CHAPTER 5
AUDITING RISK ASSESSMENT AND RISK MANAGEMENT PROCESSES

William R. Kinney, Jr.

The Institute of Internal Auditors Research Foundation

Disclosure

Copyright © 2003 by The Institute of Internal Auditors, 247 Maitland Avenue, Altamonte Springs, Florida 32701-4201. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form by any means — electronic, mechanical, photocopying, recording, or otherwise — without prior written permission of the publisher.

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

The Professional Practices Framework for Internal Auditing (PPF) was designed by The IIA Board of Directors' Guidance Task Force to appropriately organize the full range of existing and developing practice guidance for the profession. Based on the definition of internal auditing, the PPF comprises *Ethics* and *Standards, Practice Advisories,* and *Development and Practice Aids,* and paves the way to world-class internal auditing.

This guidance fits into the Framework under the heading *Development and Practice Aids*.

ISBN 0-89413-498-1
02404 01/03
First Printing

I. Introduction

Internal auditors provide assurance about the reliability and relevance of an entity's information and internal control. In an environment characterized by rapid change, global competition, new organization forms, and improved information technology, measures of an entity's current state and recent past are relatively less important, while information about and measures of what might happen in the near and even distant future are more important. In simple terms, there is a shift in emphasis from the internal audit function (IAF) "counting the beans" to threats to strategies and processes for bringing beans to market and selling them at an acceptable profit.

In today's environment, a thoughtful and forward-looking CEO might ask:

- Do possible external environment changes threaten achievement of my company's strategy objectives?
- Are factors that might impair my business processes within reasonable limits?
- Could assets of my company be stolen?
- Do internal processes, displays, and reports provide adequate measurement and communication of threats to assets, processes, and strategy achievement?
- Are my reports to outsiders in compliance with applicable standards, laws, and regulations?

All five of these questions are about possible real-word events that might seriously threaten a firm and are the subject matter of enterprise risk management and monitoring by the IAF.

Accountants and auditors are increasingly called upon to measure and report on threats to a business entity. The last decade-mandated external financial reporting reflects the new "rapid change" environment through expanded requirements for disclosure of risk assessments by management, through expanded management discussion and analysis in financial statements, and through increased disclosure of the sensitivity of accounting estimates to possible changes in assumptions. At the process level, several countries now require management or director assertions that they have adequate internal control, including risk control processes (see Miccolis et al., 2001, pp. xxiv-xxvi, for a summary). Inside the firm, the rapid change environment has had even more dramatic effects with the emergence of a chief risk officer (CRO) and development of risk management departments in many entities today.

At the standards setting (or measurement criteria) level in the U.S., the Committee of Sponsoring Organizations of the Treadway Commission (COSO, 2002) is redefining and extending its internal control framework as enterprise risk management (ERM). Management is responsible for ERM design and all personal help implement it. The board of directors oversees management's design and operation of ERM, while the IAF assists by ongoing separate evaluations of ERM's effectiveness. Through COSO, ERM provides an important basis for assessing the role of the IAF in auditing risk assessments and the risk management process.

This chapter outlines some of the opportunities for scholarly research about the role of the IAF in evaluating risk assessments and processes and reporting results. Specifically, we consider the relation of the IAF to long-term business strategy and its continuous implementation, and the role of risk as a tool for early warning of the need for changes in strategy or its implementation. We also consider the historical risk assessment and management roles of financial reporting, auditing, and the IAF. We do this within the framework of enterprise risk management as recently defined by COSO (2002).

II. Accounting, Internal Auditors, and Risk

Most agree that comprehensive risk assessment is increasingly important for success (or even survival) of an entity, but how to go about it systematically is open to debate. Part of the problem is the difficulty of measuring threats or risks. For example, quantifying past sales is relatively easy compared to quantifying threats to expected future sales. Threats are *possibilities,* and at any point in time there are many possibilities (and combinations of possibilities) leading to problems in assessing and reporting on ranges of possible outcomes. A second problem is risks can change rapidly and possible changes must be identified before they can be measured. Third, threats can't be fully evaluated even after the passage of time because some don't materialize and others arise but are prevented or mitigated by control activities. Finally, there is no natural measurement process and point in time for risk measurement as there is in measuring a sale, the purchase of an asset, or incurrence of a liability or expense.

The accounting process and the IAF have historically measured and analyzed the results of implementing operating plans, but not the risks faced. This means that a measurement system for risk must be developed. Thus, even though risk measurement is inherently more complex than measurement of the current state, its increasing importance for understanding a business demands a comprehensive business measurement system subject to appropriate monitoring for both management and relevant outsiders.

One way to characterize a business entity (the firm or a segment) and the risks it faces is in terms of its stated long-term goals, the strategy that management has chosen to achieve these goals, and the business model and operating plans for guiding actions to implement these strategies over a shorter period. Business risks are defined here as "threats to achieving the entity's objectives." These threats affect interpretation of accounting measures of financial performance and conditions. The threats can be measured and classified in various ways, and occur throughout the chain of events outlined above.

Public accountants and auditors have experience with aggregate financial disclosures for an enterprise. In the U.S., they have also become experienced in the reporting of risk assessments through the American system of accounting disclosures, securities regulations, and corporate governance (e.g., the AICPA's SOP 94-6 and the SEC's Management Discussion and Analysis required of registrants). External auditors also have some experience attending to management assertions about compliance with COSO's criteria for internal control in the U.S. and CoCo in Canada.[1]

The IAF has played a key role in evaluating internal control over risk assessments and control activities through implementation of COSO and compliance with external disclosure requirements discussed above. Thus, while they have had experience measuring profitability and progress toward achieving financial objectives, and also developing accounting systems for measurement, accountants in North America have had less experience with forward-looking risk assessments and risk assessment systems. The same applies to auditors.

By its nature, risk involves more than one possible real-word condition or event that has occurred or might occur in the future. Thus, numbers, categories, or labels to represent risk assessments are different from business process measures of a single condition at a point in time. This means that there is no single answer that can be determined to be correct in measuring or auditing risk assessments. There is inherently more uncertainty in auditing risk assessments than auditing the current cash or inventory balance. The multiple possibilities for joint occurrence of risks greatly complicate measurement of and auditing risk assessments and processes. Furthermore, the evaluation of ERM performance is hindered by the difficulty of determining whether occurrence of an undesired event is due to bad event identification, bad risk assessment, bad information, bad modeling, bad strategy, bad implementation, or simply bad luck. Yet each cause has different and important implications for the future.

Types of Business Risk

Determination of business objectives and strategies to achieve them is beyond the scope of enterprise risk management. However, assessments of all potentially serious risks inherent in strategies and business processes are part of internal control and are essential for evaluating the relevance and reliability of information and its context.

In developing a comprehensive list, business risks can be classified in many ways. One useful way is:[2]

> **External Environment Risks** — threats from broad factors external to the business including substitute products, catastrophic hazard loss, and changes in customers' tastes and preferences, competitors, political environment, laws/regulations, and capital and labor availability.
>
> **Business Process and Asset Loss Risks** — threats from ineffective or inefficient business processes for acquiring, financing, transforming, and marketing goods and services, and threats of loss of firm assets including its reputation.
>
> **Information Risks** — threats from poor-quality information for decision-making within the business (i.e., the risk of being *misinformed* about real-world conditions due to using measurement methods that are not relevant, from careless or biased application of measurement methods or their display, or from incomplete information).

Information risk overlaps somewhat with external environment and business process risks because the risk of being misinformed may be about an external environment, business processes, or asset loss risk. Information risk also applies to the risk of providing erroneous or misleading information to outsiders. The latter risks may make management liable for statements about risk just as it does for bad financial and other information.

Exhibit 5-1 presents more details of risks in each of the three broad categories. The external environmental category includes longer-term factors external to the firm that are largely beyond management's control. Catastrophic natural events (sometimes called hazard risks) are not controllable by management, yet management can limit the enterprise's exposure to their effects. Similarly, management can influence environmental change to some degree through research and development of technology, advertising, and lobbying of governments. But mostly these factors are constraints to which management must respond. Timely information about environmental change is important since management has more options (and probably lower cost options) if it has more time to react.

