Enterprise / Operational

Risk Management

Jeffrey Lee Cowherd IT Audit Manager City National Bank
Daniel P. Manson California State Polytechnic University, Pomona

Enterprise risk management (ERM) is a relatively new discipline that focuses on identifying, analyzing, monitoring, and controlling all major risk classes (e.g., credit, market, liquidity, operational risk classes). Operational risk management (ORM) is a subset of ERM that focuses on identifying, analyzing, monitoring, and controlling operational risk. The purpose of this paper is to explain what enterprise risk management is and how operational risk management fits into the ERM framework. In our conclusion, we discuss what is likely to happen in the ERM / ORM environment over the next 5 years.

Introduction

As the Internet has come of age, companies have been rethinking their business models, core strategies, and target customer bases. "Getting wired," provides businesses with new opportunities, but brings new risks and uncertainty into the equation.

Mismanagement of risk can carry an enormous cost. In recent years, business has experienced numerous, related risk reversals that have resulted in considerable financial loss, decrease in shareholder value, damage to company reputations, dismissals of senior management, and, in some cases, the very dissolution of the business. This increasingly risky environment, in which risk mismanagement can have dire consequences, mandates that management adopt a new more proactive perspective on risk management.

What is Enterprise / Operational Risk Management?

Clearly, there is a correlation between effective risk management and a well-managed business. Over time, a business that cannot manage risk effectively will not prosper and, perhaps fail. A disastrous product recall could be the company's last. Rogue traders lacking oversight and adequate controls have destroyed old well-established institutions in a very short time. But, historically, risk management in even the most successful businesses has tended to be in "silos"—the insurance risk, the technology risk, the financial risk, the environmental risk, all managed independently in separate compartments. Coordination of risk management has usually been non-existent, and identification of emerging risks has been sluggish.

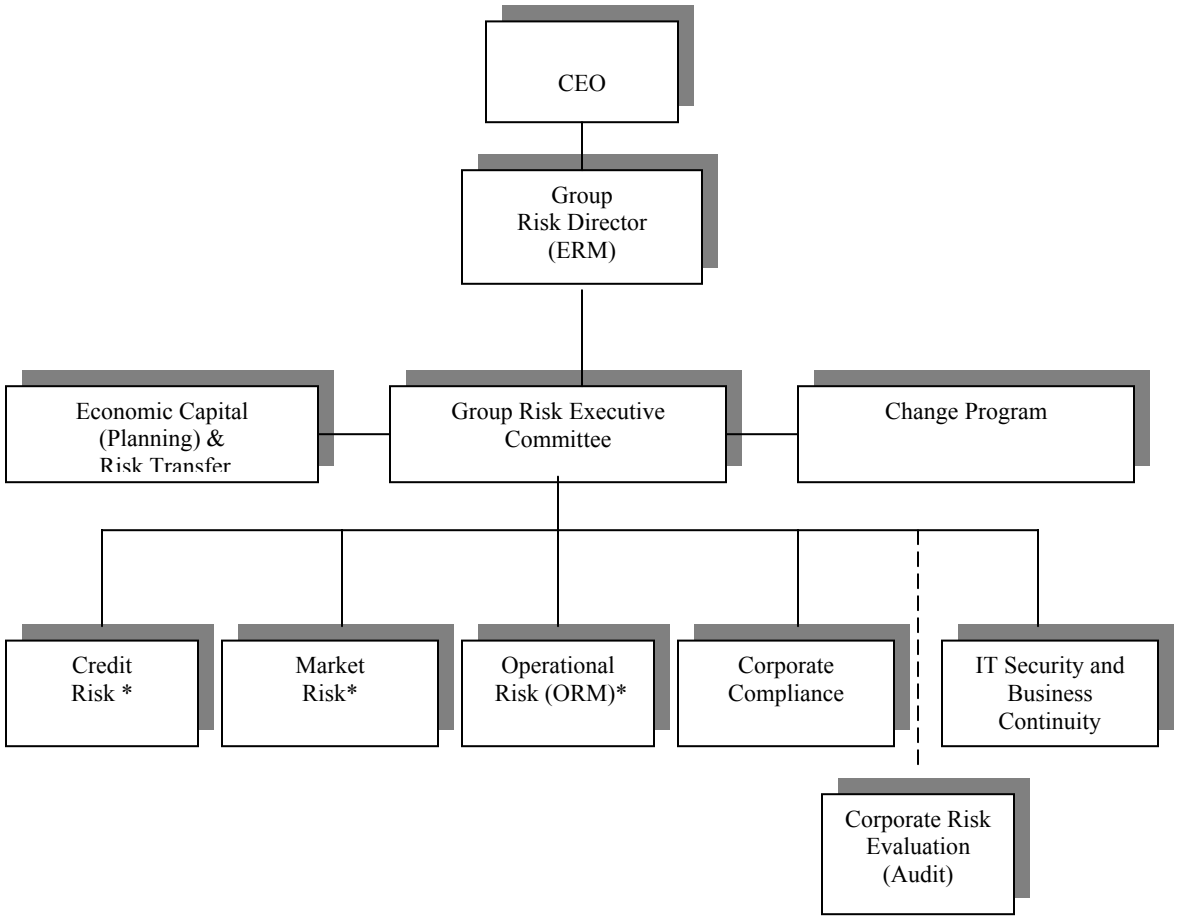
This paper espouses a recent concept—enterprise-wide risk management—in which the management of risks is integrated and coordinated across the entire organization. A culture of risk awareness is created. Companies across a wide cross-section of industries are beginning to implement this effective new methodology.

