IPPF – Practice Guide

AUDITING THE CONTROL ENVIRONMENT

APRIL 2011

The Institute of Internal Auditors

Table of Contents

Executive Summary.......... 1

Introduction 2

An Organization's Control Environment 2

Scope and Approach to Auditing the Control Environment.......... 3

Practical Considerations in Auditing the Control Environment 6

How to Audit the Control Environment.......... 9

Evaluating Control Environment Deficiencies 10

Communicating Results 11

Appendix 13

Authors 34

Executive Summary

The control environment[1] is the foundation of an effective system of internal control. Most of the well-publicized failures (including not only Enron and WorldCom, but also the governance failures that led to the 2008 financial crisis) were, at least in part, the result of weak control environments. In the absence of a demonstrably effective control environment, no level of "design and operating" effectiveness of controls within business and IT processes can provide meaningful assurance to stakeholders of the integrity of an organization's internal control structure.

The *International Standards for the Professional Practice of Internal Auditing* (*Standards*) Glossary defines the *control environment* as:

The attitude and actions of the board and management regarding the significance of control within the organization. The control environment provides discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements:

- Integrity and ethical values.
- Management philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- Human resource policies and practices.
- Competence of personnel.

Central to any approach to auditing the control environment is the assessment of risks from failure of each one of the six individual control environment elements as defined in the glossary of the *Standards*. Upon determining the risks relating to each one of the six control environment elements, the chief audit executive (CAE) may consider including in his or her annual audit plan one or more audits of higher control environment risks. The CAE may choose to address these risks in (1) a single audit of the organization's control environment, (2) a series of audits focusing on aspects of the control environment, and (3) audits of controls over specific risks (i.e., the scope includes the assessment of controls performed within the control environment as well as within business processes). Since the audit of an organization's control environment will often involve discussion of sensitive issues, the CAE must plan and execute these audits diligently.

There are many practical considerations that the CAE should pay close attention to when planning and executing a control-environment related audit. First, there should be support or buy-in from senior management and/or the board or the audit committee for such an audit. Second, internal auditing's reporting structure should be sufficiently independent to ensure minimal or virtually no scope limitation of the audit team. Third, the CAE should clearly articulate and communicate the criteria to be used, for the benefit of the auditee and the audit team members, in assessing the control environment. Finally, due attention should be given to differences in business culture, language, local laws, etc., while conducting such audits in a global organization.

Because the audit of the control environment includes auditing "soft" controls, some of the traditional testing approaches and tools may not enable gathering of sufficient direct evidence of their effective operation. The auditor will need to think "outside-the-box" to gather sufficient, competent evidential matter in such audits to ensure that audit findings are not challenged due to lack of rigorous audit procedures and evidence.

Control environment deficiencies need to be evaluated individually and it should be understood how they interact with or impact other controls in the organization. The corrective actions sometimes may need to extend beyond the immediate control environment element being evaluated.

[1] Because "control environment" includes assessing an organization's culture, the reader of this Practice Guide is also encouraged to review The IIARF publication, "Best Practices: Evaluating the Corporate Culture," by James Roth, 2010.

Communication of the control environment audit findings involve many practical considerations such as determining the appropriateness of the standard audit report format, limiting the distribution of the audit report, confidential nature of the findings, timeliness, and involvement of the general counsel and the human resource (HR) function either as the co-executive sponsor or in a supporting role, etc.

Auditing the control environment or one or more of its elements either as stand-alone or part of other internal audits is not only consistent with the intention of various standards within the International Professional Practices Framework (IPPF) but is also value-added to the organization.

Introduction

The control environment is the foundation on which an effective system of internal control is built and operated in an organization that strives to (1) achieve its strategic objectives, (2) provide reliable financial reporting to internal and external stakeholders, (3) operate its business efficiently and effectively, (4) comply with all applicable laws and regulations, and (5) safeguard its assets. Part of the blame for the 2008 financial crisis and other prominent failures of the 21st century can be appropriately attributed to failures in the control environment.

