

ERM-BASED

Internal audit can play a key role in enterprise risk management, providing assurance on ERM policies and procedures without compromising auditors' independence and objectivity.

AUDITING

GEORGE MATYJEWICZ and JAMES R. D'ARCANGELO

Internal auditing has received renewed attention since the recent corporate governance and accounting scandals here in the United States and in the 1990s in the U.K. The measures put in place to monitor corporate governance, i.e., monitoring financial controls, have now expanded to include total enterprise risk management (ERM). This provides an opportunity for internal audit to be more effective—to provide assurance and perhaps consulting roles for ERM-based auditing without risking internal auditors' independence and objectivity.

Providing assurances on ERM

One of the key requirements of the board is to gain assurance that risk management processes are working effectively and that key risks are being managed to an acceptable level. It is likely that assurance will come from different sources. Management provides the first level of assurance. This should be complemented by the provision of objective assurance, for which internal audit is a key source. Other sources include external audit and independent specialist reviews.

Internal audit will normally provide assurances in three areas:

- risk management processes—both their design and how well they are working;
- management of those risks classified as “key,” including the effectiveness of the controls and other responses to them; and
- reliable and appropriate reporting and classification of risks.

Prior to the development of ERM processes, a typical internal audit department performed audit planning by its own assessment of risk based on factors such as its perception of inherent risk for the auditable entities as defined by the department. Factors that went into this evaluation included the results of the prior audit, changes in operations, mandated frequency, and the like. This assessment was completed by internal audit, with possible interviews of responsible parties associated with the entities.

With effective ERM processes, management owns, assesses, and is the key provider of assurance on risk to the board. Management is responsible for continuously updating and monitoring its status. ERM

GEORGE MATYJEWICZ, Ph.D., is Managing Director of D'Arcangelo Software Services, distributors of Galileo and Magique in the Americas. He was formerly President/General Manager of a global digital currency company with customers in 190 countries and Chief E-Commerce Officer for a global giftware company where he experienced risk management issues first hand. He was also a Principal/Partner at a top-20 U.S. CPA/consulting firm. He is a frequent speaker, is regularly published as an expert on global business, finance, technology, and implementation, and writes and publishes E-Tailer's Digest online and in print, which reaches 50,000 retailers worldwide.

JAMES R. D'ARCANGELO, CPA, is the Managing Partner of D'Arcangelo & Co., LLP, a CPA and consulting firm with five offices in New York State. Mr. D'Arcangelo has over 35 years of experience in providing audit, accounting, tax, and information technology consulting and management advisory services to a variety of international and domestic clients. He has organized a division within the firm to help clients with their internal audit, risk management, and Sarbanes-Oxley compliance needs. Mr. D'Arcangelo is a frequent speaker on various information technology topics. He is a member of the AICPA and NYSSCPA, ISACA, the IIA, and ACUA.

infrastructure promotes the sharing of risk knowledge across the enterprise and makes it available transparently to internal audit. This information is now available to drive the audit planning process and to provide assurance on the process of ERM itself.

Research has shown that board directors and internal auditors agree that the two most important ways that internal audit provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the risk management and internal control framework is operating effectively.

David A. Richards, President of the Institute of Internal Auditors (IIA), in his closing comments at the IIA's Enterprise Risk Management and Control Self-assessment Conference in Las Vegas in September 2004, encouraged the audience by saying, "It couldn't be a better time to be in the internal audit profession," and challenged participants to advocate risk management processes within their organizations while keeping internal audit standards and basic principles at the forefront of their audit activities.

Internal audit has come a long way and has evolved through various cycles and paradigms.

History of internal auditing¹

The earliest "Statement of Responsibilities of the Internal Auditor," in 1947, described internal audit as "a control which examines and evaluates the existence and effectiveness of other controls" and included the internal auditor's objective to improve all types of operational performance. Internal audit was also defined as a service to management and dealt primarily with accounting matters. Thus from its earliest days internal auditing in theory has been associated with:

- operational as opposed to strategic matters;
- the existence and effectiveness of controls; and
- improving performance—which implies a forward-looking focus rather than historical reporting of true and fair accounts and concern

with "real" business rather than just accounting records.

In 1957 the statement referred to both accounting and other operations and in 1971 the reference was to "operations."

In 1978 the IIA published its first formal definition of internal audit:

An independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization. The objective of internal auditing is to assist members of the organization in the effective discharge of their responsibilities. To this end, internal auditing furnishes them with analyses, appraisals, recommendations, counsel and information concerning the activities reviewed.