Enterprise / Operational Risk Management

At first glimpse, there is much similarity between operational risk management and other classes of risk (e.g., credit, market, liquidity risk, etc.) and the tools and techniques applied to them. In fact, the principles applied are nearly identical. Both ORM and ERM must identify, measure, mitigate and monitor risk. However, at a more detailed level, there are numerous differences, ranging from the risk classes themselves to the skills needed to work with operational risk.

Operational risk management is just beginning to define the next phase of evolution of corporate risk management. Should firms be able to develop successful ORM programs, the next step will be for these firms to integrate ORM with all other classes of risks into truly enterprise-wide risk management frameworks. See Exhibit 1 for an example of an ERM / ORM organizational structure representative of the banking industry:

ERM Organization Chart



- Note – the major categories of risk to which financial services firms expose themselves are credit risk, market risk and operational risk. Not surprisingly, financial services firms' largest risk concentrations—credit risk and market risk are most effectively managed.

Exhibit 1

Why Enterprise / Operational Risk Management?

There are many reasons ERM / ORM functions are being established within corporations. The following are a few of the reasons these functions are being established.

Organizational Oversight

Two groups have recently emphasized the importance of risk management at the organization's highest levels. In October 1999, the National Association of Corporate Directors released its *Report of the Blue Ribbon Commission on Audit Committees,* which recommends that audit committees "define and use timely, focused information that is responsive to important performance measures and to the key risks they oversee." The report states that the chair of the audit committee should develop an agenda that includes "a periodic review of risk by each significant business unit."

In January 2000, the Financial Executives Institute released the results of a survey on audit committee effectiveness. Respondents, primarily chief financial officers and corporate controllers, ranked "key areas of business and financial risk" as most important for audit committee oversight.

In light of events surrounding recent corporate scandals (e.g., Enron, etc.), and the increasing executive and regulatory focus on risk management, the percentage of companies with formal ERM methods is increasing and audit committees are becoming more involved in corporate oversight. The UK and Canada have set forth specific legal requirements for audit committee oversight of risk evaluation, mitigation, and management which are widely accepted as best practices in the U.S.

Magnitude of Problem

The magnitude of loss and impact of operational risk and losses to date is difficult to ignore. Based on years of industry loss record-keeping from public sources, large operational risk-related financial services losses have averaged well in excess of $15 billion annually for the past 20 years, but this only reflects the large public and visible losses. Research has yielded nearly 100 individual relevant losses greater than $500 million each, and over 300 individual losses greater than $100 million each.[1] Exhibit 2 is a listing of major operational losses. Interestingly enough, the majority of these losses have occurred in financial services, which explains the industry's leading focus on operational risk management especially in the area of asset-liability modeling and treasury management models to manage risks in the highly volatile capital markets activity of derivative trading and speculation.

---

[1] Hoffman, Douglas G., Managing Operational Risk (New York: John Wiley & Sons, 2002), p. xxvi.

