

ON THE COVER

[BRINGING ERM INTO FOCUS](#) A new COSO study gives some much needed clarity and structure to the fluid topic of enterprise risk management. By CHRISTY CHAPMAN

FEATURES

[CREATING A CULTURE OF SECURITY](#) The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top. By WALTER O. BAGGETT

[A PROFESSION IN DEMAND](#) Internal auditing's importance to strong corporate governance has never been more apparent. Auditors can take advantage of their newfound popularity to chart a path to career success. By LYNN KOLLER

[REASONED AND REASONABLE](#) GAO's top official, David Walker, shares his thoughts on corporate governance, accounting scandals, and the importance of sound, ethical practices. By DENNIS BLANK

[MAKE YOUR DATA PAY](#) Analyzing transaction data to generate cost savings or improve processing efficiency and controls can enhance your accounts-payable audits. By NATALIE I. FENNEL

[STICKING TO THEIR PRINCIPLES](#) Will new recommendations designed to strengthen the Combined Code move the United Kingdom toward a more U.S.-style approach to corporate governance? By ARTHUR PIPER

Bringing ERM Into Focus

A new COSO study provides some much-needed clarity and structure to the fluid topic of enterprise risk management.

By CHRISTY CHAPMAN

ENTERPRISE RISK MANAGEMENT (ERM) — THE PROCESS of identifying and analyzing risk from an integrated, companywide perspective — has been circulating as a business concept for several years. Although most organizations are aware of ERM, few have a clear picture of exactly what the process entails. Even fewer possess a solid plan for implementing ERM within their organizations. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) seeks to change all that. The venerable assembly, composed of the American Institute of Certified Public Accountants, the American Accounting Association, Financial Executives International, The Institute of Internal Auditors Inc., and the Institute of Management Accountants, hopes to alleviate some of the ambiguity around risk with its latest study, *Enterprise Risk Management Framework*.

"Although a lot of people are talking about risk, there is no commonly accepted definition of *risk management* and no comprehensive framework outlining how the process should work, making risk communication among board members and management difficult and frustrating," notes John J. Flaherty, chairman of COSO and retired general auditor for PepsiCo Inc. "The COSO board felt that this situation was similar to that which existed prior to the publication of *Internal Control— Integrated Framework*. Just as that study helped get everybody singing off the same song sheet when it came to internal control issues, our goal is that the *ERM Framework* will offer boards and management a commonly accepted model for discussing and evaluating an organization's risk management efforts."

The initiative began in early 2001, when COSO commissioned a group of University of Virginia professors to determine whether or not a risk management framework was even needed. "We didn't want to waste our time reinventing the wheel," Flaherty says. "After a lot of literature study, the team, which was composed of experts in the risk management area, came back to us and confirmed that clear guidance was indeed needed to help organizations build effective programs for identifying, measuring, prioritizing, and responding to risk."

Once this need was identified, COSO assembled a Project Advisory Council with representatives from its five member organizations and hired PricewaterhouseCoopers to write the framework document. A draft is expected to be available for public comment in July*, with a final version of the framework to be published by year-end.

A NEED IDENTIFIED

To a large degree, COSO's work is in response to the stated needs of board members and senior management. It's difficult, if not impossible, for most organizations to expend the resources required to develop their own ERM process from scratch. "In this day and age of lean and mean organizations, most are struggling just to accomplish their day-to-day activities,"

Flaherty says. "They simply don't have the time, talent, energy, or money to undertake such a massive project on their own."

Yet, the mandate for ERM is clear. In surveys of board and audit committee members, corporate risk and risk governance consistently top the list of concerns. In addition, recent business headlines have made everyone aware of how dangerous it is to overlook or ignore potential risks. "As events have transpired in recent years, we've come to realize that we can't consider risk in a silo anymore," says Andrew Jackson, a member of the Project Advisory Council to COSO and assistant general auditor at General Motors Corp. "What we've seen is that you have to look at risks across the enterprise, and you have to look at the interdependencies of those risks. Otherwise, risk management is ineffective."

Many organizations are also seeking to build risk information into their front-end decision-making processes. "This is especially true when it comes to capital allocation," Jackson notes. "For companies seeking to provide value, rationalizing capital from a risk-return point of view is increasingly important. But, to do that, senior leadership and the board need more enterprisewide information, including the measurement of risks across the entity."

ANSWERING THE CALL

ERM, as outlined by the COSO framework, is well-suited to meet these needs. For example, the framework emphasizes the importance of identifying and managing risks across the enterprise from a portfolio perspective. Many organizations perform risk management within each subdivision, but part of the overall vision of ERM is that the risks that occur in the subunits and sublevels of the entity are aggregated and viewed from the top as an overall portfolio of risk.

"That's important for several reasons," says Douglas F. Prawitt, member of the Project Advisory Council to COSO and associate professor at Brigham Young University. "Sometimes there may be risks that magnify each other that you want to know about. Other times there may be risks in different units that offset each other. As a result, the organization may be more or less willing to allow one subunit to take on a level of risk, because another aspect in a different part of the organization would mitigate or magnify it. It's also important to develop an integrated response to risks, so that the right hand isn't unaware of what the left hand is doing."

In addition, the framework takes into consideration the strategic opportunities often associated with risk, while at the same time clearly defining risk as a negative occurrence. In doing so, the framework clarifies an ongoing debate regarding the definition of *risk*.

"An individual's background and responsibilities within an organization really drive that individual's definition of *risk*," Jackson says. "If you talk to a business unit leader who has to generate profits for a company, he or she may view risk as opportunity. However, if you talk to auditors or treasurers, they will likely view risk as downside exposure that needs to be managed. As a result, there has been a tendency to insist that any definition of *risk* include both the idea of opportunity and adversity."

The framework, however, does not claim that risk is both positive and negative. Instead, risk is clearly defined as "the possibility that an event will occur and adversely affect the achievement of objectives." The framework covers the upside of risk by calling for management to identify all potential events that could affect the organization's ability to successfully implement its strategy and achieve its objectives. Those events with potentially negative consequences represent risks to be addressed through the risk management process. Those events that may have positive outcomes, however, are defined as opportunities, which the framework indicates should loop back into the organization's strategy and objective-setting processes.

"By talking about potential events that may have either positive or negative outcomes, the framework supports both the individuals who see risk as opportunity and those who are dedicated to managing the downside aspects," Prawitt says. "Yet, it maintains its focus on risk management as a process for managing possible negative outcomes and their impacts. That's important, because if you try to put together a framework that incorporates both the positive and the negative in the definition of risk, the discussion of risk management gets unwieldy. Plus, it doesn't really fit with a lot of people's conception of what constitutes risk."

RISK AND CONTROL

A key strength of the framework, at least in the eyes of the COSO Board and Project Advisory Council, is that it *incorporates*, rather than *replaces*, COSO's groundbreaking 1992 study, *Internal Control—Integrated Framework*. "Many organizations have adopted the COSO control framework, various audit standards rely on that framework, and it looks like the internal control reporting required under Sarbanes-Oxley will be heavily based on the COSO internal control model," Prawitt notes. "So it was absolutely critical that the new risk framework not undermine COSO's earlier work."

In addition, not every organization is looking to implement ERM. "Given the size and nature of certain companies, it may not be cost beneficial to migrate to an ERM process," Jackson says. "They can, however, still assure the board and stakeholders that the control environment is effective, because it is possible to have an effective internal control environment without enterprise risk management. The original control model needs to remain intact to serve these organizations."

COSO's ERM framework is therefore broad enough to become widely accepted as a common reference point yet still ties into the COSO internal control model. Instead of simply building ERM into the risk assessment component of the control model — a move that was seen as too narrow and limiting — the project team decided to construct the ERM framework around the existing control model. The new ERM model consists of eight components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring (see "[ERM Defined](#)").

Although five of the eight components are taken from *Internal Control—Integrated Framework*, the ERM Framework is nonetheless quite different. Author PricewaterhouseCoopers estimates that 60 percent of the new document is leveraged from COSO's earlier work. But because risk is a more all-encompassing topic than internal control, the resulting discussion found in the new

framework is much more comprehensive than its predecessor. "We view the *ERM Framework* as a turbo-charged or deluxe version of *Internal Control–Integrated Framework*," Jackson says. "Not only does the *ERM Framework* include the three additional components of objective setting, event identification, and risk response, but the five taken from the control model are broader in their descriptions and in terms of the practical guidance."

USING THE FRAMEWORK

The COSO Board and Project Advisory Council envision the final ERM product as one that will prove extremely useful to boards and senior management. At the organizational level, for example, the framework is designed to:

- Help management align risk appetite and strategy.
- Make the risk appetite of the organization explicit and ensure alignment exists between the risks actually being taken and the level of risk the organization desires.
- Ensure effective risk-response decisions are being made.

The key to the framework's usefulness in these areas will be the more detailed practical application guidance, which is expected to accompany the final version of the framework later this year.

Use of the framework is also expected to enhance internal audit efforts. For instance, the framework calls for managers at the business unit, function, or even process level to develop their own composite assessment of risks for their area. "Internal auditors will want to compare their own risk assessments of an area to those developed by area management to see if adjustments should be made to their audit plan," Jackson says. "In some instances, internal auditors may be able to avoid redundancy by testing management's risk assessment for reliability, then basing their audit work on it instead of performing their own risk assessment of the area."

