# The Process of Internal Auditing

## 25. How is internal audit work actually performed?

Once a company forms an internal audit function, completes the risk assessment process and develops an internal audit plan that is responsive to the risk assessment, it can initiate individual internal audit assignments.

A framework for initiating and executing internal audit projects should include the following actions:

- **Confirm the audit assignment** (e.g., timing, purpose, scope) with the area or process to be audited (in some cases, it may be appropriate to not announce the audit, but to perform the work on a surprise or unannounced basis).
- **Complete appropriate planning** for the audit assignment. This can include the following:
  - Assess the risks of the specific area to be reviewed.
  - Develop a written work program.
  - Agree on scope, locations, sample sizes and period under review.
  - Develop a report format that will be effective.
  - Request and receive certain advance information from the area to be reviewed.
  - Access operating information, performance measures, etc., on the area to be reviewed.
  - Review any prior audits of this area by internal audit or other parties, such as regulators, external auditors and consultants.
  - Hold joint planning discussions with management and process owners of the area to be reviewed to learn their areas of interest and concern.
  - Consider whether self-assessment activities would be helpful.
  - Gather outside information on best practices.
  - Identify the internal audit resources to be assigned to the audit and ensure they have an appropriate level of experience and competency.
  - Determine if outside resources or guest auditors should be utilized, including information technology resources.
  - Consider formal entrance and closing conferences.
- **Execute actual internal audit work,** including evaluation of process and control design, as well as testing methods to determine control operating effectiveness such as inquiry, observation, examination and reperformance. Discuss and clear items noted and potential findings with management and process owners. For consulting engagements, perform agreed-upon work steps to meet the objectives of the assignment.

- **Develop a report** or other appropriate communication method responsive to the work completed and findings made. Areas that might be considered include:

  – Executive summary of major issues and findings

  – Background, objectives and scope

  – Audit findings, including management's action plan for addressing these findings

  – Other analysis and information, including appendices

  The format of internal audit reports varies by company. What is most important is to create an approach that is effective at communicating key issues and achieving positive change and resolution to the issues reported. For example, some companies may find that single-page reports are effective. Others may find that management should respond separately and apart from the audit report itself.

  In addition, the circulation of a draft report for discussion is often an appropriate and effective way to refine wording and ensure the accuracy of all information in the report.

- **Develop an effective method for tracking and following up** on audit findings and agreed-upon actions by management. This may include recording all findings in a database, scheduling follow-up audits or conference calls, or requesting status from the auditee. It may even include having management of the audited area report to senior management and the audit committee. Internal audit should also determine the extent to which resolution of auditing findings should be validated independently.

There is no one-size-fits-all approach to the execution and completion of internal audit work. Internal audit leadership, management and the audit committee should work together to create an approach that is most effective for their respective organizations. The IIA *Standards* and Practice Advisories can also provide guidance and a framework to follow.

## 26. Should an internal audit function consider information technology risks?

Absolutely. IT general controls and application controls are key and pervasive to the management of risk. The importance of considering information technology risk is supported by The IIA's *General Audit Guide No. 4 - Management of IT Auditing* (GTAG 4), which states:

> **Evaluate IT-related Risk** – It is clear that the evolution of IT introduces new risks into an organization. This guide will help the CAE understand how to best identify and quantify these IT-related risks. Doing so will help ensure that IT audit procedures and resources are focused on the areas that represent the most risk to the organization.

GTAG 4 also states:

> **Emerging Issues** – IT evolves rapidly. This evolution can introduce significant new risks into an organization. The world class CAE focuses IT audit attention on not just the basic building blocks of IT, but also new and emerging technologies. A section on emerging issues will provide specific information on a number of emerging technologies, evaluate the risks that these technologies pose to an organization, and provide recommendations for how the CAE should respond to these risks.

Failing to consider the impact of IT will result in an incomplete and ineffective internal audit function. An internal audit function should be driven by risk, and in today's business, technology has a direct relationship to risk. Technology both enables key controls in the business process or function and brings certain inherent risks. It is critical to understand how technology risks impact the overall risks to the organization. For instance, if a company considers technology a strategic business differentiator for certain business processes, the risk around the applications, technology and components related to those processes becomes more critical to the success of the business.