The purpose of this Practice Guide is to provide guidance to the internal auditor on the significance of the control environment; how to determine which elements of the control environment should be addressed by engagements in the periodic audit plan; how to scope, staff, and plan such engagements; and which items to consider in performing related audit work, including evaluating and reporting deficiencies.

Focusing only on assessing and reporting on controls within business and IT processes without assessing and reporting on the related risk of control environment failures can miss the fundamental aspects of the organization's foundation. An entity's control environment is the foundation of an organization's entire internal control structure — financial, operational, and compliance — including safeguarding of its assets. Internal auditors need to consider the risk of control environment failures in the development of annual (and other periodic) audit plans as well as in planning each individual audit.

The *Standards* defines the *control environment* as "the attitude and actions of the board and management regarding the significance of control within the organization." Specifically, Standard 2130: Control states, "the internal audit activity must assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and by promoting continuous improvement." Furthermore, Standard 2130.A1: Control states "the internal audit activity must evaluate the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations, and information systems regarding the: reliability and integrity of financial and operational information; effectiveness and efficiency of operations and programs; safeguarding of assets; and compliance with laws, regulations, policies, procedures, and contracts."

An Organization's Control Environment

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published the *Internal Control–Integrated Framework* in 1992. It uses a very similar definition to that in the *Standards* Glossary referenced above. The Executive Summary states:

"The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control,

providing discipline and structure. Control environment factors include the integrity, ethical values and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility, and organizes and develops its people; and the attention and direction provided by the board of directors."

Guidance on Control Number 1 from the Canadian Institute of Chartered Accountants Criteria of Control (CoCo) Board[2] uses four criteria as the basis of understanding and evaluating the effectiveness of an entity's internal control structure: purpose, commitment, capability, and monitoring and learning. The criteria of commitment embodies shared ethical values, integrity, HR policies and procedures, authority, responsibility, and accountability, and an atmosphere of mutual trust — essentially the same as the 1992 COSO framework and The IIA *Standards* definitions.

Similarly, the original Turnbull Guidance, *Internal Control: Guidance for Directors on the Combined Code*, issued by the Institute of Chartered Accountants of England and Wales in 1999, states that, "a company's system of internal control will reflect its control environment which encompasses its organizational structure. The system will include: control activities, information and communications processes, and processes for monitoring the continuing effectiveness of the system of internal control."

While there may be differences in control language around the world, the intent and the principles are similar and consistent. An effective control environment functions like a keystone in an arch bridge without which, no matter what, the best material and craftsmanship cannot hold the bridge together. Auditing the control environment and assessing its effectiveness is an important part of an auditor's assurance responsibility.

Scope and Approach to Auditing the Control Environment

Even though the control environment has a pervasive effect on risk management and internal controls across the entity, any approach to auditing the control environment should include an assessment of the risks from failure of each individual control environment element and their interaction with each other. This Practice Guide uses the six elements described in the *Standards* Glossary definition of the control environment:

- Integrity and ethical values.
- Management philosophy and operating style.
- Organizational structure.
- Assignment of authority and responsibility.
- HR policies and practices.
- Competence of personnel.

The level of risks may vary across geography, business unit, process, etc. For example, the level of risk relating to integrity and ethical values may be higher in some locations than others. Some business units may have a more established and experienced workforce, leading to a significant reduction in the risks associated with competence of personnel than in business units where personnel turnover is high.

There are several examples of situations that might influence the assessment of risk of failure for one or more control environment elements:

- Compensation and incentive structures can contribute to inappropriate behavior or excessive risk-taking.
- A high rate of employee turnover in key functions can lead to a lack of experience and less reliable execution of controls. This may be the result of a number of failures in the control environment, including ineffective supervision and other HR process issues.