The development of an entity-wide portfolio of risk, which is the capstone of any ERM program, should also aid the internal auditor. "If management has compiled good information in terms of an entity-wide perspective, it may alter the auditor's view of the ultimate impact or exposure of an issue at a functional or process level," Jackson says. "One challenge that's consistently posed to the chief audit executive by senior management, the audit committee, and the board is to explain what an audit finding means to them — to put the one issue in the context of the entire organization. In the past, it's been very difficult for auditors to provide that entity-wide perspective. We traditionally look at functions and activities independently, making it difficult to see the interrelationship of risks across an entire entity. With ERM, the audit team may be able to put more of their audit findings into the context of risk to the entire organization by linking their audit results to the entity-wide risk assessment."

From a broader perspective, the framework is expected to be a useful tool that boards and other stakeholders can use to measure how well their management teams are handling the risks they face. "The question, 'Do we have a risk management program in place in our organization?' is being heard more and more," Flaherty says. "This framework can be used to respond to that

question by assessing the organization against the principles outlined in the document and then using that assessment to communicate to the board and other stakeholders that there is indeed an effective program to identify, measure, prioritize, and respond to risk."

LIMITATIONS

Those involved with the project are careful to point out that neither ERM nor the framework is a panacea. "No matter how well it is designed and operated, ERM cannot ensure an organization's success or guarantee the achievement of objectives," Jackson cautions. "It doesn't provide the proverbial silver bullet against bad judgment and human failure."

That said, much care has been taken to ensure that the framework is as robust and effective as possible. "The Advisory Council comprises people from various backgrounds — academics, internal auditors, certified public accountants, chief financial officers, and private business owners — each of whom brings a certain perspective and strength to the table," Jackson says. "It's been incredible to watch the synergy between the mix of people in the room."

COSO also hopes that exposing the framework for public comment will help ensure its validity and power. "We're not smug enough to think we have all the answers," Flaherty says. "Risk is such an important topic that we want to get as much input as we can, from as many people as we can."

"It's a challenge to obtain consensus from all elements," Jackson adds. "But in the end, that give-and-take makes for a much better product."

* *The draft ERM Framework will be available after July 15 at www.coso.org.*

CHRISTY CHAPMAN is the former executive editor of Internal Auditor.

ERM Defined

ACCORDING TO COSO'S NEW FRAMEWORK, enterprise risk management (ERM) is a process, effected by an entity's board of directors, management, and other personnel, that is applied in strategy setting and across the enterprise. Its goal is to provide reasonable assurance regarding the achievement of organizational objectives by identifying events that may affect the entity and managing risk to be within the entity's risk appetite.

The framework breaks organizational objectives into four categories: (1) strategic objectives, which relate to high-level goals, aligned with and supporting the entity's mission; (2) operational objectives, which relate to effective and efficient use of the entity's resources; (3) reporting objectives, which relate to the reliability of all the entity's reporting to internal and external parties; and (4) compliance objectives, which relate to the entity's compliance with applicable laws and regulations. When ERM is effective, according to the framework, the board of directors and management have reasonable assurance that they understand the extent to which the entity is achieving operational and strategic objectives, preparing effective internal and externally published reports, and complying with applicable laws and regulations.

The framework outlines several key elements that characterize ERM. For example, it states that ERM:

- Takes note of the interrelationships and interdependencies among risks.
- Offers improved ability to manage risks within and across business units.
- Improves the organization's capacity to identify and seize opportunities inherent in future events.
- Considers risk in the formulation of strategy.
- Applies risk management at every level and unit of an entity.
- Facilitates communication by providing a common risk language.
- Takes a portfolio view of risks throughout the enterprise.

In addition to establishing a basic definition for ERM, the framework identifies all of the components that should be present in the risk management program and describes how these should be coordinated to ensure the program's effectiveness. There is a direct relationship between the four categories of objectives, which represent what an entity strives to achieve, and the components, which represent what is needed to achieve the objectives. The eight components are:

- *Internal Environment* — Internal environment reflects an entity's ERM philosophy and influences the risk and control consciousness of its people. Management formulates a philosophy for risk management, enabling entity personnel to understand how to manage risk. Management establishes the relationship among ERM, performance, and value; integrates ERM with related initiatives; forms the desired risk culture; and establishes the organization's risk appetite.
- *Objective Setting* — An entity's mission sets in broad terms what the entity aspires to achieve. From this, management sets its strategic objectives, formulates strategy, and

establishes related objectives. Strategic objectives reflect management's choice as to how the entity will seek to create value. By focusing first on strategic objectives and strategy, an entity is positioned to develop related objectives at operational levels, accomplishment of which will create and preserve value.

- *Event Identification* — Management identifies potential events affecting an entity's ability to successfully implement its strategy and achieve its objectives. Those events that may have a positive impact represent opportunities, which the entity channels back to its strategy and objective-setting processes. Events with potentially negative consequences represent risks, which the entity addresses through its risk management process. Management considers the context within which the entity operates and determines its risk tolerances. It also considers the variety of internal and external factors that influence which events may occur, including the competitive environment, trends, economic and social forces, employee capabilities, and level of process automation.
- *Risk Assessment* — Risk assessment allows an entity to consider how potential events might affect the achievement of objectives. Management assesses events from two perspectives — likelihood and impact, using a combination of qualitative and quantitative methods. There is usually a range of possible results associated with a potential event, and management considers these possibilities a basis for developing a risk response. Through risk assessment, management considers the positive and negative consequences of potential events, individually or by category, across the entity.
- *Risk Response* — Management identifies risk response options and considers their effect on event likelihood and impact, in relation to risk tolerances and cost versus benefit. Responses include avoidance, reduction, sharing, and acceptance of risk. Assessment of risk responses and assurance that a risk response is selected and implemented is an integral component of ERM; however, which particular response management selects is not. Effective ERM does not mean that the best response was chosen, only that the response selected is expected to bring the risk likelihood and impact within the entity's risk appetite.
- *Control Activities* — Control activities are the policies and procedures that help ensure appropriate risk responses are executed. Control activities occur throughout the organization, at all levels, and in all functions. They include a range of activities, such as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.
- *Information and Communication* — Pertinent information from internal and external sources must be identified, captured, and communicated in a form and time frame that enables personnel to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity. In addition, effective communication and exchange of relevant information occurs among external parties, such as customers, vendors, regulators, and shareholders.
- *Monitoring* — ERM is monitored — a process that assesses both the presence and functioning of its components, as well as the quality of its performance over time. Ongoing and separate monitoring ensures that ERM is applied at all levels and across the entity.

Internal Auditor

June 2003

According to the framework, ERM can be judged effective when all eight components are present and functioning well. In addition, the ERM Framework claims that the basic concepts outlined should be present in every entity, regardless of size. Although some small and mid-size organizations may implement component factors differently than large ones, they still can maintain effective ERM.

[Back to main article](#)

Creating a Culture of Security

The OECD standards for systems security provide internal auditors with a tool for operationalizing tone at the top.

By WALTER O. BAGGETT

MANY COMPONENTS OF INTERNAL CONTROL SYSTEMS are tangible documents and procedures. For example, an auditor can review a bank reconciliation or watch a manager approve a write-off. What an auditor cannot see quite so easily are the values that motivate the behavior of the people who operate those controls.

Since the Committee of Sponsoring Organizations of the Treadway Commission's framework was introduced, it has been accepted that internal control systems function in the social and cultural environment of an organization. Many frauds occur in companies that have excellent internal control systems because the corporate culture allows managers and employees to "look the other way" and simply ignore that controls are being overridden.

Given the realization that attitudes are as important as systems, the accounting literature and corporate governance standards have placed the responsibility for corporate culture squarely on top of the management pyramid because the board of directors and top management set the standards for an organization's belief systems.

Internal auditors are always looking for ways to document actions that indicate management at least attempts to create an effective control environment. However, if identifying and measuring belief systems is difficult, identifying how the board of directors and management go about setting them is next to impossible. The Organization for Economic Co-operation and Development's (OECD's) *Guidelines for the Security of Information Systems and Networks* may be of some help in this area. The guidelines provide a set of principles that allow auditors to study and assess the control environment. Although originally designed to address information technology, it is clear that they have wider application.

Taking action

The OECD's guidelines provide a basis for talking about and assessing organizational values. At the heart of the guidelines are nine principles that provide a comprehensive framework for creating a culture of security: awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, and reassessment (see "[Principles of a Security Culture](#)").

There are specific actions top management must take to make the principles operational. Although it is often said that management's job is planning and controlling, the reality is that management has to do a bit more. In addition to laying out action plans for operation of the organization, management must get involved in actually carrying them out, or at least demonstrating how they will be carried out. Similarly, controlling means reviewing results and taking corrective action, which leads back to the beginning of the planning and control cycle.

Thus, top management and the board's responsibilities lead to performing four basic types of tasks:

- *Stating the policy.* The policy should consist of broad planning principles.
- *Directing action plans.* These plans include specific programs or elements that must be carried out.
- *Reviewing results.* Program goals and objectives should be compared to actual results.
- *Taking corrective action.* Based upon feedback, management and the board should mandate specific actions.