Technology enables controls such as segregation of duties and limiting the execution of transactions to only those intended by management (through application security and its appropriate administration). In addition, technology provides critical controls through the programmed logic in the applications, which validates transactions, performs appropriate calculations accurately and completely, and handles error and reasonableness checks.

The inherent risks around technology include the security of the company's network and data, computer networks and related data, which are subject to internal and external risks from hackers, disgruntled employees, corporate espionage and individuals who may want to disrupt the business or learn its secrets.

As highlighted in GTAG 4, technology risks evolve on an ongoing basis. New control challenges such as Wi-Fi, remote access and global networks present an ever-changing and dynamic risk profile. Therefore, IT is an integral part of any internal audit function's focus and capability. Generally speaking, all internal audit functions should have a measurable part of their activities concentrated on IT-related risks and issues. These activities should include stand-alone initiatives and initiatives that integrate technology risks and controls into the business process audit work. In certain instances, the entire business process may be automated and the business process audit is therefore related entirely to the technology involved. Coordinating these efforts with a company's CIO organization is critical.

Effective compliance with Section 404 also requires various documentation and evaluation efforts at both the general and application control levels, further underscoring the need for an appropriate IT capability within internal audit functions.

Given the breadth and rapid change of technology and its related risks, internal audit functions should consider what outside resources, if any, are needed to supplement their own skill bases in this area. In some cases, it may be prudent to avoid increasing full-time staff levels for certain forms of IT risks and issues, and instead rely on outside resources for recurring assistance.

## 27. What types of IT audit skills should be included in an internal audit department?

While specific skills required for IT audit may differ by industry and an entity's applications, there are a number of technology skills customarily needed for an IT audit department. As technology continues to evolve and become more interwoven with business processes, the skills of the auditor must evolve and change as well. We have defined a number of specific skills that may be required to complete an IT audit plan. These include:

- **IT risk assessment and planning** – At most organizations, performing an IT risk assessment requires a distinct set of skills. Risk assessment is an art, not a science, and the better one's understanding of how technology and business risks interrelate, the more on-target the risk assessment and audit plan will be. Effective IT audit planning requires knowledge of both internal auditing and technology risks.
- **IT governance and management** – Organizations are struggling to understand all that IT governance entails, and skills in this area are evolving quickly; they include IT portfolio management, return on investment considerations, issues around IT alignment and service to the organization.
- **Security and privacy skills** – The knowledge needed to audit and understand the security and privacy areas is complex and changing rapidly. A number of regulations impact security and privacy, including the Gramm-Leach-Bliley Act, HIPAA and Sarbanes-Oxley. One of the most important areas to many companies is around Payment Card Industry (PCI) credit card security standards and how personal information and data are handled and used.
- **Enterprise application controls – security and configuration skills** – Knowledge of how IT applications function is critical. Critical programmed controls include data validation and error-checking routines, reasonableness checks around certain key processing points, logical segregation of duties, and limitations on who can initiate and view transactions. In today's large ERP applications, these controls are a critical part of the configuration of the application. Skills are needed around how these programmed controls and configurations interact with the manual procedures. Industry-specific application skills also are needed.
- **Technology infrastructure components and configurations** – This area includes knowledge of critical technology infrastructure, such as networks, databases and platforms. A number of these skills relate to complex security and configuration requirements. In addition, there are needs around specific operational aspects for the technologies, such as backup, recovery and performance issues.
- **IT process skills** – A number of process skills are needed to audit IT processes. These include security administration in the application and technical component areas, business continuity and disaster-recovery planning, data center operations, application change management, infrastructure change management, and asset and service management.

- **Information strategy, data and records management** – Data is becoming more and more independent of applications. Data shared between applications must be owned and managed. Data management issues surround e-discovery and records retention requirements, as well as other key legal issues. A growing number of skills are needed to adequately address these areas at most organizations.

All internal auditors should have a base-level capability related to IT risks and controls. In many cases, deeper specialties are needed in specific applications, ERP systems and other areas discussed above. In a number of cases, organizations choose to develop an IT specialty practice within their internal audit department, given the magnitude and recurring nature of certain IT-related issues and risks.

Internal audit functions should evaluate the depth, breadth and frequency of their IT audit resource needs, and consider when and how external resources and organizations can be of assistance to achieve the best balance of people and skills.