Exhibit 5-1
Principal Business Risks by Broad Categories

External Environment	Business Processes	Information
Catastrophic events (natural disasters, economic collapse, social revolution) Environmental change Customers' tastes and preferences New (substitute) products Technology Competition Labor, materials, and capital availability and cost Political/cultural climate Laws and regulations	Inefficient or ineffective business Loss of assets (due to theft, fraud, erosion, accident, obsolescence) Tangible Intangible (patents, goodwill, human resources (capabilities, trust, flexibility, adaptability, morale) Market-based (customer base, satisfaction and loyalty; product quality, supplier quality, alliance partner reliability) Financial risk (credit, interest rate, market, currency, collateral, counter-party) Improper incentives to employees and trading partners Reputation loss (integrity risk) Unethical behavior Unacceptable practices by employees or management Illegal behaviors by management, employees, or trading partners	Operations Unauthorized access to information Inadequate recorded accountability Internal information not relevant, reliable, complete, integrated, or accessible Financial reporting reliability Unreliable or incomplete financial information for internal decision-making or provided to outsiders Compliance Inadequate communication of laws and regulations for financial information, internal control, safety, human resources, and environment Internal behavior codes of expected behaviors and practices Contract requirements Inadequate information about failure of management, employees, or trading partners to comply with applicable laws, regulations, contracts, and expected behaviors

Kinney, W.R., *Information Quality Assurance and Internal Control for Management Decisions* (Boston: Irwin McGraw-Hill, 2000). Reproduced with permission of The McGraw-Hill Companies.

A Business Risk Example: Guiness PLC

Guiness is a UK firm with two major business units and product lines — distilled spirits (United Distillers, Johnny Walker Black) and brewing (Guiness Brewing Worldwide, Guiness Ale) — and employs about 23,000 workers worldwide. Guiness management conducted a comprehensive risk analysis with a goal of managing "where we can, and . . . transfer risk to third parties where this is cost effective."[3]

Exhibit 5-2 illustrates how Guiness manages selected environment and business process risks that it has identified, and some possibilities for information risks (Kinney, 2000, p. 63). In Exhibit 5-2, selected potentially important risk exposures are identified and listed along the real-world source of the risk. Each listed risk is assessed as to its possible magnitude (e.g., possible monetary loss) and the probability of a loss of that magnitude. Then, management's response to risk is entered. Some risks are avoided at the source, some are transferred or shared, and some are reduced by control procedures. All risks are monitored for changes, with some monitored on a more or less continuous basis and others only periodically.

External Environment Risks — Longer-term external factors related to alcohol consumption are important to Guiness as a maker of alcoholic beverages. Customer tastes and preferences for distilled spirits and brewed products determine aggregate demand and growth potential. Tastes and preferences vary by region, religion, and culture, and over time with trends in lifestyles and alternative products. Guiness tries to limit the effect of changes in tastes and preference by building its reputation for offering a premium quality product within its market.

Cultural climate risk reflects attitudes of non-customers as well as customers within a country, state, province, or municipality. Changes in social attitudes can also lead to increased regulation of the final product through prohibition of sale and strict liability laws (e.g., drunk driving laws). To mitigate cultural risks, Guiness has promoted responsible use of alcoholic products.

Finally, because of restrictions on Scotch whiskey production and aging, catastrophic loss risk for aging facilities is potentially important. Guiness considered the risk of catastrophic loss of aging facilities due to, say, a plane crash. A plane crash could destroy a small aging facility and could wipe out Scotch in process for up to a 10-year period. However, Guiness management concluded that because of the large size of its facilities, the likelihood of catastrophic loss was virtually zero and that any reasonably possible loss magnitudes could be endured. Thus, dispersion of aging facilities to many locations is judged not worth its cost — management simply accepts the risk.

Exhibit 5-2
Partial ERM Components Chart for Guiness PLC

	Assess Risk		Risk Response and Risk Control Activities				
Event identification for all potentially important risks	Exposure magnitude	Prob.	Accept	Avoid	Transfer/ share	Reduce	Risk monitoring
External Environment							
Catastrophic loss of production or storage facilities							
Terrorists	H	L		no breweries in hostile cultures			review political environments quarterly
Plane crash at Scotland aging facility	VH	VL	accept				review annually
Laws and regulations							
Restrictive regulation adoption	M	L				"responsible use" promotion	review annually
.							
.							
.							
Business Process and Asset Loss							
Financial risk							
Fluctuation in foreign currency exchange rates over next 10 years	M[1]	M			share with customers (brand loyalty)	hedge inputs and currency	review quarterly
Counter-party risk for hedges	L	L	accept				review quarterly credit reports

Kinney, W.R., *Information Quality Assurance and Internal Control for Management Decisions* (Boston: Irwin McGraw-Hill, 2000). Reproduced with permission of The McGraw-Hill Companies.

Exhibit 5-2 (Cont.)

Event identification for all potentially important risks	Assess Risk: Exposure magnitude	Assess Risk: Prob.	Risk Response and Risk Control Activities: Accept	Avoid	Transfer/ share	Reduce	Risk monitoring
Ineffective business processes							
Product and delivery quality	M	L				production quality controls/ delivery scheduling	monitor quality daily/weekly
Loss of asets - market-based customer loyalty	H	M				brand image promotion	measure customer attitudes monthly
.							
.							
.							
Information Deficiencies[2]							
External environment change information							
Leading indicators not processed or communicated							
Competitive or supply information not communicated							
Business process and asset loss information							
Asset loss not discovered/ reported on timely basis							
Public reports are materially misstated							
Financial statements							
Environmental impact reports							
Fair labor practices assertions							

[1]VL, L, M, H, and VH denote very low, low, moderate, high, and very high magnitudes and probabilities of possible loss respectively.
[2]Risks are the author's speculation rather than a communication of Guiness PLC. Risk assessments and responses and monitoring would parallel traditional auditing and application of the ERM monitoring discussed throughout this chapter.

Business Process Risks — Guiness' business process risks are interrelated. Currency risk for Guiness is high because, to be "Scotch," Scotch whiskey must be made and aged in Scotland, and the process can take up to 10 years to complete. The finished product is sold around the world in local currencies and transferred at time-of-sale currency exchanges rates. Guiness hedges its input resource commitments a year ahead, and relies on brand loyalty and the related price inelasticity that will allow raising prices to hedge final product currency fluctuations.

Brand loyalty is an important market-based asset, and risk of its loss is a very important risk. Brand loyalty is protected by effective promotion and marketing of consistently high-quality products (related to customer satisfaction risk and product quality risk). Customer satisfaction and product quality are key nonfinancial success factors that are continuously measured and closely monitored by management.

Information Risks — In the case of Guiness PLC, the information risks in Exhibit 5-2 are not necessarily the information risks that Guiness management perceives and addresses. Rather, they have been included to illustrate some possibilities (Guiness' information risks are unknown).

III. Enterprise Risk Management (ERM)

Business risks exist throughout an enterprise and must be managed individually and in the aggregate. Enterprise risk management is defined by COSO (2002) as —

> a process, effected by an entity's board of directors, management, and other personnel, **comprising internal control and applied in strategy and across the enterprise,** designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations
> - Reliability of financial reporting
> - Compliance with applicable laws and regulations

(**emphasis added** to distinguish expansion of COSO's definition of internal control, which is subsumed by ERM).[4] Thus, ERM is broad in scope and includes traditional internal control over transactions, assets, and operations.

According to COSO (2002), ERM provides risk information to the **board of directors** about the most important entity risks and how well risk is being managed, including risk-adjusted

measures of performance. The **board of directors** is responsible for overseeing management's design and operation of ERM. **Management** is responsible for the design and operation of an entity's enterprise risk management, and **all personnel** have some responsibility for successful execution of ERM. The IAF is typically responsible for evaluations of the effectiveness of the ERM.