By applying these four tasks to the nine principles, auditors can create a guide to interpret board and management actions and determine if they are fulfilling their responsibility for establishing a culture of security and control (see "Task Domains of Individual Principles," below).

Task Domains of Individual Principles				
	Stating Policy	Action Plans	Reviewing Results	Corrective Action
Awareness	X			
Responsibility	X	X		
Response		X	X	X
Ethics	X		X	X
Democracy	X		X	X
Risk assessment			X	X
Security design and implementation	X	X		
Security management	X	X		
Reassessment			X	X

Creating a Clear Picture

Considering the principles within specific task domains, internal auditors can expand on their definitions to create additional guidance in the search for signs that top management and the board are taking steps to create an appropriate culture:

1. **Awareness.** The board of directors should approve a policy statement drafted by management that clearly states that the security of the company's computer systems is the responsibility of all employees.
2. **Responsibility.** Management must assign specific responsibility for computer and network security, beginning with a policy statement and extending to development of specific staffing assignments and assignments of authority and responsibility.

3. **Response.** Planning must include a requirement for reporting security breaches. These reports are the basis for informed management responses, reviews, and calls for corrective action.
4. **Ethics.** Without question, management and the board must develop and promulgate corporate codes of conduct. In addition to discussing information and network systems, these codes must cover a broad range of commercial and social responsibilities.
5. **Democracy.** Management and the board must create and publicize a core principle of equality in company policies. If this core value of respect for the rights of others is not followed, virtually all other values of respect for privacy and security will crumble. Decisions must be based on sound economic reasoning. However, even economics may have to be held at bay if a decision leads to intolerant behavior. This principle should be a part of every review process and the basis for directing corrective actions when problems are detected.
6. **Risk assessment.** As each aspect of operations — not just computer and network systems — is reviewed, risks must be assessed. Management and the board may decide to accept some risks that cannot be avoided. There are trade-offs, and cost/benefit analyses of preventive measures should be made.
7. **Security design and implementation.** The development of systems, networks, and security requires a systematic plan. The literature, such as the acquisition and implementation domains of the Control Objectives for Information and related Technology (CobiT®), developed by the Information Systems Audit and Control Foundation of the Information Systems Audit and Control Association, generally refers to this as systems development life cycles (SDLC).

The specific elements of a given SDLC may vary depending on the project. For example, designing a computer system from the ground up is different from purchasing off-the-shelf products. The particular SDLC chosen for a project is not important. What is important is that someone has a plan that includes checkpoints, mileposts, or some other systematic way of reviewing progress against the plan. This is the definition of a true control system. In addition to measuring results, there is a comparison of results against standards and there are methods for taking corrective action. There must be both a policy statement and a specific action plan for the SDLC that include security and controls.
8. **Security management.** The assignment of responsibilities for ensuring security should lead to staffing. Security systems managers must develop and perform tasks that will identify problems and result in corrective action. Some of these tasks will be routines, faithfully followed without variance; others may be random, relying on serendipity to find outside-the-box problems and solutions. Top management and the board should state this as a policy and see that there is an action plan in place to ensure that it happens.
9. **Reassessment.** A one-time review of security or internal controls is never enough. Reviews should be periodic and scheduled.

From Another Angle

Another way to cast the nine principles is to consider what an auditor would look for in a review of the actions of top management and the board of directors.

POLICY STATEMENTS Internal auditors should review statements to determine if management has prepared and the board approved and reviewed on a periodic basis:

- *A corporate ethics policy/statement.* A broad set of ethical commitments along with a program of education and enforcement should be at the heart of any 21st century organization's charter.
- *A policy on the need for computer security.* This has already become law for u.s. health-care providers, and parts of that law are in effect for most other organizations around the world.
- *A policy on personnel assignment and responsibility.* Policies should clearly prohibit discrimination. Fair and equal treatment of all parties the company deals with must be the required norm.

Auditors should obtain copies of these policy statements for their permanent audit file and review them annually.

ACTION PLANS The internal auditors should determine if management has prepared and the board of directors approved and reviewed on a periodic basis:

- *Organization charts, position descriptions with lists of authority and responsibility, and the company's authorized check signors.* These document, policy, and procedure statements should provide specific or general authorization for people to write off accounts receivable, sign purchase orders, and perform a host of other key control functions. Management should expand on these authorizations, particularly for routine functions.
- *Reporting programs for adherence to policies that parallel the financial reporting in frequency and depth.* In addition to training and enforcement, feedback should be provided to the board to assure them that mandates are being followed. Day-to-day management supervision should play a primary role in compliance enforcement. Also, internal auditors should test adherence to policies and procedures.
- *Planning documents, including annual and capital budgets.* These basic documents should support the other nonfinancial objectives presented here, specifically the attitudes and values of organizational integrity. The relationship between moral integrity and developing profitable operations with strong long-term objectives should be clear and highlighted in the budget narratives.
- *Programs and protocols for developing information systems and networks.* The development of new information systems requires extensive management superstructures. The CobiT® framework discussed previously is an example of the type of support that must be developed to create, implement, and maintain secure, functional systems.

RESULTS REVIEW Auditors should review the feedback documents presented to the board. Similar to the review of financial information presented by the chief financial officer, management must present and the board must review and take action as needed on:

- Organizational ethics and enforcement.
- Ethical standards.
- Equality, nondiscrimination, and democracy. Problems and their successful resolution should be reviewed.
- Physical and logical network security. Management, the board, and staff need to know about break-ins and other problems and how they were addressed.

The review process should be systematic and periodic. Unexpected problems should be addressed, but they should not be used as an excuse for skipping a periodic review. The fact that people know a review will occur helps prevent lapses in adherence to values, as well as policies and procedures.

CORRECTIVE ACTION The minutes of the board as well as management's correspondence and actions should indicate that corrective measures are taken in relevant areas. If review material is in place, finding evidence of follow-up and corrective actions should be fairly easy. Corrective action should be verbally confirmed through management inquiry and supported by documents supplied by management.

A Standard for Comparison

So what does the auditor do if he or she uncovers an absence of some of these controls? A lack of certain controls may not represent a weakness. Particularly for small organizations with strong central management, it may be a waste of time to develop these policies and procedures in great detail. For such organizations, simple subsets, clearly written and publicized to employees, may be more than adequate. Auditors should review these lists with clients and suggest appropriate items and levels of detail for their organization.

For large organizations that develop policies and procedures, the OECD's guidelines provide a compelling standard of comparison. Any organization that measures up well against the guidelines should be proud of their governance structure, at least on paper. However, many companies will likely find within them suggestions for significant improvements.

WALTER O. BAGGETT, PhD, CPA, is an associate professor in the department of accounting, law, and computer information systems at Manhattan College in Riverdale, New York.

Principles of a Security Culture

1. *Awareness.* Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.
2. *Responsibility.* All participants are responsible for the security of information systems and networks.
3. *Response.* Participants should act in a timely and cooperative manner to prevent, detect, and respond to security incidents.
4. *Ethics.* Participants should respect the legitimate interests of others.
5. *Democracy.* The security of information systems and networks should be compatible with essential values of a democratic society.
6. *Risk assessment.* Participants should conduct risk assessments.
7. *Security design and implementation.* Participants should incorporate security as an essential element of information systems and networks.
8. *Security management.* Participants should adopt a comprehensive approach to security management.
9. *Reassessment.* Participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures, and procedures.

**SOURCE: Guidelines for the Security of Information Systems and Networks,
Organization for Economic Co-operation and Development**

[Back to main article](#)

A Profession in Demand

Internal auditing's importance to strong corporate governance has never been more apparent. Auditors can take advantage of their newfound popularity to chart a path to career success.

By LYNN KOLLER

IF POWER REALLY IS AN APHRODISIAC, internal auditors may find their sex appeal on the rise; relatively speaking, at least. The Sarbanes-Oxley Act of 2002 has increased not only the need for internal auditors, but also their stature in the eyes of those who hire them as well as those who aspire to be them.

"The internal auditor's role is increasing dramatically," says Karl Nagel, a principal of Karl Nagel & Co., an accounting firm based in Huntington Beach, Calif. "Although internal auditors never just looked at financial information, it was typically a priority at many firms. Now, they have a much higher responsibility: Sarbanes-Oxley compliance. Executives are depending on internal auditors not just to reduce the cost of outside auditors, but also to help the executives sleep easier at night."

Although prospective auditors face a tight job market, experienced auditors may soon see wider career options available to them. In a recent IIA Global Auditing Information Network survey of 243 chief audit executives, 44.4 percent of respondents stated that their internal audit staffs would grow in 2003. Auditors with two to four years' experience, specialized knowledge, and adequate technical skills stand a good chance of finding employment under current conditions.

Make Yourself Marketable

Although the demand for internal auditors varies around the world, experienced and beginning auditors with specialized knowledge may have a better chance of obtaining employment. Regulatory or technological specialties as well as professional accreditation and industry-specific experience can increase an auditor's market value.