In 1999 the IIA definition was radically updated to reflect changes in the work of audit departments and the unavoidable reality of outsourced functions:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

The Sarbanes-Oxley Act of 2002 forced senior executives to follow the path of establishing objectives, identifying risks that will prevent them from meeting those objectives, and establishing controls that will mitigate those risks, although it focused on internal controls over financial statement preparation and disclosures only.

The Sarbanes-Oxley Act mandated that organizations assess controls against a suitable framework, such as the original COSO report, *Internal Control—Integrated Framework*. The framework consists of three objectives categories—operations, financial reporting, and compliance—and five components: control environment, risk assessment, control activities, information and communication, and monitoring.

Internal audit had the daunting task of providing assurance to the board of directors, and in particular the audit committee, that management was in fact identifying risks and that the controls were mitigating those risks.

Sarbanes-Oxley compliance became a costly exercise for many. According to Gartner, large and midsize enterprises will spend

ERM
INFRASTRUCTURE
PROMOTES THE
SHARING
OF RISK
KNOWLEDGE
ACROSS THE
ENTERPRISE
AND MAKES IT
AVAILABLE
TRANSPARENTLY
TO INTERNAL
AUDIT.

at least \$2 million on Sarbanes-Oxley compliance through 2005.² Unlike the Year 2000 (Y2K) phenomenon, Sarbanes-Oxley compliance is an ongoing process. To ensure compliance, businesses must update and recertify their data on a quarterly and annual basis.

The Sarbanes-Oxley Act has also caused many boards of directors and executive teams to look at all the business risks they face—not just financial, but operational, social, ethical, and environmental. These organizations see that Sarbanes-Oxley-related expenditure as the beginnings of an ERM platform, which will help them meet ever-increasing and shifting regulatory demands.

What is ERM?

Simply put, ERM is based on the concept that risk is anything that gets in the way of meeting your objectives: from the corporate mission “macro” level, down to the sub-process/activity “micro” level. ERM is a structured, consistent, and continuous process across the whole organization for identifying, assessing, deciding on responses to, and reporting internally on opportunities and threats that affect the achievement of the organization’s objectives.

The board has overall responsibility for ensuring that risks are managed. In practice, the board will delegate the operation of the risk management framework to the management team, who will be responsible for completing the risk management activities. There may be a separate function that coordinates and manages these activities and brings to bear special skills and knowledge. Everyone in the organization plays a role in ensuring successful ERM, but the primary responsibility for identifying risks and managing them lies with management.

The benefits of ERM

ERM can make a major contribution towards helping an organization manage the risks to achieving its objectives. The benefits include:

- better decision making;
- greater likelihood of achieving corporate objectives;

- improved understanding of the key risks and their wider implications;
- greater management focus on the issues that really matter;
- fewer surprises or crises;
- heightened risk awareness;
- increased likelihood of change initiatives being achieved;
- more informed risk-taking and decision-making;
- improved earnings targets;
- lower earnings volatility;
- reduced governance risk;
- quantified risk tolerance;
- improved capital allocation;
- an external communication tool; and
- internal target setting.

A Canadian survey. Anne E. Kleffner, Ryan B. Lee, and Bill McGannon surveyed all members of the Canadian Risk and Insurance Management Society (RIMS) as a follow-up to the 1999 survey by the Toronto Stock Exchange entitled “Five Years to the Dey” (Dey Report of 1994). They supplemented their survey results with interviews with 21 of the respondents.³

When asked to list the greatest benefits of implementing ERM, respondents discussed such issues as the importance of consistency in risk retention limits, having a better handle on the transactional aspects of their risk management program, allowing them to see the benefit of coordinating risk management decisions, and permitting an overall reduction in risk. The bottom line was that risk managers saw ERM as an effective way to reduce overall costs by managing better and reducing risk.

A second benefit was the move toward a company-wide philosophy regarding risk management. Adopting an ERM approach was one way to align everyone with the same objective. As one person indicated, “Everyone becomes a risk manager.” This proactive mindset results in risk management permeating the entire company. Furthermore, if everyone buys in, better results are expected.

THE COSO ERM FRAMEWORK, WHICH BUILDS ON THE COSO INTERNAL CONTROL FRAMEWORK, EMPHASIZES THE IMPORTANCE OF IDENTIFYING AND MANAGING RISKS ACROSS THE ENTERPRISE.

A third benefit, one that results from a better understanding of the risks, is improved decision-making and greater comfort at the board level. This aspect of ERM is likely to become even more important as the focus on corporate governance continues to increase and the role of directors is put under the spotlight.

Improved communication was another benefit that risk managers described. ERM “forces divisions to talk and communicate” and helps to break down individual silos—each managing a different aspect of the company’s risk profile. This contributes to a better overall understanding of risk and facilitates the flow of information to senior management and the board.

