the derivatives price. This strategy will not be effective if capital markets include imperfections, including limitations on short selling, various costs (e.g., fees and taxes), and a lack of continuous trading in the markets.

Model risk

- 5. *Assuming adequate liquidity*. Models often assume liquid markets for long or short trading of financial products at current prices. During periods of volatility, especially extreme volatility, as seen during the recent financial crisis, liquidity could decline or dry up completely.

Model risk

- 6. *Misapplying a model*. Historically, model assumptions have worked well in most world markets, but tend to break down during periods of greater uncertainty or volatility.
- For example, traditional models assuming normality did not work well in many countries, including the United States, Europe, and Japan in the post financial crisis period, which has been characterized by low or negative interest rates and unconventional monetary policies. In these markets, models that include other statistical tools work better

Model risk

The Modelers' Hippocratic Oath

- ~ I will remember that I didn't make the world, and it doesn't satisfy my equations.
- ~ Though I will use models boldly to estimate value, I will not be overly impressed by mathematics.
- ~ I will never sacrifice reality for elegance without explaining why I have done so.
- ~ Nor will I give the people who use my model false comfort about its accuracy. Instead, I will make explicit its assumptions and oversights.
- ~ I understand that my work may have enormous effects on society and the economy, many of them beyond my comprehension

Mitigating Model Risk

- Model risk can be mitigated either through investing in research to improve the model or through an independent vetting process. Investing in research leads to developing better and more accurate statistical tools, both internally and externally. Independent vetting includes the independent oversight of profit and loss calculations as well as the model selection and construction process.

Mitigating Model Risk

- Model Vetting consists of:

A) *Documentation*. Documentation should contain the assumptions of the underlying model and include the mathematical formulas used in the model. It should contain a term sheet to describe the transaction, a mathematical statement of the model (all the variables and processes, payoff function and pricing algorithms, calibrations, and hedge ratios and sensitivities), and the implementation features, including inputs, outputs, and any numerical methods.

Mitigating Model Risk

B) Model soundness. Vetting should ensure that the model used is appropriate for the financial instrument being valued. For example, a model valuing option-free bonds would not be appropriate to value convertible or callable bonds.

C) *Independent access to rates*. To facilitate independent parameter estimation, the model
vetter should ensure that the middle office has access to independent financial rates

D) *Benchmark selection*. The vetting process should include selecting the appropriate benchmark based on assumptions made. Results from the benchmark test should be compared with the results from the model test

Mitigating Model Risk

E) Health check and stress test. Models should be vetted to ensure they contain all necessary properties and parameters. Models should also be stress tested to determine the range of values for which the model provides accurate pricing.

F) *Incorporate model risk into the risk management framework*. Model risk should be considered in the formal risk management governance and framework of an institution. In addition, models need to be periodically reevaluated for relevance and accuracy. Empirical evidence suggests that simple, robust models work better than more complex and less robust models.

Operational Risk

- Operational risk has been receiving increasingly significant media attention, as financial scandals have appeared regularly. The trend toward greater dependence on technology, greater competition among banks, and globalization have left the banking industry more exposed to operational risk than ever before.

Operational Risk

- Buchelt and Unteregger (2004) argue that the risk of fraud and external events (such as natural disasters) have been around ever since the beginning of banking but it is technological progress that has boosted the potential of operational risk.

Operational Risk

- Likewise, Halperin (2001) argues that “operational risk has traditionally occupied a netherworld below market and credit risk” but “headline-grabbing financial fiascos, decentralized control, the surge in e-commerce and the emergence of new products and business lines have raised its profile”.

OpRisk in Financial Institutions

- Financial institutions (and firms in general) take on operational risk in running their daily business. The following are examples of common ways of taking operational risk:
  -The use of sophisticated techniques for mitigating credit risk and market risk such as collateralization.
  -The use of credit derivatives, and asset securitization.
  -Trading activities in increasingly complex products or those based upon complex arbitrage strategies lead to significant exposure to operational risk.
  -Any form of intermediation implies that those acting in the capacity of agents take operational risk instead of the mediated credit or market risks.

OpRisk in Financial Institutions

- Likewise, Mestchian (2003) attributes the growing level of interest in operational risk management to the following factors:

  1. Increasing complexity of financial assets and trading procedures, particularly the rapid growth of financial engineering and the resulting derivative products.
  2. Introduction of regulatory capital requirement by regulators.
  3. General acceptance by business leaders of the proposition that operational risk management procedures are still inadequate.
  4. The development of sophisticated statistical techniques that can be applied to the measurement of operational risk

Approaches for OpRisk

- • Top-down models: measure at the broadest level (using firm-wide or industry-wide data)
- • Bottom-up models: start at the individual business unit or process level then aggregate to determine the risk profile of the institution. Due the nature of operational risk it is often difficult to measure and quantify operational risk.

