Section One

Achieving and Maintaining Business Continuity: an executive overview

1 Enterprise Risk Management

Andrew Hiles, FBCI – UK & France

Andrew is a Director of Kingswell International Limited, a global consultancy in all aspects of Business Risk Management.

Background

While the concept of Enterprise Risk Management has been around for over 25 years, it was formalized largely as a result of initiatives of the Committee of Sponsoring Organizations (COSO).[1]

COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission) following a number of cases of fraudulent accounting in corporations.

COSO was founded and is funded by the five main professional accounting associations and institutes in the USA:

- American Accounting Association;
- American Institute of Certified Public Accountants;
- Financial Executives International;
- Institute of Management Accountants;
- Institute of Internal Auditors.

The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control.

[1] www.coso.org. The pages describing COSO's ERM Framework that follow are copyright 2004. Committee of Sponsoring Organizations of the Treadway Commission. All rights reserved. Reprinted with permission.

The Definitive Handbook of Business Continuity Management, Third Edition.
Edited by Andrew Hiles FBCI. © 2011 John Wiley & Sons Ltd.

COSO is a voluntary private-sector organization, dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis and best practice.

Events, Risks and Opportunities

The impact of an event may be negative, positive or both. Events with a negative impact represent risk, which can prevent value creation or erode existing value. Events with a positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

Enterprise Risk Management: Definition
Enterprise Risk Management (ERM) is a process, effected by an entity's Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The definition reflects certain fundamental concepts. ERM is:

- a process, ongoing through an entity;
- effected by people at every level of the organization;
- applied in strategy setting;
- applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk;
- designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;
- able to provide reasonable assurance to an entity's management and Board of Directors;
- geared to achievement of objectives in one or more separate but overlapping categories.

The definition is intentionally broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining ERM effectiveness.

Expanding on Risk Management

The original COSO framework contains five control components needed to help assure sound business objectives. The control components are:

- Control environment;
- Risk assessment;
- Control activities;
- Information and communication;
- Monitoring.

Headline-grabbing scandals such as Enron, Tyco and Worldcom led to demands for stronger corporate governance and risk management. The result was the Sarbanes–Oxley Act, which requires internal control systems and the certification of them by management and the independent auditor. COSO's *Internal Control – Integrated Framework* remains the commonly accepted standard for the reporting requirements. Then, in 2004, COSO produced *Enterprise Risk Management – Integrated Framework*. This framework expands on these controls, providing a powerful spotlight on the wider topic of Enterprise Risk Management.

Business Objectives

COSO's Enterprise Risk Management framework aims to achieve corporate objectives. It includes four categories:

- **Strategic:** high-level goals, aligned with and supporting its mission.
- **Operations:** effective and efficient use of its resources.
- **Reporting:** reliability of reporting.
- **Compliance:** compliance with applicable laws and regulations.

The categorization means that a risk may fall in more than one category, so that it may be seen from different perspectives. Another category, safeguarding of resources, used by some organizations, is also described.

The ERM framework provides reasonable assurance of reporting and compliance requirements. For those events outside the organization's control, ERM provides reasonable assurance that management and the Board are made aware of the organization's progress towards its objectives and of any obstacles in its way.

The report says value is maximized when management sets strategy and objectives to strike an optimal balance between growth and return goals and related

risks, and efficiently and effectively deploys resources in pursuit of an entity's objectives. Enterprise Risk Management encompasses:

- **Aligning risk appetite and strategy.** Management considers an entity's risk appetite in evaluating strategic alternatives, setting related objectives and developing mechanisms to manage related risk.
- **Enhancing risk response decisions.** ERM provides the rigour to identify and select among alternative risk responses – risk avoidance, reduction, sharing and acceptance.
- **Reducing operational surprises and losses.** Entities gain enhanced capability to identify potential events and establish responses, reducing surprises and associated costs or losses.
- **Identifying and managing multiple cross-enterprise risks.** Every enterprise faces a myriad of risks affecting different parts of the organization, and ERM facilitates effective responses to the interrelated impacts, and integrated responses to multiple risks.
- **Seizing opportunities.** By considering a full range of potential events, management is positioned to identify and proactively realize opportunities.
- **Improving deployment of capital.** Obtaining robust risk information allows management to effectively assess overall capital needs and enhance capital allocation.