ERM has seven components:

- Environment
- Event identification
- Risk assessment
- Response
- Control activities
- Information and communications
- Monitoring

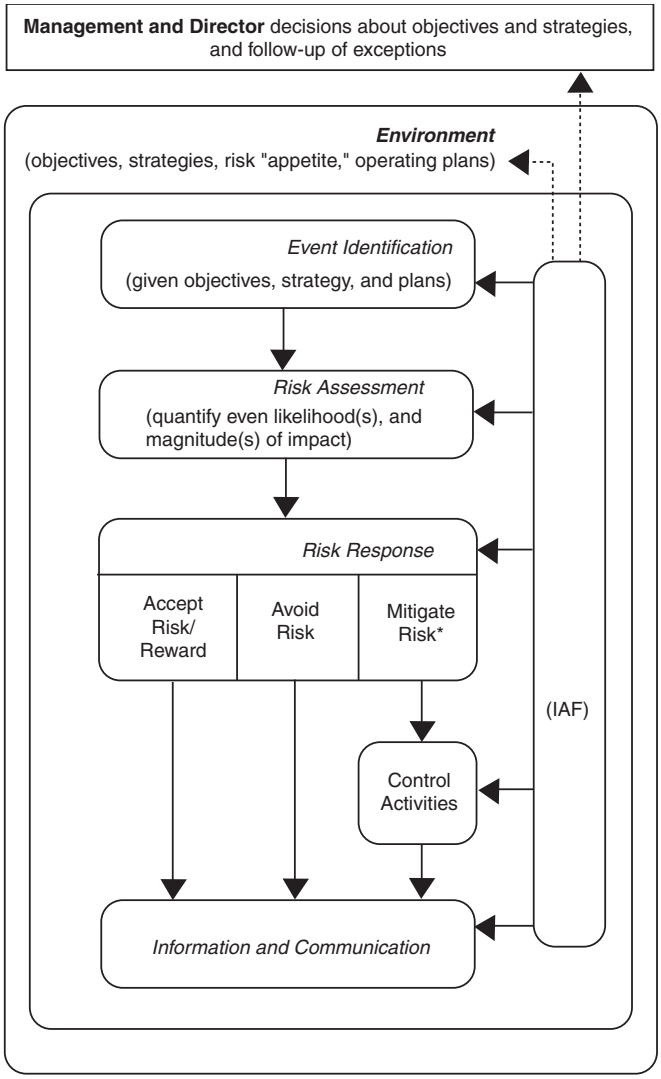
The components (discussed below) are interrelated and all must be present for effective ERM.

ERM (depicted in Exhibit 5-3) will be used to structure this chapter and the research questions for research opportunities in internal auditing for risk management. As shown in Exhibit 5-3, ERM is very broad. It includes all management activities except for decisions about enterprise objectives and strategy, and follow-up of exceptions noted in monitoring of ERM.

Environment

Directors and management determine the objectives of the entity, its strategies to achieve objectives, a business model detailing how business processes interrelate, and operating plans to implement strategies in the short-run. These choices comprise the **environment** for ERM and provide the framework within which the other components operate. The **environment** also includes what might be called a "philosophy about risk management" and an "appetite" for risk to define how it wishes to incorporate possible adverse unexpected events — some of which **will** occur. Management (and directors) must decide how to deal with the risk/reward trade-offs implicit in a strategy and its implementation. Attitudes toward risk will affect which business activities the enterprise undertakes, and it will implement strategies only if it can limit risk inherent in a strategy to an acceptable level.

Exhibit 5-3
Enterprise Risk Management, Management Decisions, and the Internal Audit Function



*Hedging, derivatives, internal controls, insurance, pricing, diversification, joint ventures, and design/implement control activities.

In considering an approach to managing its risks, management addresses how external environment factors, internal (process) factors, and information about these factors, as well as how they combine and interact to shape the entity's overall risk position or "profile."

Event Identification

Given an understanding of an entity's objectives, strategy, and plans, along with consideration of current external and internal conditions, ERM requires identifying all of the important conditions (or events) that might occur that could adversely affect the achievement of the entity's objectives. This critical step requires knowledge of the entity as well as business in general, as well as the current and likely future environment, and how to link knowledge of various types. The identification step is critical because possible events not identified may **not** be addressed in planning responses and accepting risk, thus leading to unplanned exposures.

Risk Assessment

Risk is typically assessed along two dimensions — the **likelihood**, or probability, that a given adverse event will occur, and **impact** of the event on operations, financial reporting, and possibly strategy if the event does occur. Some risks are discrete (e.g., a $5,000,000 fine if judged to have violated an ordinance) and some are continuous with a range of possible results associated with an event, each with a likelihood of occurrence. Measures for likelihood are also discrete or continuous. Measures of potential impact may be in terms of possible disruption of operations, amounts, monetary loss, or impairment of strategy objectives.

Risk assessment across an enterprise requires a combination of qualitative and quantitative methodologies. Quantitative assessment is possible when sufficient data are available. Qualitative assessment methodologies may be used where potential likelihood and impact are low or where numerical data and expertise for quantitative assessments are not available. Qualitative assessments may also be used for high-impact events that require substantive expertise for assessment. Finally, no matter how the risk for individual events is assessed, many events tend to occur together. This leads to a need to consider the (joint occurrence) risk that two or more events will occur simultaneously.

Risk Response

An entity evaluates the risk/reward trade-off for each important risk. Depending on the trade-off, it can respond to risk by accepting, avoiding, or mitigating risk. Mitigation includes

sharing, transferring, or reducing risk (including control activities as discussed below) depending on the risk/reward trade-off, price, and the entity's risk appetite. Responses are integral components of ERM, but the specific response selected is not. As with choice of objectives and strategy, the choice made by local and top management is part of management's broader role. Responses are typically reviewed *ex post* for possible improvement, however.

Control Activities

Control activities are the policies and procedures designed by management to provide reasonable assurance that the chosen risk mitigation responses are implemented. Control activities are applied throughout the organization and include approvals, authorizations, cancellations, confirmations, observations, verifications, reconciliations, reviews of operating performance, physical security of assets, and segregation of duties. Internal auditors are familiar with control activities for financial reporting, and ERM extends the concept to responding to all risks.

Information and Communication

Risk identification, assessment, response, and control activities can provide necessary risk information at all levels of an entity. But like financial and other information, risk information must be communicated in a form and time frame that enables workers, management, and directors to carry out their various responsibilities. Because of the complex and subtle nature of risk information, communication may involve more than mere display.

Information systems for risk assessment can generate periodic and real-time exception-based reports that facilitate day-to-day decisions and longer term decisions. According to COSO, "Reports may include lagging or forward indicators, performance metrics, and operational or financial results." For ERM at the entity level, multiple data and information flows must be aggregated (and integrated) to communicate an overview on the entity's portfolio risk profile.

Effective communication involves downward flows (communicating management's plans and known risks to employees), parallel flows (personnel communicating production and distribution risks across departments), and upward flows (employees informing top management of surprises). Part of an effective ERM environment regarding communication is recognition by employees that risk management is to be taken seriously and that employees are expected to communicate significant risks upstream.

Monitoring

As with internal control, an entity monitors the effectiveness of enterprise risk management and its components through day-to-day monitoring activities and separate evaluations. Day-to-day monitoring (or "ongoing monitoring," in COSO terms) occurs in the normal course of business as events and transactions take place. It includes ordinary management and supervisory activities in conducting transactions. "Separate evaluations" of ERM may be based on either planned periodic examinations or follow-up of exceptions arising in operations or day-to-day monitoring. The IAF is often the preferred provider for separate evaluations of ERM because of internal auditors' competencies, skills, and experiences with independent investigation, risk assessment, and reporting.

IV. ERM Performance Monitoring by the Internal Audit Function

We now consider the IAF's risk assessment and risk management role in more detail and identify scholarly research opportunities. In particular, we outline the IAF's role in performance monitoring for each of the seven components of COSO's ERM model and list inherent assumptions, functions, and linkages that are open to questioning and could benefit from scholarly inquiry.

The Environment — Objectives, Strategy, and Risk

The managers and directors of an enterprise determine its objectives, strategies to achieve objectives, and a business model and business processes to implement strategies.[5] Core and supporting business processes facilitate strategy implementation with the entity's suppliers, workers, capital providers, customers, and competitors. Business measurement systems are designed to measure and display key success factors for achieving objectives as well as risks of events that might happen to impair success. The measurements facilitate planning and coordination of day-to-day activities, as well as subsequent evaluation of performance.