Top Operational Risk Losses

Company	Loss Amount	Date	Description
Numerous Financial Institutions and Others	$20 million. Initial Estimates	2001	Terrorists hijacked four commercial airliners and crashed them into the World Trade Center. Over 2000 lives lost. Countless businesses impacted.
BCCI	$17 billion	1991	Regulators seized about 75 percent of The Bank of Credit and Commerce International's $17 billion in assets in a major fraud.
Sumitomo Corporation	$2.9 billion	1996	Sumitomo Corporation incurred huge losses through excessive trading of copper.
Tokyo Shinkin Bank	$2.3 billion	1990-1991	The manager of the Imasato branch forged 19 deposit certificates, which were used to raise money for stock deals.
Banca Nazionale del Lavoro	$1.8 billion	1992	Former employees plead guilty to conspiring to arrange $5 billion in unauthorized loans to Iraq.
Daiwa Bank	$1.1 billion	1983-1995	Loss due to unauthorized trading by an employee.
Barings	$1 billion	1995	This catastrophic loss has become a benchmark for operational risk. Losses due to lack of dual control and checks and balances.
Non-Financial Institutions: LTCM	$4 billion	1998	Huge market losses due to inadequate model management and inadequate controls at Long Term Capital Management.
Texaco, Inc.	$3 billion	1984	Pennzoil sued Texaco alleging that Texaco "wrongfully interfered" in its merger deal with Getty.
Cendant Corporation	$2.9 billion	1985-1998	Largest and longest-running accounting fraud in history. Former executives conspired to inflate earnings.
Dow Corning	$2 billion	1994	The company agreed to pay settlements to 18 women who indicated breast implants made them ill.
St. Francis Assisi Foundation	$2 billion	1999	Insurance fraud case in which Martin Frankel allegedly stole as much as $2 billion from this foundation.
Mettlgesellschaft	$1.8 billion	1991-1993	Loss due to liquidation of oil supply contracts.
Owens Corning Fiber Glass	$1.7 billion	1980s-1990s	Settlement of asbestos-related claims.
Orange County	$1.6 billion	1994	Largest people risk class case in financial history. Largest investment loss ever registered by a municipality.
Atlantic Richfield	$1.5 billion	1986-1990	Settlement of North Slope oil royalties dispute with Alaska.
Kashima Oil	$1.5 billion	1994	Disguised losses on FX forward contracts.
Showa Shell	$1.5 billion	1989-1993	Major oil refiner in Japan faced losses from forward currency contracts.
Prudential Securities	$1.4 billion	1994	Settled charges of securities fraud with state and federal regulators.
Drexel Burnham Lambert	$1.3 billion	1998-1993	Former employees filed a class action suit charging the company with fraud, breach of duty and negligence.
General Motors	$1.2 billion	1996	Heavy losses suffered due to 3 strikes.
Phar Mor	$1.1 billion	1992	A former president of the firm defrauded in an embezzlement scheme.

Exhibit 2
Source: Hoffman; Managing Operational Risk

Increasing Business Risks

With the increasing speed of change for all companies in this new era, senior management must deal with many complex risks that have substantial consequences for the organization. A few forces currently creating uncertainty are:

- Technology and the Internet
- Increased worldwide competition
- Free trade and investment worldwide
- Complex financial instruments
- Deregulation of key industries
- Changes in organizational structures from downsizing, reengineering, and mergers
- Increasing customer expectations for products and services
- More and larger mergers

Collectively, these forces are stimulating considerable change and creating an increasing risk in the business environment.

Regulatory

The international regulators clearly intend to encourage banks to develop their own proprietary risk measurement models to assess regulatory, as well as economic, capital. The advantage for banks should be a substantial reduction in regulatory capital, and a more accurate allocation of capital vis-à-vis the actual risk confronted.

In December 2001, the Basel Committee on Banking Supervision submitted a paper *"Sound Practices for the Management and Supervision of Operational Risk"* for comment by the banking industry. In developing these sound practices the Committee recommended that banks have risk management systems in place to identify, measure, monitor and control operational risks. While the guidance in this paper is intended to apply to internationally active banks, plans are to eventually apply this guidance to those banks deemed significant on the basis of size, complexity, or systemic importance and to smaller, less complex banks. Regulators will eventually conduct regular independent evaluations of a bank's strategies, policies, procedures and practices addressing operational risks. The paper indicates an independent evaluation of operational risk will incorporate a review of the following six bank areas:[2]

- Process for assessing overall capital adequacy for operational risk in relation to its risk profile and its internal capital targets;

- Risk management process and overall control environment effectiveness with respect to operational risk exposures;

[2] Basel Committee on Banking Supervision, Sound Practices for the Management and Supervision of Operational Risk, (Basel, Switzerland: Basel Committee on Banking Supervision, 2001), p. 11.