An effective ERM solution will provide the board of directors and management with reasonable assurance that they understand the extent to which the entity is achieving operational and strategic objectives, preparing effective internally and externally published reports, and complying with applicable laws and regulations.

The COSO ERM framework

The COSO ERM framework, which builds on the COSO internal control framework,

emphasizes the importance of identifying and managing risks across the enterprise. The new report, *Enterprise Risk Management—Integrated Framework*, was released by COSO in September 2004.

As shown in Exhibit 1, the original COSO cube has three objectives categories:

1. operational objectives, which relate to effective and efficient use of the entity’s resources;
2. financial reporting objectives, which relate to the reliability of all the entity’s reporting to internal and external parties; and
3. compliance objectives, which relate to the entity’s compliance with applicable laws and regulations.

Its five horizontal components consist of: monitoring, information and communications, control activities, risk assessment, and control environment.

As the illustration in Exhibit 1 demonstrates, the COSO ERM framework expands on the original COSO internal control framework and adds a fourth category to the original three: strategic objectives, which relate to high-level goals, aligned with and supporting the entity’s mission. Its eight horizontal components consist of: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information & communication, and monitoring.

EXHIBIT 1 Relationship of the COSO Objectives and Components

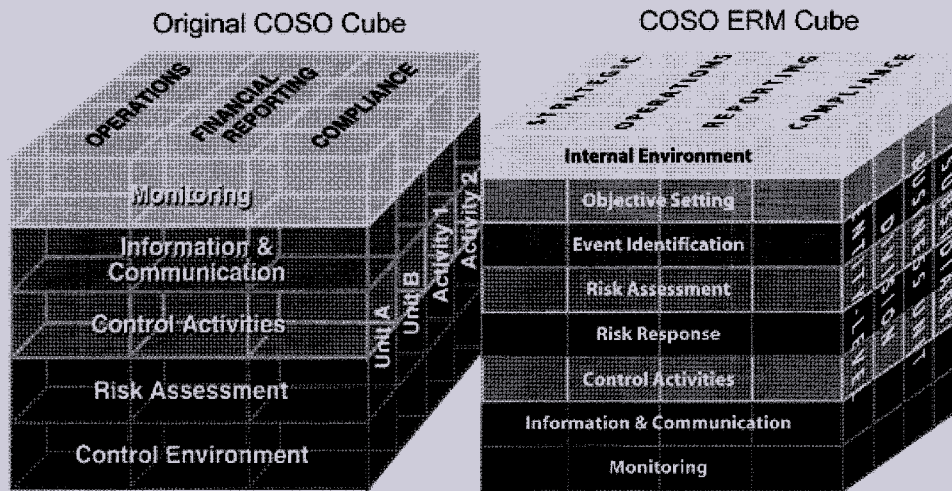
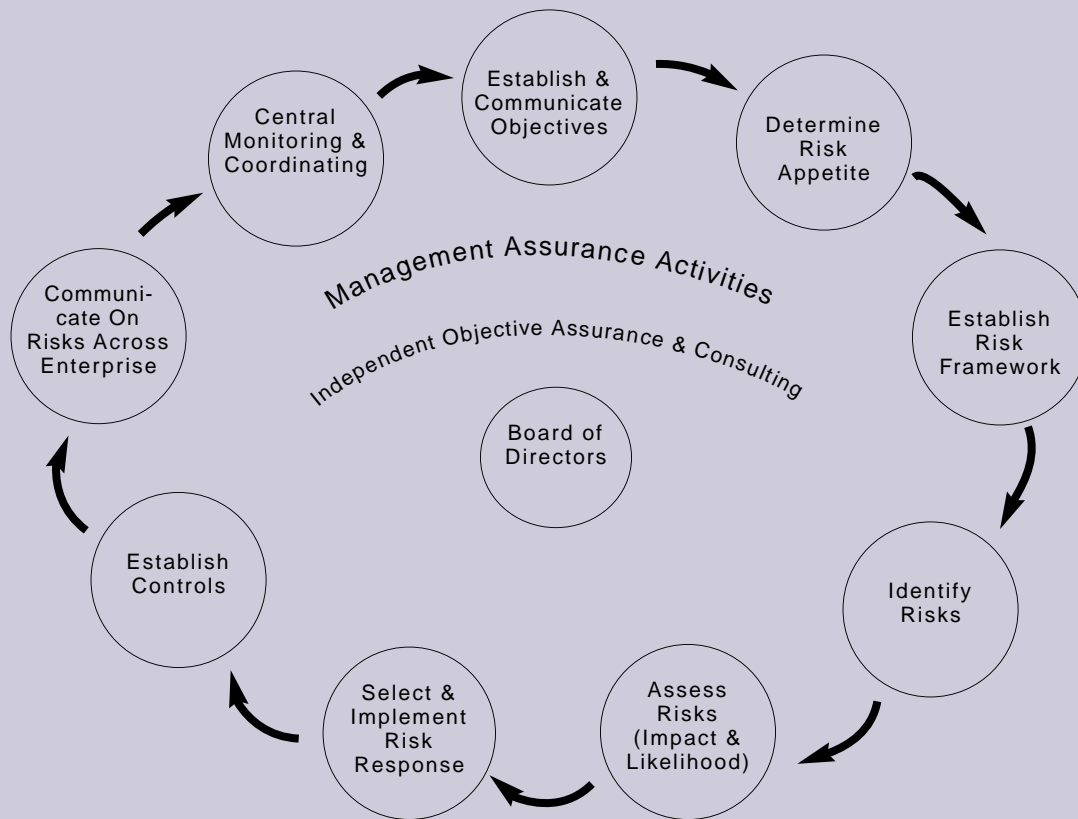