The capabilities inherent in ERM help management achieve the entity's performance and profitability targets and prevent loss of resources. ERM helps ensure effective reporting and compliance with laws and regulations, and helps avoid damage to the entity's reputation and associated consequences. In sum, ERM helps an entity get to where it wants to go and avoid pitfalls and surprises along the way.

Components of the COSO ERM Framework

The 2004 Enterprise Risk Management (ERM) COSO framework consists of eight components:

- Internal control environment;
- Objective setting;
- Event identification;
- Risk assessment;
- Risk response;

- Control activities;
- Information and communication;
- Monitoring.

The three new elements of the COSO framework are Objective setting, Event identification and Risk response.

A brief overview of the components follows.

- **Internal control environment.** The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
- **Objective setting.** Objectives must exist before management can identify potential events affecting their achievement. Enterprise Risk Management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
- **Event identification.** Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channelled back to management's strategy or objective-setting processes.
- **Risk assessment.** Risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed. Risks are assessed on an inherent and a residual basis.
- **Risk response.** Management selects risk responses – avoiding, accepting, reducing or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
- **Control activities.** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
- **Information and communication.** Relevant information is identified, captured and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across and up the entity.
- **Monitoring.** The entirety of Enterprise Risk Management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations or both.

The four categories of objectives – strategic, operations, reporting and compliance – are represented in the COSO cube diagram in Figure 1.1 by the vertical columns; the eight components by the horizontal rows; and the units within the entity by the third dimension. This portrayal shows a holistic view of the entity's ERM and at the same time permits views by category, component, entity unit or any subset of these.

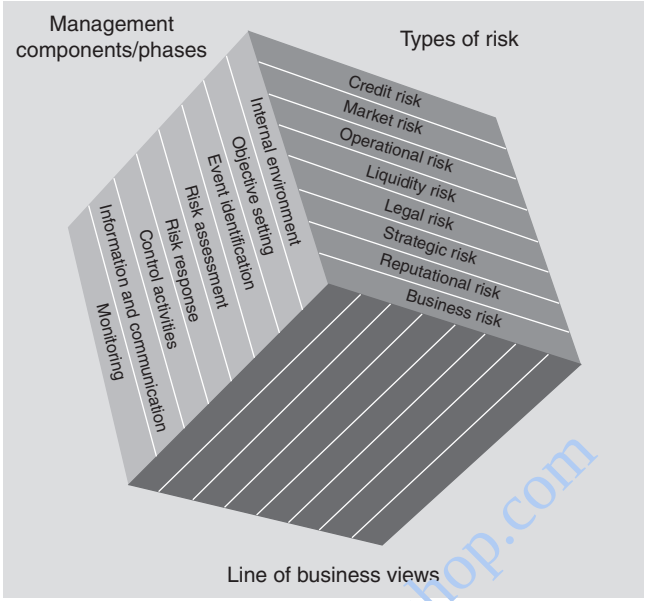

Figure 1.1—The COSO cube

Helping Organizations to Reduce their Exposure to Risk

By formally organizing ERM responsibilities and activities, an organization is much better positioned to achieve its business objectives and to ensure that sound risk management processes are in place and functioning. The *ERM – Integrated Framework* provides a comprehensive road map for establishing the critical processes needed to ensure an effective ERM effort. The framework offers a structured, consistent and continuous process to be used across the organization to identify, assess, respond to and report on opportunities and threats that affect the achievement of objectives. The framework will fill the need to meet new laws, regulations and standards for stock exchange listing and has become widely accepted.

Benefits of Implementing COSO's ERM Framework

Organizations that implement the process will have:

- a greater likelihood of achieving business objectives;
- consolidated reporting of disparate risks at the Board level;

- improved understanding of the key risks facing the organization;
- greater management focus on risks that really matter;
- more focus internally on doing the right things in the right way;
- more informed risk taking and decision making.

Effectiveness

The components of the COSO cube can be used as a basis for assessing the effectiveness of an organization's risk processes. If the components are present and working effectively, the risks must have been brought within the entity's risk appetite.

When ERM is accepted as being effective in each of the four categories of objectives, the Board of Directors and senior management are reasonably confident that they understand progress towards objectives and their reporting is reliable and compliant with relevant laws and regulations.

Smaller companies may adapt the concept and, even in less formal (COSO lite), as long as each of the components is present and working, they can still have effective ERM.