In addition to deciding what business to be in and strategies, models, and plans for the business, management and the directors decide how much risk they are willing to take in attempting to achieve their objectives. For some entities, management and the directors are willing to bear considerable risk because of high expected reward, either for the entity itself, or for related objectives. For other entities, management and the directors are unwilling to bear much risk. These attitudes toward risk can be called a "risk appetite." The appetite, then, is part of the environment for ERM in that it helps in evaluating important risks and deciding how carefully these risks must be identified, assessed, responded to, controlled, and monitored.

Overall entity risks implicit in a strategy and business plan provide an overall framework within which the other six elements of ERM operate. The objectives and risks appetite provide overall parameters for ERM. Risk assessments can provide a "risk profile" for periodic comparison with the "risk appetite" or limits the entity has set on residual risks (i.e., risk after response and control activities) it wishes to bear. The monitoring component is somewhat different from the others in that it may provide feedback to management and the directors when the assumptions implicit in the environment seem to have been violated by changes in the external environment or in the business processes of the firm. The overall environment must then be translated downward in the organization into risk management for sub-entities and segments of entities and time segments.

Information Technology, Risk, and the Environment

The ERM environment has become increasingly important in recent years due, in part, to changes in information technology and related developments. Information technology can communicate to all parties (including competitors) information about changes in the environment and has reduced the time available to react to environmental change. It has also streamlined and altered the design of business processes, and even changed the optimal form of organization for some enterprises. These developments have led to downsizing of businesses, automation of controls and communications, and fewer employees devoted to control activities. In turn, these changes affect the nature and magnitudes of risks faced. Furthermore, information technology allows operating efficiencies such as just-in-time materials arrival (eliminating materials inventory) and outsourcing of many support activities.

Information technology has changed the underlying assets and risks of businesses. An example is the risk of deterioration of market-based assets such as the value of a supplier network that effectively outsources production and inventory management and a customer base. Outsourcing reduces investment in equipment and labor but increases business risks when a key trading partner fails to perform. Customers depend on products and services that in turn depend on performance of suppliers. Managers need to know about the risk profile of trading partners and the risks unique to their failure to perform. The changes also alter the effectiveness of traditional controls over information and safeguarding of assets with many traditional recording and control activities automated in software. Automation also changes the focus of monitoring from detection and correction of errors to prevention of errors.

Research Questions

1. How can (should) management and the IAF systematically link entity strategies and business models to risks that threaten their achievement?

2. Should risk measures be formally incorporated into planning performance measurement and compensation? If so, how?

3. How do managers (directors and employees) interpret risk (and audit risk) reports?

4. Can risk templates help management and IAF develop an appropriate risk environment? If so, for which elements?

5. How does outsourcing of various functions change the risk environment and expose the entity to new risks?

6. How does information technology affect risk, risk assessment, and risk management?

Risk Event Identification

The approach to risk management outlined by COSO (COSO, 2002) is based on identification of possible risk events that could threaten achievement of objectives. Event identification is based on the **environment** and requires mapping the environment to possible risks.

Exhibit 5-4 diagrams ERM's risk assessment and control steps. It includes a column for the implicit insertion being made in the ERM process about the validity and accuracy of risks identified and managed. The remaining columns outline possible auditing procedures applied by IAF to verify the validity of the assertions. Thus, the auditing of risk assertions is parallel to auditing of financial statement assertions by financial auditors.

The first step in Exhibit 5-4 is the identification of *all* potentially serious risks. To manage risk for the company as a whole, a *complete* list of risks faced by the enterprise (or segment) is essential. Only from a complete list of potentially important risks (see *Ashby's Law of Requisite Variety* in Hare, 1967) can management be assured that threats to achieving its objectives are adequately assessed, reasonably contained, and economically managed.

Exhibit 5-4
Risk "Assertions" and Auditing Procedures for "Separate Evaluations" Monitoring of ERM Audits by IAF

ERM Component	Implicit assertion(s)	Separate evaluation monitoring procedure(s)
Environment	Objectives, strategy, and plans are reasonable given external environment and available resources; primary threats (risk events) have been considered.	Evaluate for reasonableness at the "Inherent risk" (pre-ERM) level and "residual risk" (after ERM) level.
Event Identification	All important risk events have been identified; completeness given. **Environment**; existence/ownership.	Independently derive all potentially important risks given. **Environment** using templates, analysis, linkage tools mapping strategy and business model to existing environment and business possesses.
Risk Assessment	Valid risk quantification given **Event Identification** (likelihood, impact).	Analyze/evaluate assumptions, calculation method; re-perform calculations, evaluate risk interactions (scenario building, joint occurrence, "worst case" scenarios).
Risk Response	Proper response given **Risk Assessment** and **Environment**.	Analyze/evaluate implicit risk/reward trade-off for reasonableness; evaluate counter-party risk for risk sharing/transferring/reduction responses.
Risk Activities	Control activities and cost effective **Risk Responses**.	Test effectiveness of response by analytical procedures and tests of details, assess value-at-risk, control activity effectiveness, and achieved risk (after **Risk Responses**).
Information and Communication	Risk information is effectively communicated on timely basis to appropriate persons.	Evaluate reporting system including distribution list (per **Environment**); test personnel understanding of risk reports and "red flag" exceptions.
Monitoring (ongoing or day-to-day)	Personnel execute appropriate monitoring of risks on a continuous basis.	Observation, exception review, decomposition of planned vs. recorded accountability.

Risk identification is a difficult task due to most individuals' lack of familiarity with business strategy and threats inherent in strategies and business planning. Internal auditors are often among those lacking familiarity. Of particular importance in risk identification is being *complete in the identification* — how can management or the IAF know that **all** important risks have been identified?

Study of business strategy concepts and practices can help management or the IAF identify some risks because there are many commonalities in business activities — what applies to one entity will typically apply in some form to another. Templates based upon various types of strategy or types of commercial activity can provide a checklist for risk identification. On the other hand, many new business ventures are undertaken because management sees a competitive advantage in following a strategy that does not emulate aspects of past strategies. For these situations, managers and the internal auditor must be innovative in determining any complete list of risks. For example, they might use activities such as "brainstorming" by various personnel with different backgrounds and expertise, and "scenario building" to generate ideas about possible threats. Neural networks have been explored as one way to exploit recognition of patterns in various data that can suggest possible risks as they develop (Ramamoorti and Traver, 1998).

A relatively new problem for risk assessment is assessing risks arising from outsourcing of business processes, including supply chain management. The problem arises because with outsourcing, entity personnel may not be intimately familiar with the operations of their supplier and thus not know what risks the supplier faces. In turn, the entity may not anticipate risk events that affect the supplier, which in turn affect the entity (Miccolis et al., 2000), for the different reactions of Ericsson and Nokia to a common supplier's disruption due to a hazard loss.

Research Questions

1. How does the inherent unobservability of second moment (variance or risk) vs. first moment (total or mean) affect risk assessments and how they are interpreted by management, personnel, and directors?

2. Can brainstorming and scenario building be used systematically to assist in identification of relevant risks for entities? If so, how should they be conducted?

3. How should covariation or joint occurrence of risk events be incorporated into risk assessments (e.g., conditional probability vs. joint probability)?

4. Do risk event identification techniques differ between hazard, operations, financial, strategy, and other risks?

5. How can IAF systematically audit completeness of risks of various types?

6. How can outsourcing risks be identified and measured?

7. Do risk templates that suggest consideration of specific types of risk limit IAF creativity in assessing completeness of risks (i.e., reduce "output interference")?

Risk Assessment

After all potentially important risks are identified, they must be measured as to their *magnitude* — the monetary loss or degree of adverseness if the event occurs — and the *probability* that an adverse event of a given magnitude will occur. Some events are catastrophic as to potential impact magnitude, but low in probability of occurrence, while other events have small loss magnitudes individually, but have high probability of occurrence and thus may be important in the aggregate. Determining the ultimate cause(s) or source(s) of each risk is important in seeking the best solution.