EXHIBIT 2 ERM-Based Auditing



tification, risk assessment, risk response, control activities, information and communications, and monitoring.

The objective of the COSO ERM framework is to aggregate and view risks from the top down in an organization. Authored by PricewaterhouseCoopers, the COSO ERM framework defines essential ERM components, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.⁴

Impact and value. David A. Richards opened the second day of the IIA Enterprise Risk Management and Control Self-assessment Conference by enlightening the general session audience on the global impact and value of ERM and control self-assessment (CSA). He asked internal audit professionals to pay attention to the basics of internal auditing responsibilities, including reviewing financial transactions, implementing fraud prevention and identification processing, and helping to ensure an orga-

nization's proper ethical climate. Describing an effective risk management process, Richards said internal auditors should serve as risk educators, participate in risk forums and risk management steering groups, and include detailed information about risk in all audit reports. He highlighted key ERM and CSA trends, including legislative movements around the world emphasizing the need for risk management as well as signs that internal auditors are becoming more proactive in the use of risk assessment processes. Although CSA has not been fully embedded in many organizations, he said, ERM is becoming known as a key ingredient to good governance, and internal auditors should promote its adoption and progression.⁵

ERM-based auditing

Now let's go beyond risk management and incorporate auditing into the paradigm. Combining ERM with auditing in an effec-

tive and seamless manner will yield ERM-based auditing, as illustrated in Exhibit 2.

Dr. Sarah Blackburn,⁶ one of the world's leading authorities on risk management, helped us identify the activities included in ERM-based auditing:

1. Establish and communicate the objectives of the organization.
2. Determine the risk appetite of the organization.
3. Establish an appropriate risk management framework.
4. Identify risks or events that will prevent management from meeting its objectives.
5. Assess the impact and likelihood of the risk occurring.
6. Select and implement responses to the risks.
7. Conduct control and other response activities that will mitigate the risks.
8. Provide information on risks and communicate in a consistent manner at all levels in the organization.

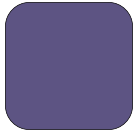
9. Provide central monitoring and coordinating of the risk management processes and the outcomes.

10. Provide assurance on the effectiveness of risk management.

11. Provide independent, objective assurance and consulting.

Establish and communicate the objectives of the organization. The organization's CEO identifies objectives and strategic alternatives—the vision for the success of the enterprise—and communicates those objectives to the enterprise as a whole. Each of the heads of the business units, divisions, and subsidiaries also identify their objectives, which must integrate with the enterprise objectives. The complexity of today's global business environment involves multiple stakeholders and collaborative decision-making. These individuals may be located in different geographic regions.

In ERM-based audits, internal audit will survey and plan audit procedures around the enterprise's and business units' stated



INTERNAL AUDITORS SHOULD SERVE AS RISK EDUCATORS, PARTICIPATE IN RISK FORUMS AND RISK MANAGEMENT STEERING GROUPS, AND INCLUDE DETAILED INFORMATION ABOUT RISK IN ALL AUDIT REPORTS.

objectives and strategies. The objective of the audit-planning process is to ensure that business objectives are effectively established and communicated throughout the organization. Internal audit reviews the goals and objectives of subsidiary operating units, ensuring that departments and individuals are aligned with the overall enterprise objectives. Internal audit defines its audit universe based on management's ERM process.

CSA exercises or audit procedures will be designed to evaluate the global understanding of objectives and goals. These would include interviews with key department personnel, and obtaining and reviewing published material, status reports, or other forms of evidence. Interim surveys could be conducted by issuing electronic questionnaires to different levels of personnel within each subsidiary and department. Questionnaires should provide space for comments by the respondent, so as to gather "soft" information about the staff's understanding of enterprise and department objectives.