Risk Categories

Risk categories relevant to the organization are identified. The following risk categories are common to all organizations:[2]

- **Natural hazards** e.g. fire, earthquakes, hurricanes, etc.
- **Man-made hazards** e.g. wars, terrorism.
- **Financial risk** e.g. credit risk, liquidity risk, bankruptcy risk, adverse movement in exchange rates, interest rates, prices, costs, etc.
- **Operational risk** e.g. production breakdowns, supply chain issues, distribution issues, product quality problems, physical safety and security, etc.
- **Strategic risk** e.g. fluctuations in demand, technological advances, economic cycles, adverse legislation, etc.
- **Information risk** e.g. incorrect information, access to confidential information by unauthorized persons, cyber crime, malicious attacks.
- **Compliance risk** e.g. penalties and fines due to non-compliance, law suits, reputation losses, losing patents, etc.

[2] *Implementation of ERM under COSO Framework*, Muhammad Mubashir Nazir, ACCA, CISA, CIA, June 2007.

Some risk categories will be more important for one organization while other risk categories will be more important for others. For example, liquidity and credit risk are the most important risk categories for a bank whereas fire risk is the most important risk for an oil refinery.

Limitations

While Enterprise Risk Management provides important benefits, limitations exist. ERM is dependent on human judgement and therefore susceptible to faulty decision making. Human failures such as simple errors or mistakes can lead to inadequate responses to risk. In addition, controls can be circumvented by collusion of two or more people, and management has the ability to override Enterprise Risk Management decisions. These limitations preclude a Board and management from having absolute assurance as to achievement of the entity's objectives.

Although the expanded model provides more risk management, companies are not required to switch to the new model if they are using the *Internal Control – Integrated Framework*.

The COSO framework has been criticized for failing to identify risks in the 2008 economic crisis. 'Changes in risk arising from changed business models were apparent in the crisis,' said David Landsittel, chairman of The Committee of Sponsoring Organizations of the Treadway Commission (COSO). 'It illustrates the importance of companies having ongoing processes that add assurance that changes in enterprise-wide risks are recognized on a timely basis.'[3] 'The causes of the financial crisis are complex and involve many factors. I'm more interested in discovering the lessons learned – what can we take from it that benefits COSO and our stakeholders? The first lesson is that the more companies know about the risks they face, the better. It's also important for companies to be able to identify changes in risk as quickly as possible. To manage such changes effectively, companies should have disciplined processes to examine enterprise risk. More importantly, those processes should be ongoing to allow for effective identification of new and emerging risks.'

ERM Organization

An example of an ERM organization is shown in Figure 1.2.[4]

[3] www.thefreelibrary.com/In+control:+COSO's+new+chairman,+David+Landsittel,+says+organizations…-a0214841445

[4] Institute of Internal Auditors' presentation *Applying COSO's Integrated Risk Management Framework* September 2004.

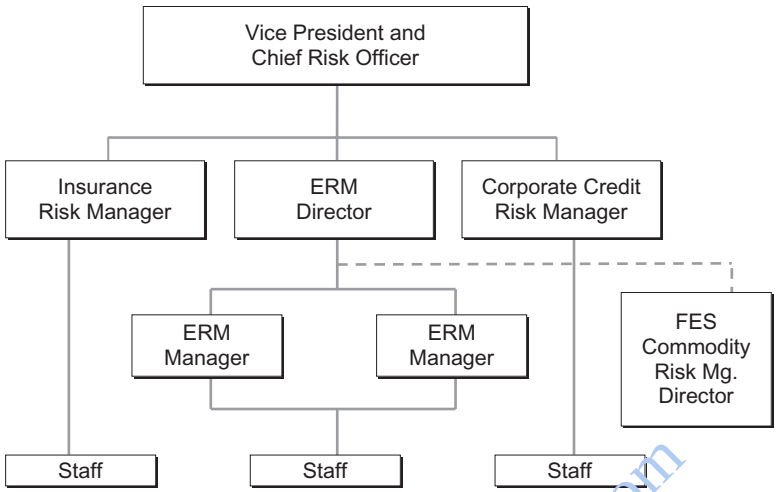

Figure 1.2—Example of an ERM organization

COSO Sources

COSO sources used in the foregoing pages of this chapter include:

Enterprise Risk Management – Executive Summary, September 2004, COSO.
Internal Control Over Financial Reporting – Guidance for Smaller Companies, 2006, COSO.
Integrated Control – Integrated Framework: Guidance on Monitoring Internal Control Systems, 2009, COSO.
Institute of Internal Auditors' presentation *Applying COSO's Integrated Risk Management Framework*, September 2004.