Risk events are yes/no conditions — either the event occurs or it does not. However, many events have different degrees of adversity associated with them. For example, the simplest case is possible loss of a fixed dollar amount. In many business activities, however, the amount may be a random variable (e.g., one may win or lose a lawsuit, but given loss of the suit, the damages could be one of a wide variety of possible amounts, each with its own probability of occurrence). Because risk is complex, the assessment of risk is also complex and so is the communication of those risk assessments.

One problem with ERM is how best to measure and communicate risks. The most common method in practice today is to assume or act as if there is a simple probability of the event and of a single magnitude. This method works well for discrete events, but not necessarily for continuous events. Risk of events can be assessed as a probability density function, as the expected value of the loss event, or as the risk of loss of a given magnitude or higher. Each has its advantages and limitations, and each is best for certain scenarios. A problem in ERM design is how to trade off measurement accuracy or "representational faithfulness" with understandability of risks.

Risks of events are often not quantifiable in objective terms such as numerical probabilities. To deal with this difficulty, subjective probability phrases are used to characterize ranges of

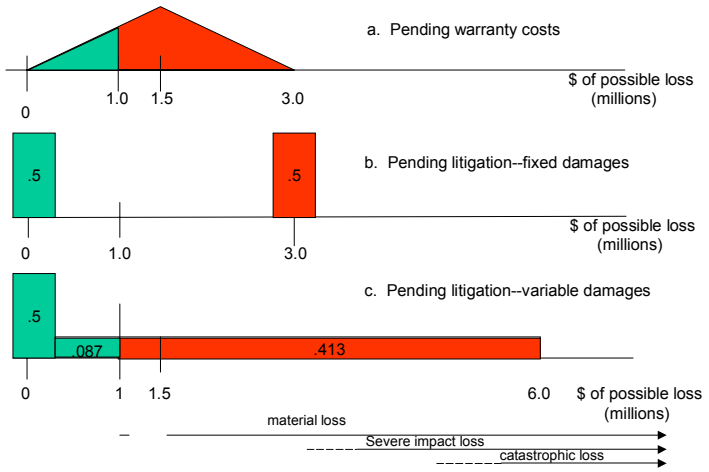
probabilities. For example, the FASB in SFAS No. 5 defines an event as "probable" if it is "likely" to occur, and "reasonably possible" if it is more than remote but less than likely. Unfortunately, the terms have different meanings in different contexts and in the same contexts across different parties.

Surveys of auditors, investors, bankers, and managers have determined broad borderlines for the phrases in terms of probabilities. These parties typically view the borderline between remote and reasonably possible as about .2, and the borderline between reasonably possible and probably as about .7, with considerable variation around these borders across individuals and contexts (Amer, Hackenbrack, and Nelson, 1995). Auditors as a group tend to view the threshold values lower than do managers, with financial statement users in between the two.

Three Loss Distribution Examples

Exhibit 5-5 shows some loss possibilities under three probability distributions. All three distributions have an expected cost equal to $1.5 million. In case A, which might represent the future warranty expense distribution, the point estimate of expense is $1.5 million, with a triangular distribution of possible values around the best estimate and well over half the distribution to the right of $1 million — an important or "material" amount.

Exhibit 5-5
Three Loss Distributions



Kinney, W.R., *Information Quality Assurance and Internal Control for Management Decisions* (Boston: Irwin McGraw-Hill, 2000). Reproduced with permission of The McGraw-Hill Companies.

Cases B and C, which might describe pending litigation, each have .5 probability of zero loss, but different positive loss probabilities. In case B, zero loss is as likely as a loss of $3 million, with no other possibilities. For case C, a zero loss has a .5 probability, and losses of $1 through $6 million are possible and equally likely. While cases A, B, and C have equal expected losses, they differ as to the maximum possible loss and the likelihood of a loss greater than or equal to $1 million. Case A has the highest probability that the loss will equal or exceed $1 million, but the lowest probability that it might have a severe or catastrophic impact on the operation of the entity. If $1 million is the smallest "material" amount, then case C has the highest probability of immaterial loss, but also has substantial risk of possibly catastrophic impact on the operations.

How would you evaluate these risks? Case A is almost certain to result in some loss, while cases B and C are "as likely as not" to have zero loss. For cases B and C, the likelihood of at least a material ($1 million) loss is more than "remote," but less than "probable" in each case. While management facing case C might argue that the .413 probability of a loss equaling or exceeding $1 million is remote, others might believe it to be important because there is a .25 probability of a loss of $1 million to $6 million. The latter might be considered a "severe impact" or even "catastrophic impact" loss. The reasonable possibility of catastrophic impact loss would be important when evaluating risk and risk disclosure under the AICPA's SOP No. 94-6 *(*adapted from Kinney, 2000, pp. 235-238).

Another risk assessment problem is possible biases of the risk evaluator. In particular, bias may arise because of differences in background and training of the evaluator, and from the position that the evaluator holds. For example, experts may be better at assessing risks than are novices or those not trained in risk. Also, an employee may consider a particular event likelihood (or loss magnitude) related to his or her area of responsibility to be low because a high assessment may imply poor performance of the employee. A supervisor or the IAF may view the same risk as much higher.

An important set of research questions for ERM is the effect of behavioral biases identified in other areas of research apply to risk assessments and auditing of risk assessments. As examples, prior research in accounting has identified biases such as "anchoring and adjustment," "output interference," "recency," and others (see Shrand and Elliott, 1998, pp. 277-278, for examples of behavioral biases affecting financial judgments).

Research Questions

1. How should risk assessments be expressed (e.g., probability density functions, Low-Medium-High, narratives, subjective probability phrases vs. objective measures, expected value vs. maximum loss, univariate vs. multivariate or configural, discrete vs. continuous)?

2. How do behavioral biases affect risk assessments by employees vs. managers vs. directors vs. IAF?

3. Are there behavioral biases (such as "anchoring and adjustments," "output interference," and "recency") affect IAF's audit of risk assessments by others vis à vis vs. independent origination of assessments by IAF?

4. What should be the standards for risk assessments that are "decision influencing" vs. "decision facilitating" (i.e., *ex ante* vs. *ex post*)?

Risk Response (Risk/Reward Trade-off)

For each potentially important risk identified and assessed, the risks versus reward trade-off is evaluated. ERM response partitions risks into three risk/return categories. Some risks are of a magnitude and probability that the risk/reward relation is acceptable at its present level. These risks are simply accepted. Other risks are of such large magnitude or probability that they are unacceptable and cannot be economically contained, thus exceeding the entity's risk appetite. These risks must be eliminated by avoiding exposure to risk through abandoning the project, or by preventing risk at the source (e.g., adopt nonpolluting technology, or filter out pollutants at point of production).

Still other risks, probably most risks, *may* have acceptable risk return/reward trade-offs, but not without some actions by management. Some risks may be transferred to others through insurance, hedging, or derivatives, or shared via joint ventures, alliances, and pricing (i.e., charging customers for the risks assumed by the firm). Risk transfer and sharing does not eliminate risk, but reduces it by changing its form. For example, a variable for fixed interest rate swap based on the London Interbank Offered Rate (LIBOR) allows a firm to exchange interest payments from a variable rate loan with fixed payments of another party holding a fixed interest loan, thus eliminating variable interest rate risk. However, the arrangement introduces a counter-party risk that the other party will fail to fulfill its contract.

Control activities (see next section) may limit these risks such that an unacceptable "inherent risk" (risk before control activities are applied) is transformed into a "residual risk" (after application of control activities) that is acceptable. Similar risks exist in varying degrees for insurance, hedging, joint ventures, and alliances. Each of these exposures creates a potential demand for assurance about the ability of the counter-party to fulfill its obligations.

Research Questions

1. How can IAF monitor the performance of risk responses (i.e., assess the reasonableness of response)?

2. How should IAF evaluate counter-party risk in monitoring risk response?

3. How can (should) risk response be linked to the risk appetite of the entity?

4. Can auditors obtain the skills necessary to evaluate responses to risk such as hedging, insurance, and derivatives? If so, how? (See Chapter 6 of this monograph.)