## 28. What should we look for in an internal audit report?

A well-written internal audit report is a highly effective tool for management, the audit committee and the process owners affected by the report to bring about positive change and to improve controls, accuracy of information and the underlying process reviewed.

The audit report should consider the following questions:

**Objective and background** – Why was the area selected for audit? Was it due to inherent or perceived high risk, known problems, history of past issues, a management change, materiality of the area or other factors? What are the key aspects, risks and objectives of the area reviewed? Was it part of the original plan arising from the risk-assessment process?

**Scope** – What was the scope of the work and when was it performed? What time period and business units did it cover, and which facets of operations were included? What key risks did the work try to address?

**Findings** – What were the overall findings? How severe were they? Are there only minor issues to be addressed, or are there significant deficiencies in internal controls or the process being reviewed?

**Recommendations** – What actions must management take to adequately address the audit findings?

**Management action plans** – Is there a clear plan to correct the deficiencies noted? Who will take responsibility for the corrective action? When will the issues be corrected?

**Follow-up and tracking** – How is internal audit monitoring management's progress in addressing noted deficiencies? Quarterly and annual internal audit reporting to the audit committee should include tracking and confirmed resolution of management action plans resulting from audit findings. One measure of an internal audit function's effectiveness is the ability to foster positive and agreed-upon changes in the organization that produce an improvement and enhanced awareness of the management internal control structure.

See Question 25 for additional information on internal audit reports.

## 29. What is control self-assessment (CSA)?

CSA is a process through which internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance by those doing the work that all business objectives will be met.

The responsibility for the process is shared among all employees in an organization. CSA is conducted within a structured environment in which the process is thoroughly documented and, as an incentive for continuous improvement, is repeatable. The CSA process allows management and work teams directly responsible for a business function to:

- Participate in the assessment of internal control.
- Evaluate risk.
- Develop action plans to address identified weaknesses.
- Assess the likelihood of achieving business objectives.

The IIA believes CSA generates information on internal control that is useful to management and internal auditors in judging the quality of control. It can also positively influence the control environment. As operating staff buy into the process, control consciousness increases.

## 30. Is there a standard definition for internal controls?

Yes. The following definition is provided by the COSO Internal Control – Integrated Framework. The SEC and PCAOB have acknowledged that the COSO framework is a suitable framework for purposes of evaluating internal control. Outside the United States there are other recognized and acceptable internal control frameworks that also include definitions for internal control and other suggested objectives.

Internal control is a process effected by an entity's board of directors, management and other personnel. It should provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

*Key Concepts*

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is effected by *people*. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.

Internal control is geared to the achievement of objectives in one or more separate but overlapping categories. Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. Although the components apply to all entities, small and midsize companies may implement them differently than large ones (smaller companies' controls may be less formal and structured). The components are:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. This is the foundation for all other components of internal control, providing discipline and structure.
- **Risk Assessment** – This component is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks should be managed.
- **Control Activities** – Includes the policies and procedures that help ensure management directives are carried out.
- **Information and Communication** – This component consists of processes and systems that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- **Monitoring** – Consists of the processes that assess the quality of internal control performance over time.

## 31. How does the COSO internal control framework relate to internal auditing?

The COSO Internal Control – Integrated Framework impacts internal auditing in two important ways. First, it provides a context for the internal auditing activity by including it as part of the "Monitoring" component of the framework. COSO states that internal auditing is a periodic monitoring technique. Second, the framework provides a foundation on which to plan, execute and report on the results of the internal audit plan. The framework:

- Provides authoritative criteria for documenting, evaluating, testing and improving internal control.
- Supports training of internal auditors, management and process owners as to the components and attributes of internal control.

- Facilitates the articulation of the scope of the internal audit plan.
- Provides a common language for use during presentations at all levels of the organization.
- Provides a stepping-stone for implementing the COSO ERM framework released in September 2004.

Now that COSO is recognized as the framework of choice for purposes of management complying with Section 404 of Sarbanes-Oxley, most internal auditors are likely to adopt it for their use. Many internal audit departments already have adopted COSO and have found it to be an effective internal control model.