Other Frameworks and Relevant Standards

Criteria of Control (CoCo) is a control framework issued by the Canadian Institute of Chartered Accountants. The Criteria of Control Board issued the framework in 1995 for evaluating controls. While there are many areas of overlap between COSO and CoCo, CoCo differs from COSO in a number of areas.

KonTrag is a German framework. KonTrag can be translated as the 'Control and Transparency in Business Act'. It promotes corporate governance in both the

public and the private sector. It targets the German capital market, aiming to bring enterprises up to international standards of corporate governance.

The Combined Code of Corporate Governance is a requirement for listing on the London Stock Exchange. The Turnbull, Cadbury and Greenbury reports on corporate governance form the background to this Code which provides guidance in adopting a risk-based approach.

ISO 31000 is an international standard for risk management published in November 2009. Its accompanying standard, ISO 31010 – Risk Assessment Techniques, followed on December 1, 2009 together with the updated risk management vocabulary ISO Guide 73.

ISA 400 Risk Assessments and Internal Control is an international auditing standard. It requires the auditor to understand the client's accounting and internal systems and to assess control risk and inherent risk. The standard aims to establish the nature, timing and extent of effective processes so as to reduce audit risks to an acceptable low level.

First introduced in 1995, the Australian/New Zealand Standard: Risk Management (AU/NZS 4360) is one of the most popular frameworks implemented outside of the USA.

The Association of Insurance and Risk Managers (AIRMIC) Risk Management Standard, first published in 2002, is a best practice guide recognized throughout Europe and internationally. It was developed by AIRMIC, the Institute of Risk Management and the Association of Local Authority Risk Managers (ALARM).

Control Objectives for Information and Related Technology (CobiT)[5] was derived from the COSO framework. It was developed by the Information Systems Audit and Control Association and the IT Governance Institute. It helps to define risk objectives at a business/technology interface level. It defines goals for the controls used properly to manage IT and ensures that IT is aligned with business needs.

How do Organizations Implement ERM?

Aon's 2010 Global Enterprise Risk Management Survey,[6] designed to illustrate the extent to which ERM has been successfully implemented by organizations around the world, revealed nine features of an advanced ERM programme. These qualities are key to a programme's effectiveness in creating value for its organization, regardless of company size, industry, sector or region.

Respondents compared themselves against Aon's five-stage ERM maturity model. This model defines a firm's ERM programme implementation level on a scale ranging from 'initial/lacking' and 'basic' at the low end to 'defined' for average maturity and 'operational' and 'advanced' for those at more sophisticated stages.

[5] www.isaca.org/cobit/
[6] www.aon.com/ermsurvey2010

Only 7% of those professionals surveyed rated themselves at the advanced level, while 58% reported ERM implementation at the defined or operational levels. 35% categorized the maturity of their ERM programmes as initial/lacking and basic. Consequently, the survey found that 93% of organizations now have the opportunity to increase the impact of their ERM programmes.

The resulting data uncovered the nine hallmarks of top-performing Enterprise Risk Management programmes:

1. Board-level commitment to ERM as a critical framework for successful decision making and driving value.
2. A dedicated risk executive in a senior-level position, driving and facilitating the ERM process.
3. ERM culture that encourages full engagement and accountability at all levels of the organization.
4. Engagement of stakeholders in risk management strategy development and policy setting.
5. Transparency of risk communication.
6. Integration of financial and operational risk information into decision making.
7. Use of sophisticated quantification methods to understand risk and demonstrate added value through risk management.
8. Identification of new and emerging risks using internal data as well as information from external providers.
9. A move from focusing on risk avoidance and mitigation to leveraging risk and risk management options that extract value.

Take-up of ERM

The concepts embedded within COSO ERM have been taken up by a number of professional bodies around the world, some of which have developed differing models. A report by Towers Perrin,[7] a global professional services firm, identified that:

> 'At most companies, responsibility for ERM resides within the C-suite. Most often, the Chief Risk Officer (CRO) or the Chief Financial Officer (CFO) is in charge of ERM, and these individuals typically report directly to the Chief Executive Officer. From their vantage point, the CRO and CFO are able to look across the organization and develop a perspective on the risk profile of the firm and how that profile matches its risk appetite. They act as drivers to improve skills, tools and processes for evaluating risks and to weigh various actions to manage those exposures.'