SARBANES-OXLEY EXPERTISE Internal auditors who have comprehensive knowledge of Sarbanes-Oxley and U.S. Securities and Exchange Commission (SEC) rules may find themselves a hot commodity, says Robert Hirth, managing director of Protiviti, an international risk consulting and internal audit firm that employs about 800 audit professionals. He suggests that internal auditors specialize to take advantage of the risk-sensitive corporate environment.

The complexity of Sarbanes-Oxley makes it challenging for organizations to assimilate, and Hirth suggests that internal auditors take advantage of that need. "Sarbanes-Oxley never existed before," he explains. "No matter who you are — with 20 years of experience or two — this is a brand new thing that you can become as expert about as anyone. Of course, general business experience and an understanding of internal controls, financial reporting, and documentation are very important."

Glen Gray, a professor of accounting and information systems at California State University at Northridge, says he recently spoke with an internal auditor at a large insurance company about how Sarbanes-Oxley was impacting his department. "Before Sarbanes-Oxley, he had reason to believe that his entire internal audit department was going to be eliminated," Gray recounts. "Auditors were being laid off, morale was down, and the chief auditor reported to the controller.

"Now, after Sarbanes-Oxley, the department is growing again, morale is up, and the audit department is reporting directly to the audit committee," Gray continues. "The reason for those changes is that Sarbanes-Oxley places a renewed emphasis on internal controls, as well as the requirements for the chief executive officer and chief financial officer to certify quarterly and annual financial reports."

TECHNOLOGY KNOWLEDGE Like regulatory expertise, having knowledge of the risks, benefits, and practical issues surrounding the latest technologies can make an auditor marketable. "Technology is a very important part of internal auditing, so we're looking for people with specific skills," Hirth says.

"As the actual technology and applications that a company uses change, the risks change and how you audit changes, as well," he explains. New enterprise- resource planning and customer-resource management applications have changed how companies function and the risks they face. Securing access to company data, safeguarding data when an employee leaves a company, and protecting Internet transactions are examples of issues now important to auditing.

Conversely, companies with older applications sometimes face a scarcity of auditors with applicable knowledge, Hirth says. This may help veteran or semiretired auditors looking for an edge in the job market.

Ultimately, auditors with a specialty can capitalize on changes in the market, Hirth adds. Other areas of specialization include security, privacy, and specific applications.

Glenn Sumners, director of the Center for Internal Auditing at Louisiana State University (LSU), warns, however, that although many internal auditors may see an increased demand for specific information technology (IT) skills, they may also see more applicants jockeying for their positions. "The demand now is not quite as good as it was a few years ago for IT auditors," Sumners explains. "But, the market will be good in the long run."

INDUSTRY EXPERIENCE According to Hirth, Protiviti looks for industry-specific backgrounds. For example, the company has hired bank regulators and certified fraud examiners with legal backgrounds. The divergence of job duties within companies of all sizes means that other employment experience can be adapted for auditing.

Protiviti once hired a Boeing engineer. "You wouldn't necessarily think of him for auditing," Hirth says. "This was a person trained in a very process-oriented world ... and when we got into a manufacturing environment, he was a lot better than a person with an accounting degree."

To compensate for his lack of financial background, the employee was sent to an intensive six-week accounting program. "We had this engineer who was now 'dangerous' because he had some accounting," Hirth says. The engineer-turned-auditor started as a senior consultant with Protiviti and is now an experienced manager.

LANGUAGE CAPABILITIES The ability to communicate in English is extremely valuable in international firms based in non-English speaking countries, says Paul Kooijmans, corporate auditor and senior vice president in charge of corporate accounting at Wolters Kluwer, an international information services company based in Amsterdam. Wolters Kluwer requires its auditors to be fluent in Dutch and English.

"If you only work for Dutch companies, you may speak only Dutch. I want them to have much more depth of experience than just working for a Dutch company," Kooijmans explains. "One guy sent me an e-mail in English. He's Dutch and lives in Amsterdam. I called the guy back immediately. He is 25 and not qualified yet. However, if we like each other and his motivation is good, I still might hire him."

Language skills are also prized at Protiviti. Candidates who are fluent in Chinese and Japanese and are familiar with U.S. accounting practices are particularly valuable to the organization for work with clients with international operations, Hirth says.

"These language skills, including reading skills, are imperative to be able to operate effectively in two distinct cultures," Hirth says. "Many times, key employees — even management — may speak limited English, or even none at all." These companies value auditors who can communicate between international offices, and also manage documentation in both English and another language.

According to Robert Melville, director of MSc Internal Auditing and Management at the Cass Business School in London, his students are seeing more opportunities internationally. "Probably the biggest growth areas for internal auditing are in the People's Republic of China — where we have a long history of very successful alumni — Greece, the former USSR, and eastern European countries about to join the European Union," he says.

CERTIFICATIONS Internal audit certifications are not required; however, many organizations prefer some professional accreditation. Certified public accountants (CPA) are common in the field, and more specific audit certification is gaining popularity. "We're hearing about a lot more companies wanting their internal auditors to have some type of certification, and many opting for one or another specialty certification," says James Cashell, professor in the department of accountancy in the School of Business Administration at Miami University in Oxford, Ohio.

According to Ashley Hartley, a product manager at KnowledgeLeader.com, an online research portal for audit professionals, the most-in-demand designations for internal audit candidates include:

- Certified internal auditor (CIA).

- Certified information systems auditor (CISA).
- Certified information technology professional (CITP).
- Microsoft certified systems engineer (MCSE).
- Certified public accountant (CPA)/Chartered accountant (CA).
- Certified management accountant (CMA).
- Certified financial services auditor (CFSA).
- Certified fraud examiner (CFE).

"In the profession, the CIA exam is growing faster than any other," says LSU's Summers. "The big advantage of the CIA over the CPA is that the CIA is international and much broader in scope. It's much more relevant to the actual job."

A JOB WORTH pursuing

Few occupational fields are impervious to economic slumps, and so it happens that internal auditors may see a slight dip — or at least no rise — in starting salaries over the short term. The field itself, however, remains strong and necessary, experts say.

The 2003 *Salary Guide*, published by Robert Half International, shows that experienced internal auditors may find sufficient job offerings and room to maneuver in the U.S. job market. However, 2003 average starting salaries for these positions will increase only marginally over 2002 salaries, and in some cases, decrease. For example, the starting salary for a senior auditor at a large company is between \$48,000 and \$61,500 this year, down 0.2 percent from 2002. An internal auditor with one to three years' experience joining the same size firm can expect to earn between \$38,500 and \$49,500 in 2003, a 0.6 percent increase from last year. An audit director at a +\$500 million corporation can anticipate the largest decrease in average annual starting salary, dropping 6.9 percent this year to between \$122,250 and \$197,500.

In the United Kingdom, Pal Chakravorty, senior consultant in audit and risk at Greythorn, a recruitment agency, estimates that internal audit candidates with four years of investment banking experience can command an annual salary of between £40,000 and £60,000, plus benefits, in London. Employment seekers with six or more years of experience are generally looking at upwards of £55,000, and candidates with strong skills, such as detailed product knowledge, can earn about £70,000. Chakravorty says that on-the-job salary increases are rarer now than in the past, due to a skills surplus.

Although salary increases are slowing, California State University's Gray contends that good working conditions and relative job security make internal auditing worth pursuing. He adds that in the past, internal auditing evoked unpleasant images for many people. "The old image of auditors was that of the company 'policeman' looking over peoples' shoulders, telling them what they were doing wrong," he explains.

In recent years, however, the field has become more dynamic, Gray says. With emphasis on corporate governance and new technologies bubbling out of Silicon Valley every week, internal auditors can count on increased interest in their work product.

Internal Auditor

June 2003

[SIDEBAR: Growing Interest in the Profession](#)

LYNN KOLLER is a free-lance writer based in Ormond Beach, Fla.

Growing Interest in the Profession

INTERNAL AUDITING IS NOT FOR THE UNEDUCATED, nor is it for underachievers — at least at entry-level. The 2003 *Salary Guide* published by Robert Half International of Menlo Park, Calif., asserts that entry-level hiring in public accounting firms has slowed. According to the report, "Recent graduates face a tough employment market, and only the best candidates with top grades and exceptional internship experience are being considered for available positions." However, this news hasn't stopped the interest in internal auditing at the college level from growing. Both awareness of the field and the number of programs dedicated to internal auditing is up, according to experts such as James Cashell, professor in the department of accountancy in the School of Business Administration at Miami University.

"Over the last few years, I think students have begun to find internal auditing more interesting," Cashell says. "It seems like the nature and perception of the work has changed. The students used to come in with a stereotype of internal auditors, and they don't seem to have that anymore."

Cashell says that students now see fraud detection, operational auditing, risk evaluation of proposed joint ventures, and contributing "value-added services" as functions encompassed in many internal audit positions. The countless functions tackled by internal auditors at different organizations means that an auditor may choose to be a jack-of-all-trades or a master of one.

According to Glenn Sumners, director of the Center for Internal Auditing at Louisiana State University, "The internal audit profession has gone from having one college-level program in 1985 to about 45 programs in seven countries today." Sumners says that many of these programs emphasize accounting as opposed to multidisciplinary approaches, leaving a gap in training. "Internal auditing is a multidisciplinary profession and accounting is only one of the attributes that people look for. Even in light of current events and Sarbanes-Oxley, we're placing more non-accounting people than accounting into internal audit positions," Sumners says. "Many areas are popular, but systems, finance, accounting, and MBAs tend to be most popular."