- Systems for monitoring and reporting operational risk exposures and other data quality considerations;
- Procedures for timely and effective resolution of operational risk exposures and events;
- Process of internal controls, reviews and audit to ensure integrity of the overall risk management process; and
- Effectiveness of operational risk mitigation efforts.

Market Factors

Market factors also play an important role in motivating organizations to consider ERM / ORM. Comprehensive shareholder value management and ERM / ORM are very much linked. Today's financial markets place substantial premiums for consistently meeting earnings expectations. Not meeting expectations can result in severe and rapid decline in shareholder value. Research conducted by Tillinghast-Towers Perrin found that with *all else being equal*, organizations that achieved more consistent earnings than their peers were rewarded with materially higher market valuations.[3] Therefore, for corporate executives, managing key risks to earnings is an important element of shareholder value management. The traditional view of risk management has often focused on property and liability related issues or internal controls. However, "traditional" risk events such as lawsuits and natural disasters may have little or no impact on destroying shareholder value compared to other strategic and operational exposures—such as customer demand shortfall, competitive pressures, and cost overruns. One explanation for this is that traditional risk hazards are relatively well understood and managed today—not that they don't matter. Managers now have the opportunity to apply tools and techniques for traditional risks to all risks that affect the strategic and financial objectives of the organization.

For non-publicly traded organizations, ERM / ORM is valuable for many of the same reasons. Rather than from the perspective of shareholder value, ERM / ORM would provide managers with a comprehensive overview of other important items such as cash flow risks or stakeholder risks. Regardless of the organizational form, ERM / ORM can be an important management tool.

Corporate Governance

Defense against operational risk and losses flows from the highest level of the organization—the board of directors and executive management. The board, the management team that they hire, and the policies that they develop, all set the tone for a company. As guardians of shareholder value, boards of directors must be acutely attuned to market reaction to negative news. In fact, they can find themselves castigated by the public if the reaction is severe enough. As representatives of the shareholders, boards of directors are responsible for policy

---

[3] Tillinghast-Towers Perrin, Enterprise Risk Management: Trends and Emerging Practices. (The Institute of Internal Auditors Research Foundation, 2001), p. xxvi.

matters relative to corporate governance, including but not limited to setting the stage for the framework and foundation for enterprise risk management.

Right now, operational risk management is a "hot topic" of discussion for regulators and in boardrooms across the US. In the wake of the 2001 releases from the Basel Risk Management Committee, banks now have further insight as to the regulatory position on the need for regulatory capital for operational risk. Meanwhile, shareholders are aware that there are means to identify, measure, manage, and mitigate operational risk that add up to billions of dollars every year and include frequent, low-level losses and also infrequent but catastrophic losses that have actually wiped out firms, such as Barings, and others. Regulators and shareholders have already signaled that they will hold directors and executives accountable for managing operational risk.

Best-Practice

Senior managers need to encourage the development of integrated systems that aggregate various market, credit, liquidity, operational and other risks generated by business units in a consistent framework across the institution. Consistency may become a necessary condition to regulatory approval of internal risk management models. An environment where each business unit calculates their risk separately with different rules will not provide a meaningful oversight of firm-wide risk. The increasing complexity of products, linkages between markets, and potential benefits offered by overall portfolio effects are pushing organizations toward standardizing and integrating risk management.

Conclusion

It seems clear that ERM / ORM is more than another management fad or academic theory. We believe that ERM / ORM will become part of the management process for organizations in the future. Had ERM / ORM processes been in place during the past two decades, a number of the operational risk debacles that took place may not have occurred or would have been of lesser magnitude.

Companies are beginning to see the benefit of protecting themselves from all types of potential risk exposures. By identifying and mapping risk exposures throughout the organization, a company can concentrate on mitigating those exposures that can do the most damage. With an understanding of risks, their severity, and their frequency, a company can turn to solutions; be it retaining, transferring, sharing, or avoiding a particular risk.