[7] Life Insurance Survey #19: *Embedding Enterprise Risk Management*, May, 2008 http://www.towersperrin.com/tp/getwebcachedoc?webc=TILL/USA/2008/200805/CFO_Survey19.pdf

The report further found that:

- 75% of companies have risk management tools;
- >80% are good or adequate;
- >80% of respondents reported that they currently have adequate or better controls in place for most major risks;
- ~60% currently have a coordinated process for risk governance and include risk management in decision making.

Despite this:

- only 29% of respondents currently have a clear vision of their risk tolerances/risk appetite and overall risk profile;
- 31% currently have robust processes to identify and prepare for emerging risk;
- only 32% currently have the ability to quantify economic capital.[8]

There can be substantial benefits to having a strong ERM framework. A.M. Best's system provides an opinion of an insurer's financial strength and ability to meet ongoing obligations to policyholders. A.M. Best states that a 'strong' ERM programme can lead to lower Best's Capital Adequacy Ratio (BCAR) capital requirements for the same financial strength rating.

Another Towers Perrin report[9] found that:

- Although companies have made progress in integrating ERM into their business, insurers worldwide continue to struggle with the challenge of embedding ERM.
- Larger insurers (those with revenues in excess of $10 billion) are significantly more advanced in most aspects of ERM implementation and are increasingly looking to realize their competitive advantage.
- North American insurers are trailing their European counterparts in key aspects of ERM implementation.
- Nearly 80% of participants reported that their ERM programme had influenced important business decisions since 2006.
- A global standard for EC methodology is emerging. Companies are increasingly adopting a one-year Value at Risk (VaR) approach, with the majority using a market-consistent terminal balance sheet.
- Globally, just 7% of participants believe they have an appropriate operational risk management capability in place.

[8] Economic capital is the amount of capital deemed appropriate by a firm to cover worst-case losses in all but the most extreme economic scenarios. Accordingly, it represents the largest cumulative loss a company can withstand without going bankrupt. It reflects a firm's internally determined capital needs, as opposed to the capital requirements imposed by external regulators.

[9] 2008 Global Insurance Industry ERM Survey Report.

Marketing	Financial	Human Resources
New business sold	Revenue	Composition (number, age, service)
Retention of old business	Underwriting profit	Total employment by department:
Mix of business: new & old	Investment profit	Turnover & % leaving company
Geographic spread	Pre-tax operating income	Vacancy rates
Market share by product	Net income	Average pay increase vs plan
Market share by customer type	Return on equity and total capital	Disciplinary cases
Average premium or assets per customer	Forex exposure	Sales per agent
% high-yield customers	Fraud	Employee commitment & engagement
Customer satisfaction	Economic value added	**Claims**
Average # of products per customer	**Sales Distribution**	Frequency & severity of claims
Underwriting	Acquisition costs per sale	Claims department
Price achieved vs target price	Retention cost per customer	**External Data**
Exposure data (# of cars, payroll etc)	Sales by distribution channel	Regulatory compliance
Exposure mix	% & value of up-sales	Credit compliance
Quotes accepted/declined	% and value of cross-sales	Interest rates
Variance analysis	**Investments**	Interest rates
Premium persistency	Cashflow	Forex rates
Loss ratio	Yield on new investments	GNP
Loss adjustment expense	Yield on portfolio & class & duration	Competitor pricing
Technology	Convexity of assets	
ICT incidents	Duration of assets	
ICT performance	Investment mix: new & old portfolio	
ICT/business alignment	Credit default	
Information security	Total return	

Figure 1.3—Overview of Enterprise Risk Management for an insurance company

- The recent wave of losses in the financial services industry is resulting in a reassessment of the role of operational risk and the need for its active management.

Figure 1.3 provides an overview of ERM in an insurance company.

While ERM has made substantial inroads in insurance, banking and the finance sector generally, it has been embraced by a number of other industries and sectors. A PricewaterhouseCoopers report[10] with the Thought Management Institute conducted a survey of 52 North American, European and Japanese financial

[10] *Seizing Risk and Opportunity – Linking Risk and Performance*, July 2009.

institutions. The report identified that the market tends to assign a higher price-to-book multiple to firms with more effective, sophisticated risk management programmes, as measured by earnings volatility, capital adequacy and capital optimization. The report quotes examples of companies using ERM as diverse as IKEA, a multinational energy company, an aerospace and defence company, a US fixed satellite service provider, a global financial services company, and cites Canadian utility Hydro One as one of the first non-financial companies to receive an improved credit rating based on an evaluation of its risk management practices.