Sumners contends that the profession is changing dramatically and faces a big training challenge. "We're going to have to refocus some of our education processes. There is a need for additional training on risk and corporate governance," he explains.

According to Robert Melville, director of MSc Internal Auditing and Management at the Cass Business School in London, although recruiting is certainly down at the large accounting firms, other job markets will absorb some of that surplus. Those looking for internal audit positions should not face unreasonable competition in the United Kingdom, he says.

"Chartered accountants used to recruit 10 percent of all the U.K. graduates, with about 10 percent of them going to just KPMG," Melville says. "Now firms are diversifying, and a lot of them are using the consultancy arms to employ internal auditors who they then farm out."

Internal Auditor

June 2003

Melville has found changes in the type of students interested in auditing careers. "One thing that I have really noticed over the years is that those wishing to make a career as internal auditors are younger — my students' average age is 23, down at least a decade in five years — and female, with an 80/20 ratio of female to male, a complete turnaround in a few years and totally against the pattern in other business courses here," he says.

Melville is seeing those changes in his own university requirements, including the MBA program. "Even our MBA students are influenced by internal auditing now," Melville says. "We now place corporate governance in the core subjects, where it has equal status with strategy and other traditional MBA subjects."

[Back to main article](#)

David Walker: Reasoned and Reasonable

GAO's top official shares his thoughts on corporate governance, accounting scandals, and the importance of sound, ethical practices.

By DENNIS BLANK

FOUR AND A HALF YEARS AGO, DAVID M. WALKER became comptroller general of the United States and head of the U.S. General Accounting Office (GAO), the watchdog agency that keeps a close eye on government waste and abuse. At age 51, he is the seventh person to hold that job. Walker is highly respected on Capitol Hill as someone who's not afraid to speak out about abuses both in and out of government, as evidenced during his frequent testimonies before congressional committees.

Before coming to the GAO, Walker was a top executive with Arthur Andersen LLP in Atlanta, serving as global managing director of the firm's human capital services practice and also as a member of the board of Arthur Andersen Financial Advisors. He currently serves as chair of the U.S. Intergovernmental Audit Forum and the Center for Continuous Auditing and sits on the board of the International Organization of Supreme Audit Institutions and the U.S. Joint Financial Management Improvement Program.

Walker is the author of *Retirement Security: Understanding and Planning Your Financial Future* and co-author of *Delivering on the Promise: How to Attract, Manage and Retain Human Capital*. He spoke to *Internal Auditor* about recent developments in both the public and private sectors and his strong belief in the importance of core values.

Mr. Walker, what do you view as the most significant differences in the challenges faced by government auditors and their counterparts in the private sector?

Government financial management information systems are more antiquated than many that exist in the private sector. The federal government has been a relatively recent player in placing strong emphasis on sound financial management practices. Federal agencies have only been subject to financial audits for a few years now. So, despite the size and complexity of the U.S. government, its financial systems and practices are not where they need to be, although we are making real progress. Many federal financial management systems are not as sophisticated, not as integrated, and just not adequate for the type of enterprise that is represented by the federal government. On the other side of the coin, the risk is lower because federal government auditors do not face the possibility of shareholder suits. Nevertheless, they do have to answer to taxpayers, and we have found there is a very real consequence to breaching trust. It can do irreparable harm to your reputation, whether you are subject to shareholder suits or not. In the case of Arthur Andersen, the firm went from being the global gold standard for professional services firms to gone in less than two years, and there is a real lesson to be learned from Andersen's fall.

In your opinion, how could the recent financial failures of very prominent companies have been avoided?

In my view, the most critical element that needs to be addressed to help ensure that these failures do not proliferate in the future is the overall governance model for public companies in the United States. I believe that the current U.S. corporate governance model for public companies is not adequate to protect the interests of shareholders and other key stakeholders. Although most public companies are required to have a board that is composed of a majority of independent directors, and certain key committees are required to be composed solely of outside directors, a closer look reveals that the independence of many boards may be more a matter of form than substance. Boards have a clear responsibility to help maximize shareholder value, manage stakeholder risks, and hold management accountable for results. This latter element is a major reason why having a board that is both qualified and independent is so important.

What governance lessons can the private sector learn from the public sector?

The ethical rules that apply to the public sector are more transparent and more stringent than one would see in the private sector. There are other areas where the government has been leading by example. For example, the GAO, as the organization responsible for auditing the U.S. government's financial statements, has voluntarily expressed an opinion on the adequacy of the federal government's internal accounting controls for the past several years. That is now required for auditors of public companies under Sarbanes-Oxley. We did that not because it was required, but because it was the right thing to do.

What, if any, long-term benefits do you see from Enron and the other corporate failures in terms of the internal audit profession?

There will be much more opportunity for internal auditors to be involved in risk management related work, and they also may have additional opportunities to work with top management and boards of directors. I see their role evolving just as the role of external auditors needs to evolve, where practitioners are not just trying to ascertain that the amounts are fairly stated but also determining the appropriateness of certain types of activities.

The GAO has frequently commented on ethical dilemmas faced in government. What advice would you offer corporate internal auditors in terms of how they can enhance the ethical culture of their own corporations?

All auditors ought to be dedicated to a set of professional standards and core values. In the final analysis, we get paid for our judgment. We need to recognize that the law, as well as accounting principles and auditing standards, represent the floor of acceptable behavior, not the desired state. We need to do what we think is right based on our professional and independent judgment, and we need to learn from the lessons of Andersen and others. Specifically, we need to recognize that it takes years to earn a reputation for integrity, but it could be lost very quickly if there is a real or perceived breach of trust.

We need to focus on substance and not form in a range of areas, including accounting policies and audit approaches. I think one of the problems that exists now is that too many people are

checking boxes and not turning on their brains. Too many people are trying to figure out what is acceptable rather than what is appropriate. When we are in an environment where people are trying to figure out what is arguably acceptable rather than what is right, we are in trouble.

In your view, what has been the effect of the Sarbanes-Oxley legislation and ensuing U.S. Securities and Exchange Commission rules so far?

There are a number of provisions in Sarbanes-Oxley on which the GAO spoke out and supported. By no means is the legislation perfect, but you can't expect any piece of legislation to be perfect. We did a lot of work to help form the provisions of the Sarbanes-Oxley Act. The bottom line is that Sarbanes-Oxley was a positive step forward, and there was a need for meaningful reform in this area. It is too early to tell how effective it is going to be because a lot of it has to do with how the act will be implemented.

Legislation is often a lag indicator. The majority of people in the private sector are well-intentioned, have integrity, and are trying to play by the rules and to do the right thing. Sometimes, you have a few bad actors that run an undue risk, and there is public outcry to make sure everybody conforms at least to some minimum standard. Hopefully, the responsible companies and players are doing better than the minimum standard and are ahead of the curve.

Because the GAO closely examines agency finances and scrutinizes their practices, your work must require some sensitivity. What is the toughest part of the job, and does the GAO feel political pressure over its reporting?

The toughest part of the job at the GAO involves our efforts to perform work in a professional, objective, fact-based, non-partisan, non-ideological, fair, and balanced way. By and large, we are successful in accomplishing that objective. For example, we recognize that the federal government's move to a travel/credit card system saves the taxpayers a tremendous amount of money in paperwork, but we also need to recognize that there are those who have abused this privilege. We recognize the need for better safeguards and controls over this as well as the need for increased transparency and accountability in conjunction with potentially abusive situations.

However, I have 535 [Senate and House] "clients" who are all very dedicated and capable public servants, but they are all politicians and each belongs to a political party. They all represent certain geographical areas, serve on various committees, and have certain philosophies, ideologies, and opinions. The toughest part of the job can be dealing with clients or executive branch officials, who often tend to look at things in a partisan light. Even though people do not dispute what we say, they may not like it because it is not consistent with their views or with their party's position. Therefore, they are concerned about the political impact of our work. Simply stated, our job is to speak truth to power and then let the elected officials make the policy calls.

We have committed ourselves to certain professional standards and a set of core values, including accountability, which is what we do; integrity, which is how we do it; and reliability,

which is how we do our work. So my view is that our clients are entitled to their opinions. We obviously want to hear what they have to say, but in the final analysis our work must be consistent with applicable professional standards and our core values. We cannot compromise these because if we do, we end up harming the reputation of the GAO and its viability and credibility as a professional, independent body.

One's reputation is priceless, and I strongly believe that we need to be dedicated to a set of core values. They represent positive beliefs and personal boundaries that we will not violate. I used to be a partner with Arthur Andersen, although I was not involved with Enron or any of their recent problem accounts; their problems evidently did not occur until after I left the firm. Andersen vanished in less than two years following the Enron scandal. That happened because a few players did bad things that had cataclysmic consequences for the entire organization. These players strayed from the firm's core values. They strayed from applicable professional standards. We can't allow that to happen to the federal government, and we do everything we can to prevent it.