Our thoughts on what will happen in the ERM / ORM environment in the next 5 years are:

In the next 5 years, it is likely that companies will no longer view risk management as a specialized and isolated activity: the management of insurance or foreign exchange risks, for instance. The new approach will

keep managers and employees at all levels sensitized to and concerned about risk management. Risk management will be coordinated with senior management oversight and everyone in the organization will view risk management as part of his or her job. The risk management process will be continuous and broadly focused. All business risks and opportunities will be covered.

In the next 5 years, the use of bottom-up risk assessments will be a standard process used to identify risks throughout the organization. The self-assessment process will involve everyone in the company and require individual units to focus and report on the threats to their individual business objectives. Through the self-assessment process, the organization will be able to understand loss potential and risk control by business, by profit center and by product. The individual line manager will begin to understand the loss potential in his or her own processing system.

In the next 5 years, the use of top-down scenario analysis will be another standard method used to identify risks throughout the organization. Top down scenario analysis will determine the risk potential for the entire firm, the entire business, organization, or portfolio of business. By its very nature, it is a high-level representation and cannot get into the bottom-up transaction-by-transaction risk analysis.

For example, because Microsoft has a campus of more than 50 buildings in the Seattle area, earthquakes are a risk.[4] In the past, Microsoft looked at silos of risk. For example, they would have looked at property insurance when they considered the risks of an earthquake and thought about protecting equipment and buildings. However, using scenario analysis they are now taking a more holistic perspective in considering the risk of an earthquake.

The Microsoft risk management group has analyzed this disaster scenario with its advisors and has attempted to quantify its real cost, taking into account how risks are correlated. In the process, the group identified risks in addition to property damage, such as the following:

- Director and officer liability if some people think management was not properly prepared.
- Key personnel risk
- Capital market risk because of the firm's inability to trade.
- Worker compensation or employee benefit risk.
- Supplier risk for those in the area of the earthquake.
- Risk related to loss of market share because the business is interrupted.

---

[4] Michel Crouhy, Dan Galai, and Robert Mark, Making Enterprise Risk Management Payoff (New York: McGraw-Hill, 2001), pp 132-133.

- Research and development risks because those activities are interrupted and product delays occur.
- Product support risks because the company cannot respond to customer inquiries.

By using scenario analysis, management has identified a number of risks that it might not have otherwise and Microsoft is now in a better position to manage these risks. The future ERM / ORM tools such as risk assessment and scenario analysis will assist companies in identifying and mitigating the majority of these risks.

In the next 5 years, companies will be using internal and external loss databases to capture occurrences that may cause losses to the company and the actual losses themselves. This data will be used in quantitative models that will project the potential losses from the various risk exposures. This data will be used to manage the amount of risk a company may be willing to take.

In the next 5 years, companies will allocate capital to individual business units based on operational risk. By linking operational risk capital charges to the sources of that risk, individuals with risk optimizing behavior will be rewarded and those without proper risk practices will be penalized.

In the next 5 years, internal audit will become even more focused on how risks are managed and controlled throughout the company on a continuous basis. Internal audit will be responsible for reporting on integrity, accuracy, and reasonableness of the company's entire risk management process. In addition, Internal Audit will be involved in ensuring the appropriateness of the company's capital assessment and allocation processes. Furthermore, audit will influence continual improvement of risk management and controls through the sharing of best practices.

In the next 5 years, management will be looking for individuals who are skilled in risk management. Professional designations such as the Bank Administration Institute's Certified Risk Professional (CRP) and the Information and Audit and Control Association's Certified Information Security Manager (CISM) will demonstrate proficiency in the risk management area and will be in demand.

In the next 5 years, external auditors will be required to report on the efficiency and effectiveness of a company’s risk management program. These companies will be required to disclose the scope and nature of risk reporting and/or measurement systems in their annual reports.

Overall, companies will be better positioned in the next 5 years to deal with the broad scope of enterprise-wide risks. By implementing the ERM / ORM process now, companies will begin to maximize their overall risk profile for competitive advantage.

Bibliography

Barton, Thomas L.; Shenkir, William G.; Walker, Paul L. Making Enterprise Risk Management Pay Off. New Jersey: Financial Times / Prentice Hall, 2002.

"Basel II Mandates a Nest Egg for Banks" US Banker. (July 1, 2002) 48. July 2002. http://web2.infotrac.galegroup.co

BITS. BITS Technology Risk Transfer Gap Analysis Tool. Washington, D.C.: BITS, 2002.