Diversity of OpRisk

- The diversity of the scope of operational risk is one feature that distinguishes it from the relatively narrowly defined market risk and credit risk, which are more widely understood and appreciated (by firms and regulators) as risk types.
- The diversity of operational risk (ranging from legal concerns to technological issues to behavioral matters to acts of God) makes it difficult to limit the number of dimensions required to describe it.

Diversity of OpRisk

- Operational risk encompasses the types of risk emanating from all areas of the firm: front office to the back office and support areas. Hence, identifying operational risk is more difficult than identifying market risk and credit risk. Buchelt and Untregger (2004) describe operational risk as "a highly varied and interrelated set of risks with different origins".
  - This feature of diversity, as compared with market risk and credit risk, gives rise to differences in determining what level of operational risk is acceptable (the so-called risk appetite).

Diversity of OpRisk

- In the case of market risk and credit risk, a wide range of methods can be used to determine the risk appetite, including risk concentrations and VAR-type calculations. At present, it is not possible to set up a formal structure of limits across operational risk because the calculation methodologies are still at an early stage of development while the lack of data means that the results are not sufficiently detailed.

Diversity of OpRisk?

- The tools (procedures, methodologies, and data collection) needed to determine the appetite for operational risk are less well developed than for credit risk and market risk. Actually, it will be some time before operational risk limits similar to those used in conjunction with credit and market risk can be derived and discussed with the same level of clarity. Operational risk is so complex in its causes, sources, and manifestations that it is impossible to agree on any sort of common understanding
  as to its limits.

One-sided Operation Risk?

- Some would argue that another distinguishing feature of operational risk is that it is “one-sided” in the sense that it is driven solely by its role as an undesired by-product of increasingly complex business operations. In this sense, the risk-return trade off associated with market risk has no equivalence in the case of operational risk, meaning that exposure to operational risk can cause losses without boosting the potential rate of return on capital and assets.

One-sided Operation Risk?

- In his critique of the Basel II Accord, Herring (2002) describes operational risk as being “downside risk”. Crouchy et al (2003) suggest a similar idea by expressing the view that “by assuming more operational risk, a bank does not expect to yield more on average” and that “operational risk usually destroys value for all claimholders”. This, they argue, is unlike market risk and credit risk because “by assuming more market or credit risk, a bank expects to yield a higher rate of return on its capital”.

One-sided Operation Risk?

- Likewise, Lewis and Lantsman (2005) argue that operational risk is one-sided because
  "there is a one-sided probability of loss or no loss".
  Alexander (2003b) distinguishes between operational risk, one the one hand, and market risk and credit risk, on the other, by arguing that operational risk is mostly on the cost side, whereas the revenue side is associated with market risk and/ or credit risk.

One-sided Operation Risk?

- But it is wrong to believe that operational risk is one-sided in this sense, because it is becoming the kind of risk that banks and other financial institutions (and firms in general) are taking deliberately for the sake of realizing potential return. If it were one-sided, then the objective of any firm would be to eliminate it completely, and this can be best done by closing down the business.

One-sided Operation Risk?

- Would anyone in his or her right mind suggest a drastic course of action like this? By taking on operational risk, firms earn income while being exposed to the risk of incurring operational losses if and when a loss event materializes. If this is not risk–return tradeoff, then what is?

One-sided Operation Risk?

- The fact of the matter is that operational risk can no longer be perceived as being solely associated with the cost of doing business. Instead, it has to be viewed as an integral part of the bundle of risks that are taken to generate profit.

Idiosyncratic OpRisk?

- A view that has been put forward repeatedly is that, unlike market risk and credit risk, operational risk is idiosyncratic in the sense that when it hits one firm, it does not spread to other firms, implying the absence of contagion or the absence of system-wide effects (that is, it is firm-specific, not systemic).

Idiosyncratic OpRisk?

- Lewis and Lantsman (2005) describe operational risk as being idiosyncratic because “the risk of loss tends to be uncorrelated with general market forces”. This is not a characteristic of market risk and credit risk: a market downturn affects all firms, and a default by the customers of one firm affects its ability to meet its obligations to other firms. But, like the argument that operational risk is one-sided, this argument is questionable.

Idiosyncratic OpRisk?

- If firm A suffers losses because of the activities of a rogue traders, this is not contagious only in the sense that firms B and C will not suffer direct losses from their own rogue traders. However, if firms B and C deal with firm A, then it is likely (depending on the size of loss) that firm A will fail to meet its obligations toward them. Hence, there is contagion and systemic effect here in the sense that firms B and C will incur (indirect) losses as a consequence of the rogue trading losses incurred by firm A.