Some people say that the new independence standards issued by the GAO last year, which impose limits on the non-audit assignments auditors can accept from government agencies, are having a "chilling effect" on some government auditors. Was that the intended effect?

It is not my understanding that there has been such a chilling effect. We have tried very hard to come up with a reasoned and reasonable approach to addressing the issue of independence and related scope-of-service issues. Independence is more than a state of mind. It is critically important that auditors maintain their independence because if they don't, their integrity and credibility are threatened. We believe it was a necessary change. If anyone doesn't understand what we are proposing, then they should inquire. We didn't come up with arbitrary limits on the amount of nonaudit services that auditors could perform. We took a very principles-based approach where people have to use their best judgment, and it is an approach that will be able to evolve as markets change. Quite frankly, the government should take that type of approach more often.

What is the GAO doing to reduce the level of waste in federal government spending?

It is not just a matter of waste. It is also a matter of what we are doing to improve economy, efficiency, and effectiveness. The fact of the matter is we should have zero tolerance for waste, but it will never be zero in the government. When we perform financial statement audits, we also look at internal controls and what government agencies are doing to minimize the areas of waste. We are voluntarily providing an opinion on those internal controls, which is not required by law but constitutes best practice. We also create increased visibility over improper payments, some of which represent waste, fraud, and abuse and some of which represent items paid without the proper documentation. We publish a biannual high-risk list of those federal functions and activities subject to a high degree of fraud, waste, abuse, and mismanagement, or that are at risk of not achieving their mission in an economical and efficient manner.

What do you do in situations where the failings of government continue to occur? Do you recommend prosecution or take some other type of strong action?

We follow up to see what type of action is taken. The reason we do that is because it's one of our measures of success. Once we ascertain that recommendations were adopted, we then see how much money was saved or how much money was freed-up for other purposes. We also want to know if the adoption of our recommendations improved safety, increased security, or enhanced privacy. In addition, we publish the aforementioned list of high-risk government agencies, and we testify before Congress and convey the status of important issues.

Do you think the ethical standards within government have gotten better or worse?

When you are dealing with an entity as big as the federal government, it is difficult to generalize. I have run three federal agencies during my lifetime, and the experience I personally have had is that an overwhelming majority of public servants have extremely high ethical standards that I think exceed those found in the private sector.

Do other government agencies dread the GAO coming to audit? If so, how do you handle that?

First of all, it has changed significantly over the last several years. We are trying to employ what I would call a "constructive engagement approach" when dealing with various executive branch departments and agencies. Granted, we work for the Congress, and part of our job is to be able to point out what is wrong and make constructive recommendations to address those problems. At the same time, we also want to acknowledge what is right, and we want to note where progress is being made. In appropriate circumstances, we want to be able to point out and share best practices. We want to develop tools and methodologies that will help others help themselves make progress. In the final analysis, we measure success based on whether or not people adopt our recommendations and to what extent those recommendations result in savings, better security, enhanced privacy, or other improvements.

For many years, people feared the GAO, but I believe it is now more the case that people respect the GAO. Our clients are somewhat guarded, but not as guarded as they used to be. They recognize we can be helpful in trying to achieve meaningful, needed, and constructive change. Right now, for example, our working relationship with cabinet-level and top-level Office of Management and Budget officials is probably the best it has ever been.

At the same time, we obviously have to maintain our independence. We do not always agree, and we are going to call it like we see it. When you are dealing with middle levels of many federal government agencies, they remember the GAO from 10 or 20 years ago. They always respected us, but there was a period in the past where they viewed us as somewhat of a "gotcha" organization. That is not what we are doing now, although there are still plenty of areas to point out that need improvement, and there always will be.

DENNIS BLANK is a free-lance business reporter.

Make Your Data Pay

Analyzing transaction data to generate cost savings or improve processing efficiency and controls can enhance your accounts-payable audits.

By NATALIE I. FENNEL

MANY ACCOUNTS-PAYABLE (AP) AUDITS focus on the financial accuracy and reporting aspects of the process or on the relationship of accounts payable to purchasing. Although these approaches are important, they can be improved by including another dimension: analyzing transaction data. This seemingly simple addition to an audit can generate cost savings and improve efficiency and controls in AP processing.

Relying on the Tried and True

Accounts-payable audits usually focus on one of two approaches:

- Evaluation of the completeness, accuracy, and validity of the financial reporting for AP, by reviewing items such as cutoffs, unrecorded liabilities, math accuracy, reconciling items, agreement of summary and detailed records, and comparing to the prior period balance. These are typical methods used to ensure that AP is represented in accordance with Generally Accepted Accounting Principles (GAAP).
- Evaluation of the relationship of AP to purchasing by ensuring that supporting and approved purchase orders exist, examining the management of vendor database activity, and reviewing vendor terms — including lost discounts for failing early payment. Common operational audit techniques for reviewing AP activities focus on ensuring that there are underlying controls over the purchasing function — the root of most AP activity. Nevertheless, they are tangential and not direct controls over AP.

Each of these approaches is necessary and serves a purpose. However, efficiencies or cost savings could be derived from a focused review of underlying AP data, as it represents AP activity. Organizations can be well controlled based on GAAP, have excellent underlying purchasing controls, and still have room for cost-saving improvement in their AP activities. Although most large audit shops already do extensive AP testing that includes data analysis, smaller or less-sophisticated audit environments may benefit from performing the additional simple tests described in this article.

Throughout my career, my audit teams have uncovered opportunities that led to thousands of dollars in cost savings, justifying the few additional audit steps and providing management with a feeling that auditing can help them save money, even if it also points out defects in controls.

Examining the Data

To perform the additional tests, the auditor must obtain the client organization's check register for a representative time period. Depending on the size of the client organization and volume of its AP activities, this could be a three-, six-, or 12-month period. This data should be obtained in a format that can be sorted easily, preferably with a common program.

To perform the tests, the auditor will need to create and save several different sorts of the check register data set. The five data sorts that follow can reveal different inefficiencies or other issues that would merit discussion with the client, or possible inclusion in the auditor's report.

1. By ascending check number. Check register data sorted by ascending check number will highlight any gaps in the sequence. Typically these gaps are the result of either spoiled or voided checks. Nevertheless, missing checks must be accounted for. Often, when a check-printing machine is used, preprinted check stock is spoiled at the beginning and/or ending of a check run, creating a gap in the numbers that can be identified by the auditor. Even if these checks can be accounted for, there is a cost in the spoilage of preprinted stock: The more check runs, the more spoilage. The level of storage controls, or lack thereof, over spoiled checks may also create a risk of their misappropriation.

Check-printing software will print checks on special paper that can have a number of security measures built in, such as magnetic inks, by the laser printer. Check-printing software access controls, when used properly, can be even better than access controls over check-printing machines or the signature plates used in them. In addition, the software allows sufficient control over the generation of checks.

Laser-printed checks allow for better controls over blank preprinted check stock because there isn't any stock to control. Therefore, blank checks don't have to be counted, reconciled, monitored, or kept in a safe. In addition, laser printing keeps spoilage to a minimum, which helps reduce gaps in future check registers.

Costly Steps to Heed

The cost of generating a check is often pegged at between \$10 and \$12. Each transaction includes steps that most clients overlook:

- Handling the mail (invoices).
- Entering invoice data into the system.
- Printing AP registers.
- Preparing checks for printing.
- Printing, signing, approving, and mailing checks.
- Filing (or document scanning) of the supporting paperwork.

In addition, the time and focus of managers with check-signing authority has to be considered. Working with vendors to reduce the number of invoices, or even just the number of checks, reduces the amount of processing and all the associated costs.

The elimination of preprinted check stock also reduces costs, while the software features may already be an available but unused part of the existing AP module. However, although laser printing can lower costs and improve certain controls, controls over check numbering could be overridden to double-number checks. Appropriate controls should be implemented and regularly reviewed.

2. Alphabetical by payee name. Sorting the check register data alphabetically by payee's name allows the auditor to see anything unusual including employee names or addresses that correspond to vendors. (Some organizations pay employee expense checks like vendors, so this may not be a cause for concern). Data extraction and analysis is another way to review vendor and employee data.

The auditor's review should also reveal any close spellings or duplicate or frequently appearing names. Each instance should be investigated and invalid entries corrected or deleted to avoid confusion or incorrect or multiple payments. The auditor should note frequent payees as well as the amount of payment to those payees. For example, if the auditor sees that the same payee is being paid weekly, or even more frequently, the auditor's recommendation for improved efficiency may be to negotiate with the payee to be paid biweekly or even monthly.

If the auditor notes any payees are paid more than once in the same check run, the transactions should be examined for possible transaction splitting to avoid control points. For example, if a second signature is required on payments greater than \$20,000, the auditor should be aware of any multiple payments to a single payee under \$10,000. If "Petty Cash Reimbursement" shows up as a frequent payee, it would be wise to review the uses of petty cash and the amount of the fund(s) for reasonableness.

If an employee is being issued expense checks every week, the auditor can evaluate or discuss with the client the effect of a policy of biweekly expense reimbursement for cash expenses — or even petty cash reimbursements of small amounts. Another cost-saving control is using some form of automated purchasing card or credit card reimbursement for most business expenses.