## 32. Are internal auditors required to follow COSO?

No. However, because the SEC and PCAOB recognize the COSO framework as suitable and available for management's assessment of ICFR, as required by Section 404, the PCAOB based its performance and reporting directives in its internal control auditing standard on the framework. Further, the COSO framework has clearly emerged as the framework of choice in the United States.

Though not required to be followed by internal auditors for their internal audit work, COSO's widespread recognition as the preferred Section 404 framework suggests that adopting COSO as the standard for internal audit work related to internal control is appropriate. As one of the founding COSO members, The IIA strongly supports COSO as a preferred internal control framework.

Outside of the United States, other similar control models have been developed and adopted. These include:

- CoCo (Canada) – The Criteria of Control Board of the Canadian Institute of Chartered Accountants (CICA) issued Guidance on Control in 1995, a framework for making judgments about control. There are large areas of overlap and consistency between COSO and CoCo, although they differ in some respects.
- The Turnbull/Cadbury Report (England) – Also called the *Combined Code of Corporate Governance*. Calls for companies to embed risk management and risk controls within the organization.
- KonTraG (Germany) – Act on Control and Transparency in the Corporate Sector provided corporate governance reform.
- King Report on Corporate Governance for South Africa – 2002 (King II Report – South Africa) – The Institute of Directors and the King Committee on Corporate Governance issued this report to promote high corporate governance standards in South Africa.

## 33. What is the COSO ERM framework and what is its relevance to internal auditing?

Following the development of the COSO Internal Control – Integrated Framework, COSO released the enterprise risk management framework in September 2004. The ERM project was initiated to develop a conceptually sound framework providing integrated principles, common terminology and practical implementation guidance supporting a company's programs to develop or benchmark its enterprise risk management processes.

As set forth in the executive summary of the COSO ERM framework, every entity, whether for-profit, not-for-profit or a governmental body, exists to provide value for its stakeholders. All entities face uncertainty; the challenge for management is to determine how much uncertainty the entity is prepared to accept as it strives to grow stakeholder value. ERM provides a framework for management to effectively deal with uncertainty and associated risk and opportunity, and thereby enhance its capacity to build value.

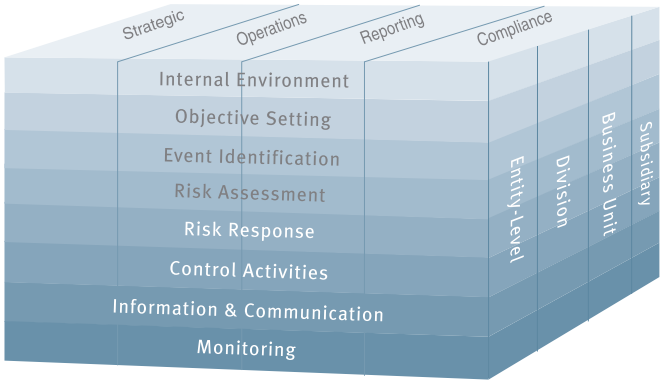
The COSO ERM framework bolsters, supports and extends aspects of the original COSO internal control framework. The framework is based on eight key components:

- Internal environment
- Objective setting
- Event identification
- Risk assessment

- Risk response
- Control activities
- Information and communication
- Monitoring

Also included in the conceptual approach is a mandate for coordination of all of these components in order to achieve the maximum effectiveness of a company's risk assessment process.

Similar to the COSO Internal Control – Integrated Framework, the COSO ERM framework is depicted in a cube-like fashion.




Thus, in terms of relevance, since COSO is the current definitive standard for internal control, the COSO ERM framework is seen as a definitive standard as it relates to risk assessment. As internal audit functions complete their risk assessment processes, they should look to the COSO ERM framework as a possible approach to complete this activity.

The IIA, a member of COSO and a participant in the development of the COSO ERM framework, supports its use by internal auditors. This framework provides a benchmark with detailed guidance for internal auditors to use in the evaluation of their organization's risk management efforts. It also suggests guidance on various risk management processes and tools to consider when implementing or strengthening an organization's ERM process.

COSO comprises the following organizations:

- American Institute of Certified Public Accountants (AICPA)
- American Accounting Association (AAA)
- Financial Executives International (FEI)
- The Institute of Internal Auditors (The IIA)
- Institute of Management Accountants (IMA)

The framework can be found at www.erm.coso.org.