Idiosyncratic OpRisk?

- In general, if firm A is subject to the operational risk of rogue trading, firms B and C will be subject to at least two kinds of risk: credit risk, resulting from the possible default of firm A on its obligations to firms B and C and settlement (liquidity) risk, which is a type of operational risk.

Idiosyncratic OpRisk?

- Thus, operational loss events are not contagious only in a very limited sense. The liquidation of a bank does not not lead to the liquidation of other banks, but it adversely affected them. Just like the counterargument that operational risk is not one-sided, the counterargument that it is not idiosyncratic seems to make some sense.

Unit of OpRisk?

- One major difference between operational risk, on the one hand, and market and credit risk, on the other, is the difficulty of defining a suitable "unit" of risk in the case of operational risk (McConnell, 2003). In the case of credit risk, the unit of risk is the entity or individual who could default.
- In the case of market risk, the unit of risk is an asset (bond, equity, currency, etc) whose adverse market price movements cause a loss. But in the case of operational risk, the unit of risk is an "operational process" whose failure causes a loss. The problem is that this unit varies across and within firms.

Unit of OpRisk?

- Yet another difference between operational risk, one the one hand, and credit risk and market risk, on the other, is that the concept of exposure is not clear in the case of operational risk. In the case of credit risk, for example, exposure is the amount lent to a customer. But in operational risk it is not straightforward

Definitions of OpRisk

- The definitions of operational risk range from the very narrow (regulatory approach) to the extremely broad classifications. Few issues divide the risk management community so completely as operational risk, but this does not alter the fact that the measurement of operational risk must start with a clear understanding of what is to be measured.

Definitions of OpRisk

1. Process risks, such as inefficiencies or ineffectiveness in the various business processes within the firm. These include value-driving processes, such as sales and marketing, product development and customer support, as well as value-supporting processes such as IT, HR, and operations.
2. People risks, such as employee error, employee misdeeds, employee unavailability, inadequate employee development, and recruitment.
3. Technology (or system) risks, such as the system failures caused by breakdown, data quality and integrity issues, inadequate capacity, and poor project management.

4. External risks, such as the risk of loss caused by the actions of external parties (for example, competitor behavior, external fraud, and regulatory changes) as well as macroeconomic and socioeconomic events.

5. The risk of loss resulting from errors in the processing of transactions/ breakdown in controls/errors or failures in system support

6. The risk run by a firm that its internal practices, policies, and systems are not rigorous or sophisticated enough to cope with untoward market conditions or human or technological errors

6. The risk that a firm will suffer loss as a result of human error or deficiencies in systems or controls

7. The risk that deficiencies in information systems or internal controls will result in unexpected loss.

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

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

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 (D9A)	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

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

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

- Operational risks must be proactively managed by a bank's board of directors and senior managers as well as its business line managers and employees. The 11 fundamental principles of operational risk management suggested by the Basel Committee are:

- 1. The maintenance of a **strong risk management culture** led by the bank's board of directors and senior managers. This means that both individual and corporate values and attitudes should support the bank's commitment to managing operational risks.

- 2. The operational risk framework (referred to as the “Framework” in this reading) must be **developed and fully integrated into the overall risk management processes** of the bank.

- 3. The board should **approve and periodically review** the Framework. The board should also oversee senior management to ensure that appropriate risk management decisions are implemented at all levels of the firm.

- 4.The board must identify the types and levels of operational risks the bank is willing to assume as well as approve **risk appetite and risk tolerance statements**.

- 5. Consistent with the bank's risk appetite and risk tolerance, senior management must **develop a well-defined governance structure** within the bank. The structure must be implemented and maintained throughout the bank's various lines of business, its processes, and its systems. The board of directors should approve this governance structure.

- 6. Senior management must **understand the risks, and the incentives related to those risks, inherent in the bank's business lines and processes**. These operational risks must be identified and assessed by managers.

- 7. New lines of business, products, processes, and systems should require an **approval process that assesses the potential operational risks**. Senior management must make certain this approval process is in place.
- 8. A **process for monitoring operational risks and material exposures to losses** should be put in place by senior management and supported by senior management, the board of directors and business line employees.

- 9. Banks must put strong **internal controls, risk mitigation, and risk transfer strategies** in place to manage operational risks.
  10. Banks must have plans in place to survive in the event of a major business disruption. **Business operations must be resilient**.
  11. Banks should make **disclosures** that are clear enough that outside stakeholders can assess the bank's approach to operational risk management.