3. By check date. The check register data sorted by date is used to see how frequently batches of checks are printed, and whether special, short check runs are produced between regular check runs. This sort may also help point out the need to reduce the frequency of transaction processing. Staying with only one weekly or biweekly printing and no special check runs can save processing time and cost. Clearly, there will always be a need for "emergency" individual checks, but the client should implement the discipline of regular check runs. However, if the total number of checks produced remains the same, there is still more work for the auditor to do in identifying efficiencies to be gained.

4. By descending dollar amount. The check register data sorted by descending dollar amount should be analyzed and the auditor should take note of:

- The number and total percentage of spending represented by payments in excess of a set amount (depending on the size of the organization, this may vary from greater than

\$50,000, or greater than \$100,000, or greater than \$1 million). The "80:20 rule" often applies to the check register, in that there are typically fewer checks issued for large-dollar amounts and more checks issued for small-dollar amounts. Often, a single or small group or a large supplier of materials or services is paid in large sums.

In such cases, the auditor should discuss with the client the benefits of wire transfers and ACH [Automated Clearing House] payments. Electronic payments, which can be designed with the help of the client's bank, allow transaction controls and more immediate confirmation than issuing checks. More timely transfers may provide an opportunity to negotiate price concessions with the vendor. Stratifying the check values will also allow the auditor to focus his or her audit efforts on the highest value checks.

- The number and total percentage of spending represented by payment amounts below a set threshold, such as \$100. Sometimes there are hundreds of checks produced under \$100, some even under \$10. At the estimated cost of \$10 to \$12 to produce a check, it is clearly not cost-effective to prepare these checks. Some alternatives include paying certain small expenses with petty cash, through employee expense reports or with credit/purchasing cards, where such options are available and don't present a distortion of any AP or tax information.
- Multiple checks paid to the same or different payees for the same amount on various dates, especially a rounded amount. This circumstance raises a potentially questionable situation; as would a scenario where there were multiple payments to a single payee on a single date that may appear to split transaction(s), as noted above. The auditor who notes such circumstances should bring them to the attention of the client's finance management and further evaluate the payments to determine whether they are legitimate.

5. By invoice number, if available. Sorting check register data by invoice number shows such things as the frequency with which one vendor is used, which highlights whether the company may be a large customer of that vendor. If there are only small gaps between invoice numbers over the test period, the company may represent a sizeable portion of their invoicing and be a large customer.

As a large customer, the company could be in a better position to negotiate requests to minimize the frequency of payments to the vendor. If the data reveals that all the invoice numbers are in sequence for a particular vendor, the auditor should raise the question of possible fraudulent invoices. In addition, all payments and supporting documentation should be reviewed knowing that the invoices may have been inserted in the AP process for frequent, or small payment of amounts that may not receive any scrutiny (such as checks under \$200, that may not be subject to manual signature).

There is additional support for further evaluation of check register data by applying Benford's Law, a simple theory regarding the naturally occurring frequency of numbers. It has some relevant application that could lead to the identification of suspicious transactions, based on the frequency of number appearance in the check register. For instance, checks for rounded

amounts or ending in the same digit(s) could be highlighted for further review using Benford's Law. Because it can also be applied to other financial accounts, such as payroll, those interested in further information are encouraged to find seminars available on this specific topic.

Looking for Clues

From the tests described above, the auditor should be able to determine whether any of the following circumstances exist at the client organization.

- Gaps indicating excessive check spoilage.
- Use of pre-printed check stock.
- Unusual vendor names/addresses.
- Frequent payments to the same payee.
- Multiple payments to the same payee.
- Excessive frequency of check processing.
- Very large or very small payment amounts.
- Unusual invoice sequences (sequential, out of order with date).
- Multiple small or unusual payments.

Based on his or her analyses, the auditor should be able to draw some conclusions and make potential cost-saving or control-improving suggestions.

- Laser printing checks for reduced cost and improved control.
- Review of vendor database contents and access controls.
- Reduced frequency of check processing to reduce costs.
- Reduced number and/or frequency of payments to payees to reduce check processing costs.
- Evaluation of controls over transaction splitting.
- Potential signs of fraudulent payments. (Such a finding would bear on the controls over the setup and management of the vendor database.)
- Potential for using various types of payment methods, including wire transfers, petty cash, employee expense reports, and/or purchasing cards.
- Potential signs of fraudulent invoices.

In cases where the client organization has multiple locations responsible for AP, even a modest finding, when extrapolated to all sites, could yield significant cost savings. Alternatively, the auditor may discuss with management the reasons for or against consolidation of accounts payable processing into a shared-service site.

Making it count

The auditor should — in addition to his or her GAAP analysis and other operational controls — incorporate the simple steps noted above into any AP process review. Cost savings and efficiency suggestions can help gain the respect of any audit client.

NATALIE FENNEL is vice president of internal audit for Power-One Inc.

Sticking to Their Principles

Will new recommendations designed to strengthen the Combined Code move the United Kingdom toward a more U.S.-style approach to corporate governance?

By ARTHUR PIPER

AS THE DEADLINE FOR CONSULTATION ON THE latest proposals to overhaul the United Kingdom's corporate governance regime approached this April, the clatter of gin-and-tonic glasses rising out of every London club reached such a crescendo that it was heard down the road by government policy-makers in Whitehall. The rather un-British public brawl that has surrounded recent proposals to rework corporate governance in the United Kingdom has uncovered a deep rift within the business community. And it has highlighted in a graphic way the differences in approach between governance policy-makers on both sides of the Atlantic.

A Battle Based on Principles

The tiff started in January when the ex-investment banker Derek Higgs and his colleague Sir Robert Smith published their separate government-sponsored reports, *Review of the Role and Effectiveness of Non-executive Directors* and *Audit Committees Combined Code Guidance*, respectively. The recommendations in these documents are designed to strengthen the Combined Code, which is followed as best practice by companies listed on the London Stock Exchange. Although companies are not bound by law to comply with this guidance, they do have to explain any deviations to increasingly active shareholders.

The scuffle for attention among those who oppose and support the reforms has been unseemly. The opposition, in particular, has taken off the verbal gloves. Sir Nigel Rudd, one of Britain's most influential industrialists, led the opposition charge with a high-profile attack in the United Kingdom's business bible, the *Financial Times*, complaining that Higgs' reforms could seriously harm the city of London's financial center. Sir Nigel, who is non-executive chairman of the glassmaker Pilkington and the motor dealer Pendragon, said some of Higgs' suggestions were "absolutely barmy" and could undermine good corporate governance in the United Kingdom. "A lot of what Derek Higgs said is common sense, but you could say it was stating the bloody obvious, and what good companies do already," he told the *Financial Times*. "I increasingly come to the conclusion that we didn't need [the review]. Other executives at FTSE 100 companies (the top 100 businesses listed on the London Stock Exchange), including Niall FitzGerald, chairman of Unilever; Sir Christopher Bland, chairman of British Telecommunications; and Donald Gordon, chairman of the retailer Liberty, hold similar views. Behind the circus of the public row is a serious issue about whether the suggested amendments to the Combined Code, which have the backing of the government, will preserve or destroy the United Kingdom's cherished principles-based approach to corporate governance.

Many believe that Higgs in particular introduces so many requirements that it is simply legislation by the back door. This, they complain, will lead to a box-ticking culture that will see companies going through the motions in their annual report and accounts to keep shareholders happy, while ignoring the spirit of good governance because it has become too onerous. What is

needed, they conclude, is a light touch to good practice, where those who are remiss are gradually embarrassed into compliance by peer pressure.

This approach has been the blueprint for the United Kingdom system since the Cadbury Report formally adopted it as best practice in the early 1990s. Although directors in the United Kingdom are now rather glibly saying that financial scandals such as those at Enron, WorldCom, and HealthSouth are a U.S. phenomenon born out of prescriptive, box-ticking American corporate governance practice, those with longer memories will recall that Turnbull grew directly out of the ordure known as the Maxwell pensions scandal. Those were the heady days of British malfeasance. The government report into Robert Maxwell's Mirror Group Newspapers (MGN) revealed that he had bullied the non-executive directors (NED) — Sir Robert Clark, Alan Clements, Lord William of Elvel, and Joseph Hains — into a state of inertia. Their careless behavior compounded financial problems at the company and while three of the NEDs had financial experience, they failed to meet regularly or check what financial controls existed at MGN for fear that Maxwell would "proceed all over them" — in the words of the financial adviser Samuel Montagu. Hundreds of thousands of people lost their pension rights, and Maxwell's companies collapsed.

Higgs on Good Governance

In light of such a background, it is perhaps not surprising that Higgs follows the line taken in the Cadbury Code — and updated by the Turnbull Report in 1999 — that if you get the right people into the right business structures, good governance practice will flourish without the need for onerous and commercially restrictive legislation. That is why Higgs focuses on the role of executive and non-executive directors. Although the U.K. business community believes that it does a good job of attracting the right quantity and quality of people onto executive boards, good independent NEDs have been hard to come by, and much of Higgs' efforts are aimed at improving the NED "gene pool."