## 34. Are there specific performance measures for internal auditing?

Like any function or process within an organization, appropriately developed performance measures help to drive results, performance, quality and continuous improvement. Internal audit should also have its own set of performance measures or key performance indicators.

Example performance measures for internal audit could include:

*Quality*

- Customer/process-owner satisfaction scores from auditees
- Audit committee and management evaluation scores
- External audit evaluation score from company's external auditor
- Upward feedback scores on CAE and internal audit managers from internal audit staff
- Percentage of internal audit staff with CIA or other relevant certifications
- Performance evaluation scores on internal audit staff
- Control breakdowns/deficiencies in areas recently reviewed by internal audit
- Internal control scorecard results by major area within the company
- Results of internal and independent quality assessment reviews

*Cost*

- Percentage of fully loaded internal audit cost as a percentage of company revenues and assets
- Actual cost per internal audit report and average
- Average cost per internal auditor
- Cost per audit hour in total
- Cost per audit hour based upon actual audit work only, excluding administration
- Travel costs of the internal audit function and average cost per trip
- Training cost and training cost per auditor
- Technology licensing costs and other outside costs
- Costs related to use of outside resources

*Timeliness*

- Report cycle time from completion of fieldwork to issuance and finalization of report
- Budgeted hours versus actual hours by individual audit
- Percentage of audits called for in the audit plan that are not yet complete
- Unresolved/incomplete recommendations from prior audit reports
- Average length of audit assignment in person hours or weeks
- Major risk areas not audited in the last year
- Aging/status of open, unresolved audit findings (especially those beyond their due date)

*Other*

- Degree of reliance on internal audit work by external auditor
- Turnover rates
- Percentage change rate in the annual audit plan
- Percentage of assets, revenues, locations, business units, etc., covered by the internal audit plan
- Linkage of key risks to specific skills of the internal audit team
- Degree of IT-related audit work relative to total audit effort

A selected number (approximately six to 12) of key performance measures should be agreed upon between internal audit, the audit committee and management. Having too many measures is not productive in the long run, nor is utilizing too few. Also, a balanced scorecard of measurements focusing on cost, quality and timeliness will help to drive the most effective result for a company. Of course, companies should develop their own specific measures that best meet their needs.

Reporting of these measurements at least annually is appropriate in some cases. However, certain measurements might be reported at each audit committee meeting or more frequently than once a year.

## 35. Should internal audit departments consider using an automated work paper software package?

Yes. Automated work paper software packages are becoming best practice. They provide an organized, efficient approach to completing and documenting internal audits. The software often allows team members to share and review work papers at any time or at any stage of the audit process. The automated tool can also be used to boost efficiency and serve as a capacity multiplier for understaffed departments. Other benefits of using work paper software packages include:

- Creates a central and secured repository for all audit documentation.
- Enables multiple users to access documentation at the same time.
- Enables access to audit information and documentation regardless of location, time zone or stage of audit process.
- Improves ability to control and validate final version of reports and information.
- Provides a highly structured format to support the audit process, reporting, follow-up and document management.
- Potentially reduces document storage costs.

For many organizations, identifying the need for an automated work paper tool is an emerging process. Different factors drive the need for this type of software package. For example, an organization may be starting a new department or facing specific events, issues or key risks; a merger may bring together two sets of auditors; departments without audit technology may realize they have become inefficient; or firms with technology already in place may find that it is no longer effective and may need to update their current software package to properly assess governance, risk and compliance all at once.

Because of these evolving needs, it makes sense for internal audit organizations to assess the need for a tool during the annual planning process. When considering this need, internal audit departments should ask the following questions. If you answer "yes" to any of these questions, your department might be in need of an automated work paper tool:

- Is your internal audit department tasked with managing Sarbanes-Oxley compliance in addition to traditional internal audit responsibilities?
- Are you seeking a flexible, configurable application that will allow you to automate your audit process from risk assessment through reporting?
- Do you wish to achieve any of the following?
  - Improve audit efficiency, accuracy and quality
  - Automate issue tracking
  - Access prior or current work papers from remote locations
  - Perform the same audit multiple times in one fiscal year and compare results
- Are your current tools being used ineffectively?