Control Activities

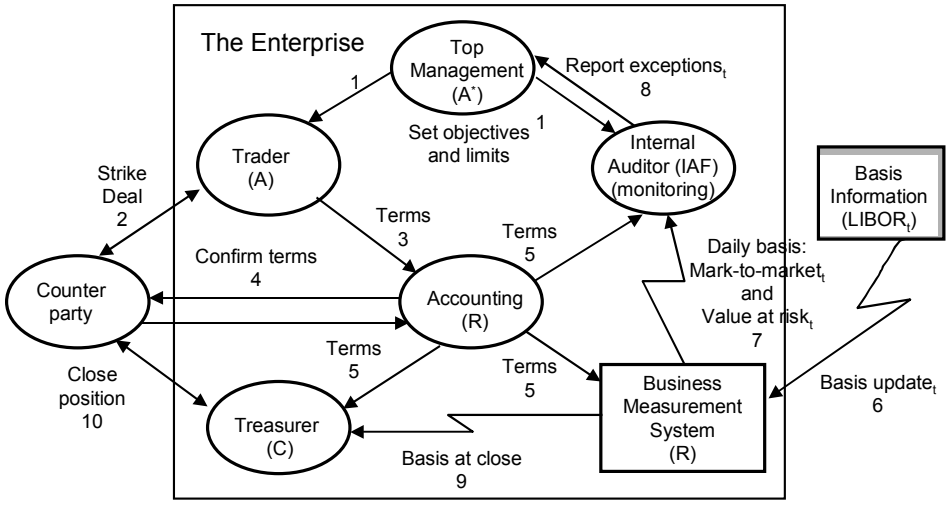
Many risks may be mitigated by the design of business processes that limit or otherwise reduce the likelihood or magnitude of risks faced. Many of the internal control procedures or control activities for control of transactions and asset protection are examples of business risk control activities. Some activities are themselves complex and require technical expertise in risk and risk management.

Derivatives are a widely used mechanism for managing some types of risk. Derivatives have also led to multimillion-dollar losses and even failure of large commercial and financial institutions. The next example shows how separation of traditional control activities can be used to mitigate risk for a derivative based on an interest rate swap.

A Derivatives Control Activities Example

Exhibit 5-6 shows five parties within the firm, the outside (counter) party with whom interest payments are exchanged, and the underlying basis information and the value of the London Interbank Offered Rate of Interest (LIBOR) that fluctuates over time. Top management sets objectives for derivatives using the swap and sets limits on risk exposure (operationalizing "risk appetite"). These objectives and limits (part of the environment) are communicated to the trader (in the finance department) authorized to negotiate derivatives and to IAF that monitors performance of the process (see arrows labeled 1 in Exhibit 5-6).

Exhibit 5-6
ERM for Derivatives



* A – authorization, R – recording, C – asset custody

Kinney, W.R., *Information Quality Assurance and Internal Control for Management Decisions* (Boston: Irwin McGraw-Hill, 2000). Reproduced with permission of The McGraw-Hill Companies.

The trader negotiates terms of the swap with an outside counter-party (arrow 2), and communicates terms of the transaction (information and communication) to accounting personnel (arrow 3), who independently confirm terms (ongoing monitoring) with the counter -party (arrow 4). Accounting then records the terms and thus informs the treasury department, the internal auditor, and the business measurement system will then obtain access to LIBOR and calculate the value of the derivative position and the value at risk on a daily basis (arrow 6).[6]

IAF monitors the derivative portfolio position by comparing its measured value against the objectives and limits set by top management (arrow 7). If the limits are exceeded, the IAF reports the breach to top management for a decision about follow-up actions (arrow 8). When the swap position comes due or is to be closed, treasury department personnel (cash custody) calculate the settlement amount and transfer or receive cash to settle the position (arrows 9 and 10).

Information technology and complex calculations are used to measure the value and value at risk of derivative financial instruments. However, the control activities still apply and allow control. Specifically separation of authorization for objectives and limits from authorization for day-to-day-trades, and independent confirmation and recording of transaction terms, independent measurement for monitoring, and settlement allow management of risk and protection of company assets (adapted from Kinney, 2000, pp. 104-106).

Research Questions

1. How can traditional auditing procedures for control activity compliance and substantive tests (analytical and details) be adapted for monitoring risk control activities?

2. How can information technology be used to assist IAF monitoring of risk control activities?

3. How can internal auditors become sufficiently knowledgeable to audit the efficacy of responses to complex derivatives and joint outcome possibilities?

4. To what extent can (or should) IAF rely on outside experts to evaluate controls over risk?

Information and Communication

Several parties within an enterprise create demand for relevant and reliable information about risk assessments and risk management processes. Management wants to inform itself and to be able to credibly inform others that management is carrying out its fiduciary and legal responsibilities. Management also wants workers to be appropriately informed about risks that workers face and to inform management about exceptions noted in day-to-day operations. Audit committees and outside directors exercising oversight responsibilities would be comforted by assurance that risks are being managed adequately and could use IAF's assurance reports as evidence that they have carried out their oversight responsibilities.

Information about risk can be displayed within the organization using information technology and periodic internal reports. But how can management and directors be assured that risk and risk process information is being effectively communicated? Communication effectiveness also requires understanding of what displays mean regarding the possible internal and external environments as well as what the information implies for the enterprise's business processes and strategy.

The IAF can verify that displays are accurate and timely and are made available to the proper parties. In evaluating users' understanding (communication effectiveness), the IAF may need to review educational programs for employees as well as evaluate techniques for display of risk information. As an example of interpreting what risk displays mean, the IAF may need to use experts to test employees' comprehension of risk reports and consider conducting research to determine the most effective form of display such as graphs, probability phrases, odds, or outcome trees.

In addition to those with direct responsibility for design and implementation of ERM, others also have an interest in being informed about risk and risk management. Suppliers, customers, and workers would like assurance about entity risk and risk management processes because of the effects on their future welfare in dealing with the entity. Also, investors and creditors, prospective investors, and regulators charged with regulating businesses would like such assurance as a means of reducing information surprise and asset loss.

All of the parties above have an interest in risk and risk mitigation processes and want to be assured that a high quality risk management is in place. However, they differ in their demand for details because they differ in their abilities to act upon knowledge of particular risk exposures. Thus, reports on risk assessment and risk management take on different meanings for different groups, and require consideration of trade-offs. Because the IAF is part of the entity, attestation by the IAF has limited value in reporting on ERM to outsiders. However, an effective IAF is an integral part of management's assertion to outsiders that it has effective ERM. Also because the internal auditor is part of the entity, the IAF faces potential barriers in reporting on performance of top management to independent directors of the enterprise. The basic issue is the efficacy of communication that is essentially reporting poor performance by one's own boss.

Communication of risk and risk assessments are also somewhat more difficult because of several barriers. These include the lack of (a) adequate criteria for measuring risk assessment and risk management quality, (b) adequate criteria from separating bad risk assessments and processes from bad decisions and bad outcomes, (c) adequate methods for auditing risks and processes, and (d) a reporting regime to accommodate differing users and uses while protecting the interests of management, the entity as a whole, and the internal auditor. Some of the communication barriers can be overcome with improved procedures for auditing risk as described in this chapter. Also, some barriers can be overcome with differentiated reporting (Kinney, 2000). Other barriers remain, however.

Research Questions

1. To whom should particular risk or risk process information be communicated — management, other personnel, audit committee, board of directors, regulators, trading partners, outsiders?

2. When is information about processes (rather than risk measurements) sufficient (or preferred) communication?

3. How should risk assessments be presented to maximize understanding — probabilities, subjective phrases, graphs, integrate with financial reporting?

4. Can the IAF reliably communicate management failure to manage risk to independent directors?

5. Under what conditions can IAF monitoring and ERM attestation have value to those outside the enterprise?

6. What liability do directors, management, and IAF face with respect to risk audits and reports?

Monitoring Risk

The last component in ERM is continued monitoring for unexpected conditions and changes in conditions. We've discussed several risks auditing procedures at each prior step and won't repeat them here. We will consider an integrative analytical tool (decomposition) that has considerable power in risk monitoring and is well suited to application by management accountants in risk assessment and by the IAF in monitoring risk. Finally, we will explore whether the focus of ERM and the IAF's efforts should be risk assessments or the *process* that generates risk assessments.