However, there is room for improvement in embedding ERM. In a survey of senior executives:

- just 37% of respondents said their companies linked key risk indicators (KRIs) with key performance indicators (KPIs);
- 45% of survey respondents said their organizations did not link risk and performance indicators at all;
- 15% were uncertain whether their companies did so.

A North American survey of actuaries working in risk management was released in conjunction with the 2010 ERM Symposium in Chicago. 82% stated senior leadership within their organizations hold a holistic approach but only 47% claim that ERM is deeply integrated within corporate culture. The survey also found that systemic risk (risk involving a whole system or market – e.g. the 2008 collapse of the financial markets) is the second most important issue that executives and Boards of Directors will face this year.

PricewaterhouseCoopers' 2008 Management Barometer indicated that 51% of the executives surveyed said that one person (most frequently the CFO) or group is responsible for both risk management and performance management, and 49% reported that oversight resides with a combination of executives. The survey concludes that a centralized, top-down approach to risk may work for some companies, but a more collaborative, integrated accountability structure that provides appropriate incentives at every level of the organization may be better suited to managing risk alongside performance in an increasingly interconnected business world.

Although the CFO is often de facto the CRO, other positions acting as CRO may include the Compliance Manager, Legal Manager, Asset and Liability Management (ALM) manager(s) and the Treasurer.

Since the financial scandals and banking collapse, there has also been an increase in the emphasis on ethics and integrity, with Integrity Managers being appointed to work against unscrupulous practices, corruption and fraud – previously understood to be the province of the Auditor. In April 2009, the Inter-American Development Bank in Washington, D.C. was advertising for a Principal Integrity Officer reporting to the Chief of the Office of Integrity, which reported directly to the President of the Bank. The role was 'to combat fraud and corruption and to foster integrity within the Bank and the activities it finances.' The background

required legal, forensic accounting or criminology qualifications. Equally, there has been growth in the number of Corporate Responsibility Officer positions, to ensure organizations behave like good citizens: the Corporate Responsibility Officer's magazine has a 20 000 subscription base.

The Chief Risk Officer

The title of CRO goes back to 1988, when it was first mentioned in a Peat Marwick survey. Accountants Grant Thornton see the emergence of the CRO role not just in private sector organizations, but also in the public sector:

> 'In response to the growing concern, an increasing number of colleges and universities are establishing the position of Chief Risk Officer (CRO), following the example set by for-profit entities in health care, energy, insurance and financial services. While many CFOs consider themselves to be their organization's de facto risk officer, the trend is to create a separate position for this function.
>
> Even if organizations don't establish such a position, they need to make certain that the function exists within the organization. This can be achieved by establishing a committee comprised of individuals representing key risk areas or by explicitly adding these specific duties to another officer's responsibilities.'[11]

A Forrester Research report in 2004 stated that the executive ranks of any company that has revenue of at least $1 billion and can be classified as 'critical infrastructure' – such as financial institutions, utility companies and health care providers – are likely to include a CRO – 75% of such organizations that did not, planned to have one in place over the following few years. A joint survey in fall 2009 by *Disaster Recovery Journal*/Forrester Research identified that three-quarters of large, critical infrastructure organizations had a formal ERM office with a CRO or equivalent role. The survey also found that:

- only 20% of companies had risk management silos not connected by a single programme;
- 64% of BC programmes have a relationship with ERM.

The CRO role: job description

The CRO's job is to:

- promote the risk management perspective in strategic decision making;
- seek to ensure the organization complies with ERM best practice;

[11] *OnCourse*, Spring 2009, Grant Thornton.

- ensure the Board of Directors has defined the organization's risk appetite;
- raise risk awareness (risk culture, risk attitude, risk mentality) and secure the commitment of senior management to the ERM programme;
- communicate with all business and support units in the entity and develop, with their cooperation, an agreed-on risk framework;
- identify all risk owners, ensure they understand the risks for which they are responsible and provide them with advice, support and incentives for effective risk management;
- ideally, to standardize, integrate and aggregate all risks within the organization; or at least raise risk visibility; these risks include (at least) geopolitical risks, compliance and regulatory risk, market risks, credit risks, trading risks, operational risks, reputation and brand risk, strategic risks, physical risks (natural and man-made), terrorist and criminal risks, ethical risks, supply chain risks, technology risks, environmental, health and safety and employee risks;
- implement economic, risk-based capital allocation and risk adjustment for optimum performance measurement;
- identify and report on the top risks a company faces and on any significant change in their probability or impact;
- be a source to which 'whistleblowers' can, without prejudice, report any risk or ethical issues.