Higgs recommends that at least half the members of a company's board, excluding the chairman, should be independent NEDs. In addition, he says that no individual should chair more than one FTSE 100 company and that the roles of chairman and chief executive should be separated. Higgs also suggests a definition of the term *independent* for inclusion in the Code to replace the confusing number of definitions that have sprung up among institutional investors, analysts, and businesses. At present, about one in four boards of the FTSE 100 companies

British Boards

The board structure in the United Kingdom is unitary, meaning that there is a single body of directors responsible for making decisions on all of the company's activities. However, to provide a balance of views on the board, the Combined Code says that it is best practice for all boards to appoint a number of non-executive directors whose role it is to ask strategic questions about the business' activities. These people are supposed to be "independent" in the sense that they do not have any financial connection to the business — except for a salary — for working the 20-or-so days a year that they spend on company affairs. They are not generally rewarded by share options. The Higgs and Smith reports enhance the role of non-executives, particularly on audit committees where such groups are expected to be composed solely of non-executives.

have fewer than 50 percent NEDs, according to a recent survey by head-hunting agency Armstrong International.

The Higgs report also provides an extensively detailed account of how NEDs should be appointed and the extent of their roles and responsibilities. NEDs who have been offered an appointment are expected to conduct their own due diligence of the company in question "to satisfy themselves that they have the knowledge, skills, experience, and time" to do the job. On acceptance, the company would have to offer the NEDs a comprehensive induction program — presumably including a look at the internal audit function — and the chairman would be responsible for making sure that resources are available for the ongoing development of all directors. In addition, Higgs proposes that NEDs should be paid, but not through share options.

More controversial, however, is the creation of a new type of NED — the senior non-executive director. The report says: "The senior independent director should be available to shareholders if they have concerns that have not been resolved through the normal channels of contact with the chairman or chief executive." As well as having to attend the company's annual general meeting, this super-NED would also have to "attend sufficient of the regular meetings of management with a range of shareholders to develop a balanced understanding of the themes, issues, and concerns of shareholders." He or she would then discuss these matters with both the executive and non-executive members of the board. Higgs proposes other measures to bring NEDs and investors together and supports moves by the government to encourage a more active approach by institutional investors to portfolio management. Sir Stanley Kalms, former chairman of the U.K. electrical retailer Dixons, is among those who have warned that the creation of a super-NED position would lead to the kind of two-tier board prevalent on continental Europe but criticized in the United Kingdom because it is seen as too unwieldy.

From Smith's Perspective

Fortunately, internal auditors do not need to worry too much about the Higgs report, which goes into tedious detail in its 126 pages about who should sit on the board. But auditors do need to worry about the Smith report, which will directly shape how companies are run in the future and what is expected of internal auditing. Sir Robert's review recommends that audit committees contain at least three NEDs, all of whom should be independent under the Higgs definition. At least one audit committee member should also have "significant, relevant financial experience," and the audit committee itself should be given sufficient resources to perform its duties. These recommendations mirror those rules set down by the U.S. Securities and Exchange Committee (SEC) in its endeavor to turn the Sarbanes-Oxley Act of 2002 into workable legislation.

Sir Robert's report also spells out in greater detail the roles and relationship between audit committees and the internal audit function. It says that the committee's role should include "reviewing the company's internal financial control system and risk management system unless the latter is addressed by a separate committee or board" and "monitoring and reviewing the effectiveness of the internal audit function."

The Combined Code also gets amended under the Smith report to state that companies without internal auditing must consider annually their need for such a function and explain their decision

not to have one in the annual report and accounts. In other words, it has set the principle that directors need to convince investors that it is a good idea not to have internal auditing. The New York Stock Exchange, on the other hand, has adopted a listing rule that has made internal auditing mandatory.

The Smith report goes on to say: "The audit committee should review and approve the internal audit function's remit, having regard to the complementary roles of the internal and external audit functions. The audit committee should ensure that the function has the necessary resources and access to information to enable it to fulfill its mandate, and is equipped to perform in accordance with appropriate professional standards for internal auditors." It adds by way of a footnote that the standards it has in mind are those of The IIA Inc.

In fact, the audit committee would become the main conduit to the board and to shareholders for internal auditors. The finance director in many companies currently performs this role. As well as approving the appointment and termination of the head of internal auditing, the audit committee would also work to ensure that "the internal auditor has direct access to the board chairman and to the audit committee and is accountable to the audit committee." In addition, the audit committee would work closely with heads of internal auditing to review and assess the annual internal audit work plan; receive regular internal audit reports; review and monitor management's responsiveness to the internal auditor's findings and recommendations; meet with the head of internal auditing at least once a year without the presence of management; and "monitor and assess the role and effectiveness of the internal audit function in the overall context of the company's risk management system."

A Closer Look at Turnbull

There is little doubt that when the ink is dry on the revised Combined Code, it will look like a pretty robust system of corporate governance in principle. But what will happen in reality? The auspices do not look good. But before exploring why, it is worth remembering that Sarbanes-Oxley needs measuring primarily against Turnbull, as this will be the underlying basis of the United Kingdom's new regime. It also gives an indication of how companies are likely to adopt the new principles.

Ernst & Young has pointed out that many U.K. companies feel that Sarbanes-Oxley does not introduce any new requirements, but that they are wrong in this belief. (See "[Turnbull vs. Sarbanes-Oxley](#).") Most importantly, the legislation introduces the requirement that directors have to say that their internal controls are effective. Turnbull simply asks directors to say that they have reviewed them, not to say that they actually work in practice.

This leaves an enormous potential gap in the U.K. governance regime that Higgs and Smith fail to address. It means that shareholders and stakeholders are relying on company directors to embrace the spirit of good governance in following set principles. But an extensive new survey by the accountant Grant Thornton found that 81 percent of FTSE 350 companies had "failed truly to embrace the principles championed by Nigel Turnbull." A dismal 36 percent of companies complied fully with the recommendations of the Code five years after it was published. And although 94 percent of companies who disclosed noncompliance stated in what

areas they were noncompliant, many did not take the additional step of explaining why they did not comply.

Survey report author and head of risk management services at Grant Thornton, Simon Lowe, says: "It appears that most companies are merely paying 'lip service' to the guidelines. The research indicates that embedding corporate governance best practice into the culture of an organization is still a long way off for most companies. Instead of wholly embracing the changes, companies are merely ticking boxes to ensure that they comply with the bare minimum, rather than embracing the spirit. The annual reports are one of the few avenues open to them to demonstrate their commitment. If they cannot or will not use them, then shareholders and potential investors may have to assume the worst."

This finding should shed new light on criticisms that have been made about Higgs and Smith. For example, Don Cruickshank, outgoing London Stock Exchange chairman, has said that the proposals would force "companies to resort to box-ticking." However, it looks as though his warning has come too late if the findings from Grant Thornton are to be believed. There has always been a concern that the United Kingdom's principle-based approach suffers from a fatal flaw: The companies that follow the principles are the well-run ones that have good governance anyway, whereas the minority that sail close to the wind will have no qualms about doing what they please. It may well be the case that the principles-based approach that is lauded in the United Kingdom is actually far less effective than the U.S. model that is so heartily derided.

Whatever the answer to this question might be, U.S. internal auditors and their U.K. counterparts are going to be in for a tough time. If executives are going to have to attest to the fact that their internal controls are effective in the United States and be able to comment on their effectiveness in the United Kingdom, internal auditors are going to have to provide that assurance. Internal audit functions are themselves going to be assessed for effectiveness. In a recent report, KPMG said that 71 percent of NEDs at FTSE 350 companies believed that they would need to "exert greater oversight of the quality of the company's internal controls" — in other words, scrutinize the internal audit function more closely. But is there a single methodology for "monitoring and reviewing the effectiveness of the internal audit function" as called for by Smith? Is that something that should be left to the NEDs to conduct, as Smith suggests?

Moving Forward

The U.K. government has said that it does not intend to water down the proposals recommended by either Higgs or Smith, but it has recently agreed to extend the time business can consult on the recommendations. The Financial Reporting Council is currently redrafting the Combined Code to take their suggestions into account. It may be that the principles-based approach will continue to thrive on the Continental side of the Atlantic, while rules will remain the norm in the United States. But if companies on either side of the ocean fall back on simple box-ticking, it could prove a bleak day indeed for good corporate governance.

ARTHUR PIPER is publisher of Internal Auditing & Business Risk, the magazine of the IIA—U.K. and Ireland, and director of Smith de Wint, an editorial services company.

Turnbull vs. Sarbanes-Oxley

ALTHOUGH MANAGEMENT HAS ALWAYS BEEN responsible for internal controls, they now have to prove they work. On the face of it, both Turnbull and the Sarbanes-Oxley Act have the same objective — to safeguard shareholders' investment by ensuring there is a system of internal controls over the accounting and financial reporting of the company. The difference lies in the disclosures that management makes in its annual report:

Turnbull Requirement

Management must confirm it has reviewed the effectiveness of the company's system of internal controls throughout the financial reporting period.

Management is not required to report its assessment of the effectiveness.

There is no auditor attestation.

Sarbanes-Oxley Requirement

Management must assess the effectiveness of the internal controls and procedures for financial reporting.

The auditor is required to attest to, and report on, the assessment made by management.

Internal controls will need to be documented in considerable detail and subjected to rigorous audit testing.

[Back to main article](#)