- Have any of the following events recently occurred?
  - Change of leadership
  - Significant staff turnover
  - Significant technology event such as a changeover in company platforms

## 36. What factors should internal audit consider when issuing an opinion on internal control?

Senior management and the board often expect the CAE to communicate an overall judgment about the organization's risk management process and system of internal control. This opinion can be one of positive or negative assurance.

The IIA recommends in its paper *Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control* that when the CAE is issuing an opinion on internal control, he or she needs to consider the scope of the audit work and the nature and extent of audit work performed, and evaluate what the evidence from the audit says about the adequacy of internal controls. Such an opinion should express clearly:

- The evaluation criteria and structure used
- The scope over which the opinion applies
- Who is responsible for establishing and maintaining internal control
- The specific type of opinion being expressed by the auditor

The IIA also recommends that CAEs consider a few other items in this process:

1. Be careful that the opinion expressed is consistent with the internal audit activity's charter as approved by the board and supported by a sufficient amount of audit evidence.
2. Resist expressing an opinion related to a subject that is inconsistent with the charter.
3. Do not express an opinion that is not supported by sufficient audit evidence.
4. Understand fully the reason and proposed use of any opinion he or she is requested to use.
5. Ensure that any opinion is appropriate for its intended use and audience.

With regard to Sarbanes-Oxley Section 404, a number of CAEs have been asked to sign an attestation stating that internal auditing has evaluated ICFR and found either that the controls were effective or that they have material weaknesses or deficiencies. These attestations are often drafted based on the attestation to be signed by the CEO and CFO of the organization for inclusion in the annual filings with the SEC.

The IIA recommends that CAEs carefully consider the wording of such an attestation before signing it. Signing an attestation is similar in effect to expressing an opinion and is subject to the concerns discussed above. The IIA further recommends that CAEs consider:

- Whether a positive or negative assurance opinion is appropriate for the situation
- Limiting the opinion to the areas that have been audited according to the audit plan
- Not implying that the CAE has any management responsibility for internal control as part of his/her opinions expressed in support of Section 404
- Whether there has been any impairment of internal audit's independence and objectivity

## 37. What is an integrated audit?

A good way to think about an integrated audit is that it encourages a holistic approach to the internal audit process. To fully incorporate integrated auditing into an internal audit approach, auditors must be able to understand and assess the risks the organization faces at the strategic, operational and tactical levels. They also need to know about corporate governance, risk management and control models. Internal audit functions should consider moving toward using this audit approach if they are not already doing so.

In the past, the term "integrated audit" was used to describe performing a single audit to address both automated and manual controls and related risks at the same time. These days, the term refers to audits of internal control that are integrated not just across the process and IT areas, but also across all three spheres of the COSO model: financial reporting, regulatory compliance and operational effectiveness and efficiency. This brings to the forefront the importance of assembling and orchestrating teams with the right skills for these audits who will work in tandem.

Following the COSO frameworks can help a company perform an integrated audit. It is important to note that COSO does not demand the use of an integrated audit approach. However, if a company follows the COSO model in the audit planning and execution stages, it will likely conduct an integrated audit.

AS5 also encourages using an integrated audit approach when external auditors are performing the audit of ICFR and the audit of the financial statements to accomplish the objectives of both audits simultaneously. In addition, AS5 supports this approach through encouraging external auditors to rely on the work of others, where appropriate, when issuing an opinion on ICFR. The PCAOB believes this will help make the Sarbanes-Oxley compliance process more efficient and effective.

## 38. What is continuous monitoring and how does it strengthen the internal audit process?

In the *Global Technology Audit Guide 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment* (GTAG 3), The IIA defines continuous monitoring as "the process that management puts in place to ensure that policies, procedures and business processes are operating effectively. It typically addresses management's responsibility to assess the adequacy and effectiveness of controls."

This GTAG goes on to report that the key to continuous monitoring is for management to own and perform the process as part of its responsibility to implement and maintain an effective control environment. Since management is responsible for internal controls, it should have a means to determine, on an ongoing basis, whether the controls are operating as designed. By being able to identify and correct control problems on a timely basis, the organization's overall control environment can improve. A typical additional benefit to the organization is that instances of error and fraud are significantly reduced, operational efficiency is enhanced, and bottom-line results are improved through a combination of cost savings and a reduction in overpayments and revenue leakage.