A typical CRO job description follows.

The CRO manages, provides resources for, and directs the ERM programme. Primary responsibility is to provide objective assurance and advisory services to ensure appropriate coverage in developing the company risk profile, identification of significant risks, establishing the appetite for risk and seeking to ensure activities remain within it, and risk response strategies/actions.

- Responsible for developing and maintaining the ERM programme, aligned with the COSO ERM Integrated Framework.
- Leads development and annual planning for ERM activities, budgets and resources.
- Hires, manages and develops direct reports to support organization's mission.
- Maintains a trusted, collaborative relationship with organization management to promote appropriate engagement in ERM activities.
- Manages and coordinates requests for information from external constituents (auditors, regulators and rating agencies).
- Leads scheduled enterprise risk reporting requirements. Works with Financial, Legal, Compliance, Information and Communications

Technology, and Operations teams to ensure complete, high-quality, timely and reliable reporting for Executive Management and the Audit Committee of the Board of Directors.
- Supports business and support units with the identification, evaluation, understanding, management and communication of significant risks.
- Reviews key performance indicators/metrics and assists management in the early identification of risk trends.
- Conducts detailed assessments, data mining and analysis to identify, validate and quantify existing and emerging risks.
- Builds strong alliances inside and outside work units to positively influence identification and resolution of significant risks/opportunities.
- Works with business and support unit management to prepare risk self-assessments, including analysing the effectiveness of existing controls, identifying gaps and creating action plans.
- Provides risk support for major initiatives and ongoing programmes as appropriate, including M&A activities and related integrations; community programmes; supply chain activities; new projects; design, development and launch of new products; and major system/process improvements. Support may include due diligence, assessment of project management, collaborative development or improvement of controls, consulting on key concerns or exposures and managing audit activity.
- Creates and delivers presentations to Executive Management and the Audit Committee for risk reporting, training, etc.
- Leads the development and delivery of ERM training programmes. Continuously assesses changes in the programme content to ensure ongoing effectiveness.

Education: BS in Business Administration, Finance, Accounting or related field required; advanced degree preferred.

Experience: 10+ years of Enterprise Risk Management, audit, project management or related experience required.

Certifications: CERA, CRM, CPA, CIA, CFA, CISA

Relations in Risk Management

Crisis Management, Continuity Management, Contingency Management, Emergency Management, Operational Risk Management, ICT DR, Security, Corporate Governance…Where and how do all these fit together? Well, they don't actually fit together. They are sometimes recognizably discrete activities and sometimes merge fluidly. Sometimes one is incorporated within another, sometimes they sit

Figure 1.4—Governance, risk and plan relationships

within silos, depending on the organization. But however they are managed, an ERM-oriented organization needs to deal with all the aspects of risk that sit within Figure 1.4 – and maybe more!

Conclusion

ERM is well entrenched and its implementation is spreading. It provides a proven framework within corporate governance for risk management. Whether this framework is applied by a full-time CRO, the Audit Committee, some other group of people within an organization or a series of dotted line relationships to a CFO/CRO, ERM activities are a prerequisite for sound governance and risk management. There are many players involved with risk within any organization. It is simply unrealistic to expect them all to present a coherent concert without having the same music and without a conductor.

Business Continuity is an important part of ERM and will continue to be so: it covers, or partly covers, several of COSO's risk categories. But, by itself, BCM cannot protect an organization from all of the categories of risk that face it. To do that, we need a wider framework that also covers:

- natural hazards;
- man-made hazards;
- financial risk;
- operational risk;
- strategic risk;
- information risk;
- compliance risk.

We need a holistic approach to all risks within these categories, with perspectives across all units, that covers:

- **Strategic:** high-level goals, aligned with and supporting its mission.
- **Operations:** effective and efficient use of its resources.
- **Reporting:** reliability of reporting.
- **Compliance:** compliance with applicable laws and regulations.

That is the real benefit of the COSO and other ERM risk frameworks: it really is *Enterprise* Risk Management.

The author gratefully acknowledges the permission of COSO to reproduce material from the *Enterprise Risk Management – Executive Summary* and other COSO documents in this chapter.