Bock, Jerome T., The Strategic Role of "Economic Capital" in Bank Management, Wimbledon, London: Midas-Kapiti International, 2000.

Business Banking Board. RAROC and Operating Risk. Washington, D.C.: Corporate Executive Board, 2001.

Business Banking Board. Risk Management Structure. Washington, D.C.: Corporate Executive Board, 2001.

Consultative Document Operational Risk. 2001. Bank for International Settlements and Basel Committee on Banking Supervision. July 2002. http://www.bis.org/publ/bcbsa07.pdf

Crouhy, Michel; Galai, Dan; Mark, Robert, Risk Management. New York: McGraw-Hill, 2001.

"Elements of a Successful IT Risk Management Program". Gartner. (May 2002.) 9. July 2002. http://www.gartner.com/gc/webletter/bindview/issue1/ggarticle1.html

Ernst & Young, Integrated Risk Management Practices. Unpublished PowerPoint slides, Ernst & Young: 2000.

Hively, Kevin; Merkley, Brian W.; Miccolis, Jerry A. Enterprise Risk Management: Trends and Emerging Practices. Florida: The Institute of Internal Auditors Foundation, 2001.

Hoffman, Douglas G. Managing Operational Risk. New York: John Wiley & Sons, Inc., 2002.

"In Brief: Ferguson Urges Investing in Risk Control". American Banker. (March 5, 2002) 1. July 2002. http://0proquest.umi.com.opac.library.csupomona.edu

James, Christopher, RAROC Based Capital Budgeting and Performance Evaluation: A Case Study of Bank Capital Allocation. Pennsylvania: The Wharton School, 1996.

Jameson, Rob; Walsh, John, "The Leading Contenders," Risk Magazine, (November 2000). 6. July 2002. http://www.financewise.com/public/edit/riskm/oprisk/opr-soft00.htm

Insurance Industry - Participating companies: Allianz, AXA, Chubb, Mitsui Sumitomo, Munich Re, Swiss Re, Tokio Marine and Fire, Xl, Yasuda Fire and Marine and Zurich. Insurance of Operational Risk Under the New Basel Accord. Insurance Industry, 2001.

Lam, James, "Top Ten Requirements for Operational Risk Management" Risk Management (November 2001) July 2002. http://0-proquest.umi.com.opac.library.csupomona.edu

Marks, Norman, "The New Age of Internal Auditing" The Internal Auditor (December 2001) 5. July 2002. http://0-proquest.umi.com.opac.library.csupomona.ed

McNamee, David; Selim, George M. Risk Management: Changing the Internal Auditor's Paradigm. Florida: The Institute of Internal Auditors Research Foundation, 1998.

National Association of Financial Services Auditors. "Enterprise Risk Management," National Association of Financial Services Auditors. Spring 2002. 12-13.

netForensics is a Web site that discusses those regulations that govern information security in financial services, healthcare and government. http://www.netforensics.com/verticals.html

Ong, Michael; "Why bother?" Risk Magazine, (November 2000). 6. July 2002.
http://www.financewise.com/public/edit/riskm/oprisk/oprcommentary00.htm

Practice Advisory 2100-3: Internal Audit's Role in the Risk Management Process. March 2001. The Institute of Internal Auditors. July 2002.
http://www.theiia.org/ecm/guide-frame.cfm?doc_id=73

Santomero, Anthony M., Commercial Bank Risk Management: an Analysis of the Process. Pennsylvania: The Wharton School, 1997.

Sound Practices for the Management and Supervision of Operational Risk. 2002. Bank for International Settlements and Basel Committee on Banking Supervision. July 2002. http://www.bis.org/publ/bcbs86.htm

The Financial Services Roundtable, Guiding Principles in Risk Management for U.S. Commercial Banks. Washington D.C.: The Financial Services Roundtable, 1999.

Verschoor, Curtis C. Audit Committee Briefing – 2001: Facilitating New Audit Committee Responsibilities. Florida: The Institute of Internal Auditors, 2001.

Working Paper on the Regulatory Treatment of Operational Risk. 2001. Bank for International Settlements and Basel Committee on Banking Supervision. July 2002. http://www.bis.org/publ/bcbs_wp8.pdf