Continuous monitoring can be achieved through automated technology or through manual processes and procedures. But before deciding on which approach to take, the key is for management to determine what works best for the organization to achieve the ultimate goal: strengthening the control environment. This goal is in line with the definition of internal auditing, which says the function should help "an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes."

When an organization effectively implements continuous monitoring processes, the amount of detailed testing required by internal auditors decreases. This further allows the internal audit function to employ a risk-based audit approach and focus on areas of the organization with the greatest need.

## 39. How can internal audit assist in developing and maintaining an effective corporate governance environment?

Internal auditors are part of the foundation on which effective corporate governance is built. By being involved in this arena, internal auditors can better fulfill the complete definition of internal auditing.

However, it is important to be clear that it is the responsibility of the board of directors to develop and maintain an effective corporate governance environment. The IIA states in the position paper *Recommendation for Improving Corporate Governance* that internal audit's role is to be "a critical, independent observer of that process." The IIA *Standards*, which follow the COSO model, acknowledge that evaluating the corporate governance environment is part of internal audit's role in the organization. This evaluation process in turn assists management (and thus the board) in developing and maintaining an effective corporate governance environment.

*Standard 2100 – Nature of Work* states that "The internal audit activity must evaluate and contribute to the improvement of governance, risk management, and control processes using a systematic and disciplined approach."

*2110 Governance* – The internal audit activity must assess and make appropriate recommendations for improving the governance process in its accomplishment of the following objectives:

- Promoting appropriate ethics and values within the organization
- Ensuring effective organizational performance management and accountability
- Communicating risk and control information to appropriate areas of the organization
- Coordinating the activities of and communicating information among the board, external and internal auditors, and management

The role internal audit plays in governance is highly influenced by the maturity level of the organization's governance processes and structure, as well as the roles and qualifications of internal auditors. Typically, internal auditors operate in two capacities regarding corporate governance. First, auditors provide independent, objective assessments on the appropriateness of the company's governance structure and the operating effectiveness of specific governance activities. Second, they act as catalysts for change, advising or advocating improvements to enhance the organization's governance structure and practices.

Internal audit should have a clear set of published audit objectives to ensure that corporate governance mechanisms such as the internal control systems, risk management processes and financial reporting systems are monitored at all times. By providing assurance on the risk management, control and governance processes within an organization, internal auditing can fulfill its role as one of the cornerstones of effective organizational governance.

## 40. To what degree should the internal audit function coordinate its activities with its external audit firm?

While internal and external auditors differ with regard to their relationships to the organization, the scope of their work, their audit objectives and their mutual interest in the organization's internal control structure should drive the board of directors to require coordinated audit efforts. Doing so will increase the economy, efficiency and effectiveness of the overall audit process and help the board fulfill its audit process oversight responsibilities.

The IIA recommends that internal and external auditors meet periodically to discuss common interests; benefit from their complementary skill, areas of expertise and perspectives; gain an understanding of each other's scope of work and methods; discuss audit coverage and scheduling to minimize redundancies; provide access to reports, programs and working papers; and jointly assess areas of risk.

Practice Advisory 2120-A1-4, *Auditing the Financial Reporting Process*, also outlines a number of roles the CAE may consider to better coordinate internal and external audit activities and ensure the reliability and integrity of financial reports. These additional efforts facilitate internal audit's role in supporting the organization's governance process and the governing board and audit committee's oversight responsibilities.

AS5 also emphasizes the importance of this coordinated effort through its "relying on the work of others" language and the importance of reviewing internal audit reports related to ICFR.

## 41. What should the role of internal audit be in connection with a company's compliance efforts?

Internal audit should most definitely be involved with a company's compliance efforts since "compliance with applicable laws and regulations" is an integral part of COSO's definition of internal control. However, it is important to remember that compliance efforts are management's responsibility. The role of internal audit is to verify that management meets that responsibility through the risk assessment and audit process. Ultimately, management must own the responsibility around compliance in the applicable locations and areas.

The IIA *Standards*, which follow the COSO model, acknowledge that regulatory compliance risk is part of internal audit's role. Compliance with applicable laws and regulations is an integral part of the definition of internal control. Internal audit's involvement in a company's compliance efforts is directly supported by *Standard 2100 – Nature of Work*, which says the internal audit activity must evaluate and contribute to the improvement of governance, risk management and control processes.