Comparison of recorded performance from the business measurement system with expected performance via plans and budgets, and contemporaneous performance of competitors is a powerful way of monitoring for changes in the risk environment. Differences from expectations can be explained as to cause, or "sourced," and may point to changed environmental or business process conditions outside the limits suggested by prior risk analyses. Relevant timely measurements and decomposition as to cause allow timely reaction by management.

Monitoring for changes in risks already identified can also lead to sensing new risks and changes in the risk environment. Companies that are dealing with present risks adequately may be unprepared to deal with an environmental change that presents new risks that may threaten the continued existence of the firm.[7]

One way to monitor ERM performance is by comparing end-of-period operating data with that planned at the beginning of the period. LJ Appliances, Inc. illustrates this decomposition to assess risk management performance.

A Decomposition Example: LJ Appliances, Inc.

LJ Appliances, Inc. operates a chain of appliance stores throughout the Midwest. Its strategy is to be the lowest cost source of refrigerators to final consumers, a strategy that management believes should yield a 10 percent market share. Based on information available at the start of the first quarter of 2000, LJ Appliances' sales management planned to sell 10,000 refrigerators chain-wide. The plan was based on an aggregate demand forecast of 100,000 refrigerators for LJ's trade area and a target market share of 10 percent. Their planning model was simply aggregate demand times .1.

Recorded sales units for the first quarter were 9,650, for an aggregate difference between planned and recorded performance of 350. LJ's internal auditor's investigation of the difference revealed the following:

- A tornado destroyed LJ's Tulsa store, resulting in the loss of 250 planned sales.
- Aggregate demand of refrigerators in LJ's trade area was 5 percent higher than the amount predicted at the start of the first quarter.
- A new competitor takes refrigerator orders via the World Wide Web and ships from a central warehouse in Des Moines. The company was unknown prior to the start of the quarter, but is estimated to have sold 4,200 units (a 4 percent market share) in LJ's trade area during the quarter.

There are many ways to decompose these conditions. LJ's internal auditor prepared the following summary:

Planned unit sales as of start of quarter (100,000 x .1)	10,000
Information error ((105,000 – 100,000) x .1)	500
Strategy assumption error (unanticipated competitor type) (105,000 x .04)	-420
Chance event (Tulsa tornado)	-250
Revised planned unit sales	9,830
Recorded unit sales for quarter	9,650
Unexplained difference	-180

Based on this decomposition, LJ's management could decide what it meant for performance evaluation in operations, planning, and information sources.

Here are the results.

- Management decided that since information about aggregate demand was off by only 5 percent, it was not cost-effective to try to improve the aggregate prediction process.

- Except for the new competitor and the tornado, LJ achieved about a 10 percent market share, so the business model seemed acceptable.

- Tornadoes and other natural disasters occur with some regularity worldwide but are not predictable as to locality or timing. The Tulsa tornado was judged unlikely to affect planning of future sales, although it did cause management to consider whether insurance was needed to mitigate the hazard risk.

- The presence of a new type of competitor had a small impact the first quarter, but might have a large impact in the future. Further analysis showed that the new

competitor's sales came disproportionately from LJ's — possibly as many as 840 sales units were lost by LJ. Reconsideration of LJ's strategy was appropriate. It decided that it must either enter the Web-based market or change its expectations and prediction model by lowering LJ's planned market share.

- The unexplained difference of -180 units could be due to error in implementing the first quarter plan, error in measuring units sold, or a large number of other causes. Given the relatively small effect of these unexplained causes in the aggregate and the cost of further investigation as to cause(s), LJ management decided to ignore them for this period and in planning for the future.
  (Adapted from Kinney, 2000, pp. 28-29)

In the LJ Appliances example, we see that decomposing historical differences from expectations can be used to evaluate performance and the risks of environmental change, as well as the risk of accounting errors and fraud. In particular, decomposition allows insight into the causes of any deviations and suggests follow-up actions. Decomposition may allow isolation of differences as measurement error in recording, chance events, implementation error (plans misunderstood or carelessly implemented by employees), poor information for planning, and a flawed business model. It may also suggest that long-term strategy needs alteration.

As to reporting IAF risk monitoring results, there are inherent difficulties in measuring and communicating risk information. When top management is the recipient of the IAF report, risk monitoring by the IAF is otherwise essentially similar to other internal auditing. However, when the performance of top management regarding ERM is ineffective, the internal auditor may face exceptional difficulties in communicating this finding to the independent directors. Part of the difficulty is due to the subjective and complex nature of risk — it is hard to be sure about risk mismanagement. Another part is the inherent dependence of risk conclusions on the parameters set by management, including the choice of strategies. In a sense, the internal auditor must "second guess" the wisdom of strategies and enterprise risk appetite choices in deciding whether ERM performance by top management is poor enough to warrant reporting. The uncertainties and hazards faced may make it impracticable for the IAF to communicate top management's failure at enterprise risk management.

Finally, it is useful to consider two issues that transcend ERM components. One is the ERM role of IAF in smaller organizations. In particular, for organizations that are too small to employ a chief risk officer (CRO), the internal auditor may, by default, serve as the CRO. In some ways, this may be a good choice for the organization. The internal auditor has broad experience in business and the risks that a business faces. On the other hand, the internal

auditor has other duties that may make timely risk assessment hazardous. Also, the internal auditor may be unable to function as CRO in identifying, assessing, and responding to risk, and perform the monitoring of ERM for the same organization. The extent to which one can reasonably review one's risk assessments may be more hazardous than auditing accounting records that one has prepared.

The other issue that transcends ERM components is whether the focus of IAF should be on risk assessments or the process that generates risk assessments. For example, should the IAF audit particular risk assessments as of a point in time or audit the risk assessment process? The question is parallel to whether one should audit the temperature of the nuclear power reactor in Springfield, or whether the dials on the control room panels are able to display the temperature in real time, across time. The answer is probably — both. Some *ad hoc* risk assessments are sufficiently important at a particular point in time that management would like to have assurance about the particular assessment as of a particular time. Other recurring risks are sufficiently important on a continuing basis that management would like to have assurance that the risk measurement system will capture and promptly display risk information in real time.

A related question is the degree of comfort than can be taken by recipients of IAF monitoring reports. Again, the answer is mixed. Process information may give comfort because the recipient has assurance that a valid measurement process is in place on a continuing basis — and the particular display doesn't need auditing because of confidence in the process. Likewise, when the potential impact of occasional risk events warrants the effort, assurance about the magnitude and likelihood of the risk can provide comfort that is cost effective.

On balance, then, the role and allocation of IAF monitoring effort remains an open question and one that requires further experience, thought, and research.

Research Questions

1. When auditing ERM performance, how can IAF decompose *bad risk assessment* from *bad information*, *bad decisions*, and *bad outcomes?*

2. How can directors evaluate IAF performance in risk assessment and risk auditing?

3. How best to *audit* risk assessments or risk assess processes — i.e., what approach or procedures and what skills should IAF possess? (See Chapter 6 of this monograph.)

4. What are the comparative advantages of IAF for risk assessment (systematic exams, reporting skills, independence, broad experiences, and skills)?

5. How does entity size change the role of IAF (e.g., risk assessment vs. risk audits)?

6. Should IFA report on risks *per se* vs. risk management process?

7. What does a risk process report imply about risk assessments at a particular point in time?

8. What are the limits on IAF for monitoring in ERM, and how do the designated roles and responsibilities of management and the board of directors affect these limits?

9. What adds value to risk services by IAF (measurement/completeness/process assurance/second look/objectivity)?

V. Conclusion

The engagement risk management approach outlined in COSO (2000) generalizes the COSO approach to internal control for risk. The seven components of ERM provide a conceptual framework for addressing threats to an organization achieving its stated objectives. ERM holds considerable promise as a systematic way of addressing risk management.