Determine the risk appetite of the organization. What risks can the organization tolerate? Risks are those factors that could influence the achievement of business objectives, either positively or negatively. The nature of the risks will be related to the objectives under consideration. Strategic objectives are likely to be affected by high-level and wide-ranging risks and process-level objectives by risks that are more discrete and tangible. Dimensions of risk may include potential impacts on people, environment, and reputation, as well as financial or operating performance.

Internal audit will not set the risk appetite or tolerance. That is solely the role of the organization's board of directors and management. However, internal audit can provide assurance that tolerance levels have been determined, quantified, and communicated, and are effectively executed as to policy, procedures, and practices. Tolerance for enterprise spending limits for acquisitions, major projects, or new programs are to be reviewed and compared to actual results. Enterprise policies for authorization, allowable types of transactions, capital budgeting constraints, operating returns, and the like are cascaded through the organization and can

be evaluated as to conformity with strategic objectives.

Internal audit can provide assurance that management is performing within its stated boundaries for tolerances for financial thresholds, timescales for accomplishment of projects, and appetite for personal conduct, safety, and employee attitude.

Establish an appropriate risk management framework. COSO is rapidly becoming the de-facto standard for financial reporting risk management. In the SEC's final rule on management's reports on internal control over financial reporting, the SEC states, "The COSO Framework satisfies our criteria and may be used as an evaluation framework for purposes of management's annual internal control evaluation and disclosure requirements."

The board and senior management establish and manage an ERM framework. The new COSO ERM framework will most likely become the standard for ERM. Internal audit performs evaluations of entity-level and subsidiary-level implementation of the framework as to the congruence of the stated structure versus the actual structure. The framework will be documented and, in most cases, imbedded in a tool that will facilitate dynamic changes, monitoring, and management self-assessment. Internal audit will have access to the framework and will perform review and evaluation procedures to detect gaps in the structure and function of the framework. Management's support of this framework and its cultivation of corporate culture will be included as part of internal audit's scope of evaluation.

Identify risks or events that will prevent management from meeting its objectives. A risk is the possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. For example, Coca-Cola had as an objective to expand to new markets in Russia. The risks associated with that objective might include government issues, marketing risks, acceptance by customers, and delivery times. However, they learned that the most significant risk was discretionary spending power. The Russian people had limited discretionary spending money, which meant when another company entered the mar-

ket, the competition was for the limited pocketbook, and not the products. Management needs to identify potential events that could influence risk, either positively or negatively, and the probability of the events actually occurring.

In ERM-based audits, internal audit will study the risk universe and evaluate the inclusion of all significant risks. Risk definitions, categories, and other attributes will be examined to ensure that there is consistent application across the enterprise. Internal audit will review that risk identification at all levels links to the organization's overall objectives and strategies.

Tools employed will permit internal audit to detect gaps in the identification of similar risks when making comparisons by objectives across divisions and departments. Incomplete, inconsistent, and missing risks will be subjected to additional audit procedures and reporting.

Assess the impact and likelihood of the risk occurring. In addition to identifying risks, management also needs to identify the impact the risk will have on the organization and the likelihood that the risk will occur. The combination of impact and likelihood is a ranking of risks, and it behooves the organization to address those risks with high impact and likelihood.

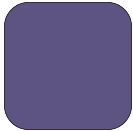
Internal audit is to provide assurance that risks are correctly evaluated. In the evaluation of the risk assessment process, internal audit will question the quality of management scoring of impact and probability, given the reality at hand. Examination of documentation and the process to determine gross inherent risk will be a standard procedure. Tools should track changes in gross risk over time, and internal audit should evaluate trends in its selection of areas to audit.

When evaluating inherent risk scores, comparisons to stated risk appetite should be made, with explanations requested from management. Analysis of risk by root cause, by category, and by objectives across the enterprise will help internal audit in its evaluation of management's scoring. Patterns such as lack of understanding of ERM and risk assessment on the part of management have further implications for internal audit's overall assessment of the ERM process.

Select and implement responses to the risks. Once the risks have been identified and ranked, the controls needed to mitigate them should be chosen, in the context of actions to contain risks to an acceptable level or to increase the probability of a desired

outcome. The strategy a company adopts to manage risks varies according to the organization's risk appetite. Risk management experts often summarize the options as treat, terminate, transfer, or take (or tolerate)—the four Ts.

Treating a risk means taking direct action to reduce either its potential impact or its



**INTERNAL
AUDIT
DEFINES ITS
AUDIT
UNIVERSE
BASED ON
MANAGEMENT'S
ERM PROCESS.**

likelihood of occurrence. In many instances the treatment is internal control.