Tools used to manage Operational Risk

1. Audit oversight
2. Critical self assessment (subjective evaluations using checklists, questionnaires, workshops etc)
3. Key risk indicators (objective measures e.g. early warning signs)
4. Earnings volatility after removing the effects of credit and market risks (assumes only remaining risk is op. risk)
5. Causal networks (describe how losses can occur given different causes)
6. Actuarial models (model the frequency and amount of losses due to op. risk)

Mitigating Operational Risk

Recall:

A risk manager must decide whether to:

- avoid (the risk) altogether
- reject the need for financial coverage, eg if risk is trivial
- retain, in part or fully
- transfer (insure or subcontract all the risk)
- share.

Ways of minimizing operational risk

- **Internal Control Methods** **External Control Methods**

1 Separation of functions Confirmations

2 Dual entries Verifications of Prices

3 Reconciliations Authorization

4 Tickler systems Settlement

5 Controls of amendments Internal/External Audits

Measuring Operational Risk

- Quantifying operational risk is a prerequisite for the formulation of an effective economic capital framework. Indeed, a model designed to measure operational risk should provide answers to some vital questions pertaining to
- (i) the most significant operational risks facing the firm;
- (ii) the impact of the most significant risks on the firm's financial statements;
- (iii) the worst the impact can be;
- (iv) the weight of the impact in stress situations;
- (v) how the impact is affected by changing the business strategy or control environment; and
- (iv) how the impact compares with the experience of similar firms.

General problems and conclusion

- In general, statistical/actuarial approaches to the measurement of operational risk create many challenges for the user, including the following:
  1. The size of internal loss data necessary to develop a risk profile for a business line or the whole firm.
  2. How to combine internal and external data, and should external data be scaled?
  3. How to fit loss data to a distribution, particularly when the data are not collected from a zero loss level (for practical reasons all loss data are collected above a threshold level, the choice of which can be rather subjective).

General problems and conclusion

- 4. How are loss frequencies estimated, particularly when data are collected from different sources over different time periods and with different threshold levels?
  5. How to conduct mathematical backtesting?
- Notwithstanding these (serious) problems (or perhaps because of them), major banks are actively indulging in (and spending a lot of money on) operational risk modeling. If for nothing else, they are required to do so by the regulators responsible for the implementation of the Basel II Accord

Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions

- Risk management is typically implemented via computer systems that help to automate gathering data, making computations, and generating reports. These systems can be made available commercially, and are typically used by smaller firms, while larger firms tend to use their own in-house systems, often in combination with commercial models. The implementation process for computing risk is usually referred to as the firm's *VaR model*, although the general computation process can apply to any risk measure other than VaR

Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions

- Data preparation is crucial in risk measurement systems. There are three types of data involved:
  1. *Market data* is time series data (usually asset prices) that is used in forecasting the distribution of future portfolio returns. Market data involves obtaining the time series data, removing erroneous data points, and establishing processes for missing data. All of these steps can be costly but necessary.
  2. *Security master data* is descriptive data on securities, including maturity dates, currency, and number of units. Building and maintaining data for certain securities, including equities and debt, can be challenging; however, it is critical from a credit risk management perspective.
  3. *Position data* matches the firm's books and records but presents challenges as data must be collected from a variety of trading systems and across different locations.

Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions

- Once the data is collected, software is used to compute the risk measures using specific formulas, which are then combined with the data. Results are then published in documents for reporting by managers. All of these steps can be performed in numerous ways and can lead to several issues within the risk measurement system. We focus on two of these issues: the variability of the resulting measures and the appropriate use of data.

  Variability in risk measures, including VaR, is both a benefit and a problem. Managers have significant discretion and flexibility in computing VaR, and parameters can be freely used in many different ways. This freedom in measuring VaR leads to two significant problems in practice:

Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions

- *1. Lack of standardization of VaR parameters*. Given the variability in VaR measurements and managers' discretion, parameters including confidence intervals and time horizons can vary considerably, leading to different measurements of VaR.
  2. *Differences in VaR measurements*. Even if VaR parameters were standardized, differences in measuring VaR could lead to different results. These include differences in the length of the time series used, techniques for estimating moments, mapping

Explain how model risk and variability can arise through the implementation of VaR models and the mapping of risk factors to portfolio positions

- techniques (discussed in the next section) and the choice of risk factors, decay factors in using exponentially weighted moving average (EWMA) calculations, and the number of simulations in Monte Carlo analysis. Varying parameters can lead to materially different VaR results. For example, one study using different combinations of parameters, all within standard practice, of portfolios consisting of Treasury bonds and S&P 500 index options indicated that VaR results differed considerably by a factor of six or seven times. A simple read of the different VaR models published in the annual reports of some of the larger banks can give an indication of the variability in their measurements.