The role of the internal audit function as envisioned by ERM holds great potential for valuable service by internal auditors. In this chapter, we have attempted to address some of the questions about the ability of internal auditors to fulfill this role. The questions have purposely been left at a fairly general level so that the reader must think creatively about how to address the basic issues. In a new and exciting area such as risk and risk management processes, creativity in developing new and broad-based solutions should be encouraged.

VI. Appendix I: Chapter Research Questions

The Environment

- How can (should) management and the IAF systematically link entity strategies and business models to risks that threaten their achievement?
- Should risk measures be formally incorporated into planning performance measurement and compensation? If so, how?
- How do managers (directors and employees) interpret risk (and audit risk) reports?
- Can risk templates help management and IAF develop an appropriate risk environment? If so, for which elements?
- How does outsourcing of various functions change the risk environment and expose the entity to new risks?

Event Identification

- How does the inherent unobservability of second moment (variance or risk) vs. first moment (total or mean) affect risk assessments and how they are interpreted by management, personnel, and directors?
- Can brainstorming and scenario building be used systematically to assist in identification of relevant risks for entities? If so, how should they be conducted?
- How should covariation or joint occurrence of risk events be incorporated into risk assessments (e.g., conditional probability vs. joint probability)?
- Do risk event identification techniques differ between hazard, operations, financial, strategy, and other risks?
- How can IAF systematically audit completeness of risks of various types?
- How can outsourcing risks be identified and measured?
- Do risk templates that suggest consideration of specific types of risk limit IAF creativity in assessing completeness of risks (i.e., reduce “output interference”)?

Risk Assessment

- How should risk assessments be expressed (e.g., probability density functions, Lo-Med-Hi, narratives, subjective probability phrases vs. objective measures, expected value vs. maximum loss, univariate vs. multivariate or configural, discrete vs. continuous)?

- How do behavioral biases affect risk assessments by employees vs. managers vs. directors vs. IAF?

- Are there behavioral biases (such as "anchoring and adjustments," "output interference," and "recency") that affect IAF's audit of risk assessments by others vis à vis vs. independent origination of assessments by IAF?

- What should be the standards for risk assessments that are "decision influencing" vs. "decision facilitating" (i.e., *ex ante* vs. *ex post*)?

Response

- How can IAF monitor the performance of risk responses (i.e., assess the reasonableness of response)?

- How should IAF evaluate counter-party risk in monitoring risk response?

- How can (should) risk response be linked to the risk appetite of the entity?

- Can auditors obtain the skills necessary to evaluate responses to risk such as hedging, insurance, and derivatives? If so, how? (See Chapter 6 of this monograph).

Control Activities

- How can traditional auditing procedures for control activity compliance and substantive tests (analytical and details) be adapted for monitoring risk control activities?

- How can information technology be used to assist IAF monitoring of risk control activities?

- How can internal auditors become sufficiently knowledgeable to audit the efficacy of responses to complex derivatives and joint outcome possibilities?

- To what extent can (or should) IAF rely on outside experts to evaluate controls over risk?

Information and Communication

- To whom should particular risk or risk process information be communicated — management, other personnel, audit committee, board of directors, regulators, trading partners, outsiders?

- When is information about processes (rather than risk measurements) sufficient (or preferred) communication?

- How should risk assessments be presented to maximize understanding — probabilities, subjective phrases, graphs, integrate with financial reporting?

- Can the IAF reliably communicate management failure to manage risk to independent directors?

- What liability do directors, management, and IAF face with respect to risk audits and reports?

Monitoring

- When auditing ERM performance, how can IAF decompose *bad risk assessment* from *bad information*, *bad decisions*, and *bad outcomes?*

- How can directors evaluate IAF performance in risk assessment and risk auditing?

- How best to *audit* risk assessments or risk assess processes — i.e., what approach or procedures and what skills should IAF possess? (See Chapter 6 of this monograph.)

- What are the comparative advantages of IAF for risk assessment (systematic exams, reporting skills, independence, broad experiences, and skills)?

- How does entity size change the role of IAF (e.g., risk assessment vs. risk audits)?

- Should IFA report on risks *per se* vs. risk management process?
- What does a risk process report imply about risk assessments at a particular point in time?
- What are the limits on IAF for monitoring in ERM?
- What adds value to risk services by IAF (measurement/completeness/process assurance/second look/objectivity)?

Footnotes

[1]Internal control examination and reporting requirements and experiences differ around the world (see Miccolis, 2000, and Harrington, 2002a).

[2]Others are Miccolis et al., 2000, and Armour, 2000.

[3]Adapted from EIU, *Managing Business Risk*, pp. 87-91.

[4]According to COSO (2002:8), "ERM expands and elaborates on those elements of internal control relevant to enterprise risk management."

[5]For discussion of the relation of business models and processes to strategy and objectives, see Magretta, 2002.

[6]Daily calculation of value of position and value at risk may not be needed for a simple swap, but the valuation of a portfolio of derivatives, hedges, and positions taken can be complex and warrant daily measurement and monitoring.

[7]Two subtle but pervasive risks are the risks of failure to maintain the organization's capacity to identify and exploit opportunities (Criteria of Control (CoCo), CICA, 1995, para. 7), and risk of failure to maintain the organization's resilience or capacity to respond and adapt to unexpected risks and opportunities.

References

Amer, T., K. Hackenbrack, and M. Nelson, "Context-Dependence of Auditors' Interpretations of the SFAS No. 5 Probability Expressions," *Contemporary Accounting Research*, Fall 1995, 12: pp. 25-39.

Armour, M. "Internal Control: Governance Framework and Business Risk Assessment at Reed Elsevier," *Auditing: A Journal of Practice and Theory,* Supplement 2000, pp. 76-81.

Ashby, W.R., *Introduction to Cybernetics* (New York: Wiley, 1963).

Bodine, S.W., A. Pugliese, and P.L. Walker, "A Road Map to Risk Management," *Journal of Accountancy*, December 2001, pp. 65-70.

(The) Committee of Sponsoring Organizations of the Treadway Commission (COSO). *Enterprise Risk Management Framework Key Concepts Briefing Document*, (COSO: July 1, 2002).

DeLoach, J.W., *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity* (Financial Times Prentice Hall, 2000).

Hare, V.C. *Systems Analysis: A Diagnostic Approach*, (especially Chapter 6) (New York: Harcourt, Brace, and World, Inc., 1967).

Harrington, A., "Risk Goes Into Free Fall," *CA Magazine*, July 2002a, pp. 41-42.

Harrington, A., "Keep it Off Line," *CA Magazine*, July 2002b, p. 44.

Kinney, W.R., *Information Quality Assurance and Internal Control for Management Decisions* (Boston: Irwin McGraw-Hill, 2000).

Kinney, W.R., "Research Opportunities in Internal Control Quality Assurance," *Auditing: A Journal of Practice and Theory,* Supplement 2000, pp. 83-90.

Lam, J., "Enterprise-wide Risk Management and the Role of the Chief Risk Officer," *Erisk.com.* March 2000, pp. 1-5.

Lindow, P., and J. Race, "Beyond Traditional Audit Techniques," *The Journal of Accountancy*, July 2002, pp. 28-33.

Marquette, M., "Why Business Models Matter," *Harvard Business Review*, May 2002, pp. 86-92.

McNamee, D., and G. Selim, *Risk Management: Changing the Internal Auditor's Paradigm* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998).

Miccolis, J.A., K. Hively, and B.W. Merkley, *Enterprise Risk Management: Trends and Emerging Practices* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 2000).

Office of Government Commerce, *Draft Guidelines on Managing Risk* (London: Office of Government Commerce, 2001).

Ramamoorti, S., and R. Traver, *Using Neural Networks for Risk Assessment in Internal Auditing: A Feasibility Study* (Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation, 1998).

Schrand, C., and J. Elliott, "Risk and Financial Reporting: A Summary of the Discussion at the 1997 AAA/FASB Conference," *Accounting Horizons*, September 1998, pp. 271-282 (especially pp. 277-278).

Acknowledgments: The helpful comments of Andy Bailey, Audrey Gramling, Rashad Abdel-Khalik, and Sri Ramamoorti are gratefully acknowledged.