To terminate a risk is to walk away from it. A company with a low risk appetite, faced with the risks of competition from the pocketbook, and not others offering the same products, may simply decide to source products elsewhere.

Risks may also be transferred to others, either by insurance or through contracts, often with outsourced service suppliers. It should be noted that the primary risk often remains with its original owner. If the right goods do not reach a retail store on time and in good condition, there may be a penalty clause that can be invoked against the logistics supplier, but it is still the supplier that loses sales and customer goodwill.

Finally, there are some risks that go with the territory. The organization must decide to accept, tolerate, or take them. Companies with high risk appetites that also have good risk management processes often reap the rewards of higher profits.

Some say there may be a fifth “T”—tomorrow. Many companies tend to put off until tomorrow what they should have done today, often with disastrous results.

Internal audit provides assurance on the risk management process, as well as the selection and implementation of risk response. Management documents its planning and decisions as to the most economical and effective means to mitigate the risks that stand in the way of achieving objectives. In their review of documentation and through interviews, internal auditors will seek answers to questions regarding management’s choice of singular or a combination of multiple strategies. Should a risk have been terminated, rather than taken, given the organization’s risk appetite and competencies?

Internal audit will review the process of risk management as to its evaluation of risk strategies given the possible interdependencies and correlations between business units and departments across the enterprise.

Net risk scores, taking into consideration employed strategy, will be evaluated by internal audit as to reasonableness. Overly optimistic managements may assign low scores to risks with otherwise high inherent risks. Management’s false reliance

on low risk scores, albeit recorded in error, or worse, intentionally, will be identified by internal audit as a serious flaw in the ERM process.

Conduct control and other response activities that will mitigate the risks. Once the risk response strategies have been selected, management must undertake control and other risk response activities. Management must test to ensure that the design and effectiveness of the controls and other response activities actually work.

Control and other response activities are affected by management’s choice of specific risk response strategies, and therefore have a bearing on which controls will be audited. It is important for internal auditors to gain an understanding of the design of controls and to evaluate their appropriateness in the context of the risk response choice. A risk response strategy that embraces operational attributes relates to how actions are to be performed, consistent with the organization’s direction and policies.

In its evaluation of security as a risk response, internal audit needs to test the effectiveness of physical and logical barriers, and the protection of information and access controls. A company treats risk by employing security, for that risk that it chooses to take.

Provide information on risks and communicate in a consistent manner at all levels in the organization. The risk team, in conjunction with internal audit, must communicate its findings of risk across the entire organization. Management needs to understand the risks that will prevent it from meeting its objectives, and what controls are in place to mitigate those risks.

Internal audit needs to evaluate the reporting of key risks at all levels of the enterprise. Internal audit will test the accuracy, relevance, and completeness of information, reporting, and communication. Timely reporting of changes in risks, driven by events or a failure of controls, is a quality attribute in internal audit’s assessment of the ERM process. The availability of the information and communication infrastructure, and the dissemination of content, should be tested.

Provide central monitoring and coordinating of the risk management processes and the outcomes. In a study by Ernst & Young, as

reported at the IIA's Enterprise Risk Management and Control Self-assessment Conference in Las Vegas in September 2004, almost two thirds of enterprises plan to use CSA for ongoing evaluation and monitoring. Of the respondents, 44 percent plan to use periodic surveys and 27 percent plan to use data analytics.⁷

Monitoring activities are performed by management on a routine and ongoing

IN ERM-BASED AUDITS, INTERNAL AUDIT WILL STUDY THE RISK UNIVERSE AND EVALUATE THE INCLUSION OF ALL SIGNIFICANT RISKS.

basis. These activities are designed to ensure compliance with risk response strategies. Management performs its own monitoring and demonstrates this by documenting its test processes and making the results available for evaluation by internal audit. ERM tools will be repositories for documentation and test results.

Electronic surveys, questionnaires, and CSA activities can be conducted independently by internal audit for assurance. Internal audit will review self-appraisals, which can be conducted throughout departments in prescribed formats. These self-appraisals should be at the business unit or individual performance levels.

Effective ERM implementation provides for follow-up activities through the use of action-tracking procedures. Knowledge gained through internal audit's review of action identification history, status, and resolution is part of its assessment.

Provide assurance on the effectiveness of risk management. Members of management must certify that they have reviewed the risks and controls in place and that the controls mitigate the risks that will prevent them from meeting corporate objectives.

Assurance to the board by management that the risk process is working effectively is fundamental. Certification and sub-certification by different levels of management is the primary means of providing formal assurance to the board. Internal audit will develop audit strategies based on its overall assessment of integrity, performance, competence, quality, and culture. Internal audit will take into consideration its evaluation of these aspects

from ERM activities and processes in its risk identification and test design.