Standard 2120.A1 further notes that internal audit must evaluate risk exposures relating to the organization's governance, operations and information systems regarding the reliability and integrity of financial and operational information; effectiveness and efficiency of operations; safeguarding of assets; and compliance with laws, regulations and contracts.

## 42. Should an internal audit function coordinate its efforts with the company's chief risk officer?

A successful risk management process is truly an integrated effort and should involve a number of key players throughout the organization. Because of this, it is critical for the internal audit function to coordinate its risk management role with the company's chief risk officer (CRO).

The role of the CRO, like that of the CAE, has evolved in recent years from being a compliance officer to serving as a high-profile, board-level advisor. CROs now play a pivotal role in determining an organization's risk strategy and ensuring the completeness and consistency of the organization's risk management processes across different business areas. The risk management function's value increases when risk professionals partner with the business lines (including internal audit), and vice versa, to achieve better understanding of the business operations and associated risks.

The IIA *Standards* support internal audit's role in identifying and evaluating significant risk exposures to the company. This effort should be a normal and ongoing part of internal audit's duties and provides invaluable insight to the risk management process. Practice Advisory 2100-3 recommends that internal audit's role in risk management efforts "be codified in the charters of the internal audit activity and the audit committee."

This Practice Advisory further states that risk management "responsibilities and activities should be coordinated among all groups and individuals with a role in the organization's risk management process. These responsibilities and activities should be appropriately documented in the organization's strategic plans, board policies, management directives, operating procedures and other governance type instruments."

Such a coordinated effort is a win-win situation for the company. First and foremost, establishing a risk strategy enables an organization to determine the priorities of the internal audit plan. Creating a risk strategy also allows an organization to establish a framework for assessing risk. This framework can in turn act as the cornerstone of a company's ongoing risk management foundation.

## 43. What should the role of internal audit be in evaluating a company's use of outsourced services?

Outsourcing services traditionally executed internally by the organization is not a new phenomenon. For decades, this trend has been sparked by an increase in productivity through technological innovations or a change in geopolitical institutions to foster a supportive environment for business. This strategy brings with it significant risks that must be recognized and managed. If not properly managed, companies may negatively affect their operations – and their customers. The execution of a service can be outsourced, but the ownership of the service cannot. The risk for delivering the service stays with the company. Because of the significant operational and financial risks associated with outsourcing processes to third parties, the internal audit function should be continually involved in assessing the risks and internal controls related to the processes performed by the service provider.

Practice Advisory 2100-13, *Effect of Third Parties on an Organization's IT Controls*, outlines procedures to be performed by internal auditors in reviewing the risks and internal controls related to outsourced services. These include:

- Obtain and document an understanding of the relationship between the services provided by the third party and the organization's control environment.
- If third-party services are significant to the organization, assess these controls to determine whether they function as described, operate effectively and assist the organization in achieving its control objectives.
- Assess the likelihood (or control risk) that the IT environment has weaknesses in control existence, design or operation. The auditor should identify where the control weakness exists, assess whether the control risk is significant and determine what effect it has on the control environment.
- Review the contract (possibly with the assistance of the organization's legal counsel) to determine the third-party's role and responsibility for assisting the organization in achieving its control objectives.
- Identify and review the components of the third-party service provider's corporate governance process.
- Consider the contractual relationship between the organization and the third-party provider and the third-party provider's evaluation and reporting on their controls.
- Review reports from independent sources on the third-party provider's controls.
- Consider whether the third party has an internal audit department. The presence of internal auditors can enhance the strength of the control environment.
- If the auditor decides to directly review and test controls at the third-party provider, the auditor should:
  - Work with management and, as applicable, internal audit of the third-party provider to plan the engagement, set its objectives and scope of review, and determine timing, staffing needs and other issues.
  - Address issues such as access to third-party systems and assets, as well as confidentiality.
  - Develop an audit program, budget and engagement plan.
  - Validate control objectives.
- Determine whether the third party uses subcontractors to provide systems and services, as well as the effect the subcontractors may have on the third-party's controls.

Outsourcing is a critical component of many companies' processing capabilities, and all indicators point to outsourcing's continued growth. Organizations must establish ways to effectively manage and control their outsourced processes in order to meet the growing scrutiny of regulators, management and key stakeholders.