In ERM-based audits, internal audit will independently review the results of management's assessment of risk and will issue a contradictory report to a no-exception certification. All elements of the ERM process, including the establishment of objections to central monitoring, will be considered in their appraisal of certification.

Provide independent, objective assurance and consulting. This last step is the function of internal audit, whose core role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management. The two most important ways that internal audit provides value to the organization are in providing objective assurance that the major business risks are being managed appropriately and providing assurance that the company's risk management and internal control framework are operating effectively.

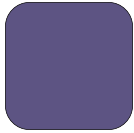
Internal audit may provide consulting services that improve an organization's governance, risk management, and control processes. The extent of internal audit's consulting in ERM will depend on the other resources, internal and external, available to the board and on the risk maturity of the organization; it is likely to vary over time. Internal audit's expertise in risks—in understanding the connection between risks and corporate governance—positions it as being well qualified to act as facilitator for ERM, especially in the early stages of its introduction.

As the organization's risk maturity increases and risk management becomes more embedded in the operations of the business, internal audit's role in facilitating ERM will be reduced. Internal audit can provide value by concentrating on its assurance role, providing assurance for the risk management process and specific risks.

Consulting roles

Dr. Sarah Blackburn states:

It could be argued that all audit work which gives advice and recommendations rather than checking compliance is a form of consultancy. The 1947 definition shows that rudimentary consultancy activity was already legitimated by the desire to improve operational performance. This grew naturally from the experienced auditor's perspec-



COMPANIES WITH HIGH RISK APPETITES THAT ALSO HAVE GOOD RISK MANAGEMENT PROCESSES OFTEN REAP THE REWARDS OF HIGHER PROFITS.

tive, visiting many locations and observing what worked and what did not. Requiring the local management to comply with an official procedure was recognized as unhelpful if the procedure itself was faulty. To challenge the procedure, the internal auditor usually had to take his or her recommendations up several levels to someone empowered to change the system. To influence the decision makers, the auditor had to provide information, analysis, and advice. Again this approach really needed some expertise to provide the authority to act as consultant and the ability to look at the system from the perspective of more senior management.

Consulting services are advisory and related client service activities, the nature and scope of which are agreed upon with the client, are intended to add value and improve an organization's governance, risk management, and control processes without the internal auditor assuming management responsibility. Examples include counsel, advice, facilitation, and training.

Some of the consulting roles that internal audit may undertake include:

- making available to management tools and techniques used by internal audit to analyze risks and controls;
- being a champion for introducing ERM into the organization, leveraging its expertise in risk management and control and its overall knowledge of the organization;
- providing advice, facilitating workshops, coaching the organization on risk and control, and promoting the development of a common language, framework, and understanding;
- acting as the central point for coordinating, monitoring, and reporting on risks; and
- helping managers to identify the best way to mitigate a risk.

In the 1990s, internal auditors also discovered business process reengineering and, using their knowledge of systems, often helped their organizations to reorganize operations. This led to questions of independence and the segregation of duties. In some cases, internal auditors may have ensured the retention of greater levels of control; in other cases their own acceptance of internal control as an end rather than a means was challenged.

The key factor in deciding whether consulting services are compatible with the assurance role is to determine whether the

internal auditor is assuming any management responsibility. In the case of ERM, internal audit can provide consulting services so long as the department has no role in actually managing risks—that is management's responsibility—and so long as senior management actively endorses and supports ERM. Whenever internal audit acts to help the management team to improve risk management processes, its plan of work should include a clear strategy and timeline for migrating the responsibility for these activities to members of the management team.

Internal auditors also aspire to independence, but with less justification since until recently they generally reported to management, often the finance director, particularly when they were restricted to looking at internal financial controls. Internal auditors can provide a better service if their knowledge of the business is closer. Yet that knowledge can lead to conflicts with independence.

Simultaneously there are internal auditors who emphasize their role in helping management to improve its management of risk. They argue that the outcome of a successful audit is an improvement in process or performance: the audit report is a byproduct.

Risk-based internal auditing throws a much clearer light on the independence issue. It is argued that a high-level business risk assurance internal audit function cannot proclaim independence while actively partnering with internal customers. After a series of scandals in large companies, flaws in the independence of the external auditors have increased the pressure on internal auditors to return to policing. Non-executive directors on audit committees demand substantive testing against definitive policies and standard operating procedures and extol the virtues of "positive fear."

Safeguards

Internal audit may extend its involvement in ERM, provided certain conditions apply:

- Management remains responsible for risk management.
- The nature of internal audit's responsibilities should be documented in the

audit charter and approved by the audit committee.

- Internal audit should not manage any of the risks on behalf of management.
- Internal auditors should provide advice, and challenge and support management's decision making, as opposed to making risk management decisions themselves.
- Internal audit cannot also give objective assurance on any part of the ERM framework for which it is responsible. Such assurance should be provided by other suitably qualified parties.
- Any work beyond the assurance activities should be recognized as a consulting engagement, and the implementation standards related to such engagements should be followed.

Skills and body of knowledge

Internal auditors and risk managers share knowledge, skills, and values. Both, for example, understand corporate governance requirements, have project management, analytical, and facilitation skills, and value having a healthy balance of risk rather than extreme risk-taking or risk-avoidance behavior. However, risk managers as such serve only the management of the organization and do not have to provide independent and objective assurance to the audit committee. Nor should internal auditors who seek to extend their role in ERM underestimate the risk managers' specialized areas of knowledge (such as risk transfer and risk quantification and modeling techniques), which are outside the body of knowledge for most internal auditors. Any internal auditor who cannot demonstrate the appropriate skills and knowledge should not undertake work in the area of risk management. Furthermore, the head of internal audit should not provide consulting services in this area if adequate skills and knowledge are not available within the internal audit function and cannot be obtained from elsewhere.

Conclusion

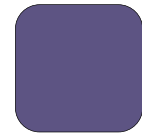
Risk management is a fundamental element of corporate governance. Management is responsible for establishing and

operating the risk management framework on behalf of the board. Enterprisewide risk management brings many benefits as a result of its structured, consistent, and coordinated approach. Internal audit's core role in relation to ERM should be to provide assurance to management and the board on the effectiveness of risk management. When internal audit extends its activities beyond this core role, it should apply certain safeguards, including treating the engagements as consulting services. In this way, internal audit will protect its independence and the objectivity of its assurance services. Within these constraints, ERM can help raise the profile and increase the effectiveness of internal audit.

ERM is never a finished product. Organizations must continuously adjust risk and event interdependencies and identify relevant risk factors. Management must constantly monitor actual performance versus the business plan, and must ascertain that the controls in place mitigate the risks that will prevent management from meeting its objectives. By taking advantage of this rich base of knowledge, internal audit can become more efficient in its independent and objective assurance to the board that the ERM process is under control. ■

NOTES

- ¹ Dr. Sarah Blackburn, *Internal Auditing at the Crossroads: a paradigm shift or a case of paranoid schizophrenia?—a practitioner's perspective*, The Wayside Network Limited (2003), available online at www.brookes.ac.uk/business/bs/research/IAatthecrossroadsBlackburn.pdf (accessed October 2004).
- ² Gartner Research, sponsored by IBM, *You'll Have to Spend to Attain Sarbanes-Oxley Compliance* (October 2003), available online at www.knowledgestorm.com/sol_summary_61309.asp (accessed October 2004).
- ³ Anne E. Kleffner, Ryan B. Lee, and Bill McGannon, "Stronger corporate governance and its implications on risk management," *Ivey Business Journal Online* (May/June 2003), available online at http://66.102.7.104/search?q=cache:jSjFhesjFUSJ:www.iveybusinessjournal.com/view_article.asp%3FintArticle_ID%3D420+list+of+benefits+of+ERM&hl=en (accessed October 2004).
- ⁴ For more information on the COSO ERM framework, see COSO's website at www.coso.org.
- ⁵ IIA press release titled "Adopt and promote risk management processes, Richards says," available online at www.theiia.org/iaa/index.cfm?act=iaa.news&detail=4856 (accessed October 2004).
- ⁶ Dr. Sarah Blackburn, MA, MBA, DBA, FCA, CISA, ADipC, ADipCM, PGCE, MAPM, is chief executive of the Wayside Network, a consultancy that develops organizations and individuals to expertise in internal auditing, risk management, and consultancy



INTERNAL AUDIT'S CORE ROLE IN RELATION TO ERM SHOULD BE TO PROVIDE ASSURANCE TO MANAGEMENT AND THE BOARD ON THE EFFECTIVENESS OF RISK MANAGEMENT.

: skills. A former audit director in several top-100 UK-
: listed companies, she is chairman of the Technical
: Development Committee of the IIA-UK and Ireland,
: a member of the Commission for Healthcare Audit
: and Inspection, the Internal Audit Committee of
: the Institute of Chartered Accountants in England

and Wales, and the Audit Committee of the Open
University. She is also the author of *A Practical
Guide to Internal Auditing*.

⁷ The Institute of Internal Auditors, Enterprise Risk
and Control Self-Assessment Conference, Las Vegas,
Nevada (September 8-10, 2004).