- The absence of a defined code of conduct and ethics and/or a whistleblower policy, the failure to establish an ethics hotline, the absence of a process to evaluate the effectiveness of the code of conduct and ethics policy, a high number of reported frauds, or management over-ride of established controls can all lead to inappropriate activity that is not detected and addressed timely.
- Key functions may be staffed by personnel who do not possess the necessary level of competence. The level of risk is heightened if there is a perception that they hold their positions by virtue of their relationship to senior managers, the promoters, or executive directors of the board.
- The board may not provide effective oversight over the conduct of the organization's operations, and may not understand and monitor the broad organizational control environment.
- Key managers in the organization may tend to make business decisions without clearly understanding the risks related to their decisions; management may not exhibit risk and control consciousness in its decision-making.
- Processes relating to defining job descriptions for key positions may be weak, background checks and/or reference checks are not consistently performed, or the organization has difficulty hiring and retaining qualified individuals.

Once the CAE has assessed the risks relating to each of the six control environment elements, he or she may include one or more audits of the higher control environment risks in the annual audit plan. The CAE may determine the frequency of auditing the control environment based on his or her assessment of risk of control failures associated with one or more of the control environment elements.

The CAE may decide to address the risks in:

- A single audit across the organization.
- A series of audits, each of which addresses selected aspects of the control environment (such as the ethics hotline, board and committee operations, etc.).
- Audits of the control environment within selected divisions or operating units[3].
- A variation of the above.

For instance, if individual operating units have their own ethics policies and autonomous compliance committees, separate control environment audits at each unit may be the best approach. If each division investigates ethics violations based on organizational guidelines and tips from a centralized hotline, an organizationwide audit focusing on the hotline combined with local audits focusing on the investigations may be more relevant. If new personnel hiring and screening is considered an important control environment activity and this process is centralized, an organizationwide audit may be the best approach.

Although the initial scope and approach can be altered over time as better assessments and knowledge of the organization's control environment comes to light, the CAE should consider:

- What are the control environment elements and their attributes (ethics policy, board governance, compliance, fraud detection, etc.) that are key to the entity's control environment?
- How are these elements and related attributes managed during day-to-day operations? Is there clear accountability across the organization?
- Can these elements and attributes be managed effectively and efficiently in the scope of one large audit or would separate focused audits of each principle and related attributes be more effective and efficient?

[3] Risks related to the control environment at a location or within a business unit might also be included as part of the scope of broader individual audit engagements of that location or business unit. For example, an audit of a factory in China might include assessments of control environment elements (such as code of conduct and ethics awareness) as well as controls over inventory and procurement. An audit of the shared service center in Ireland might include assessments of HR practices in addition to general ledger and accounts payable controls.

- Does the balance of centralized versus decentralized operations within the organization influence how the control environment operates and thus the nature of audit work?
- What combination of control environment audits will allow the CAE to provide assurance to senior management and the board regarding the organization's system of internal control?
- Should the control environment audit be one annual audit, one audit occurring periodically every few years, or separate focused audits each year on different principles rolling up into a review of all control environment principles every few years?
- If the control environment has not been reviewed previously, what knowledge is there that would guide the decision on the audit approach? Would a high-level risk assessment of all control environment principles provide a basis for decisions? Should a first year audit be different than the ongoing audits that have been put in place in the audit plan?
- Should any aspect of the control environment assessment be performed at the direction of legal counsel; for example, those pertaining to investigations?
- Are adequate audit resources available?
- Are there any explicit senior management and board preferences (e.g., a stated desire to have the assessment completed by a certain date)?

As noted earlier, the audit plan may include a single audit of control environment risks. It may also include multiple audits, each addressing separate elements of the control environment, or control environment elements in different locations or business units. Where the plan includes multiple control environment audits and the CAE is planning to provide an overall assessment based on the results of these individual audits, the CAE should:

- Determine, during the initial planning phase, the process that will be used to aggregate the results of the individual audits into an overall assessment of the control environment.
- Plan the individual audits so that differences in their timing do not impede the overall assessment. In the case of a substantial time lag between individual audits, it may be necessary to perform procedures to update the results of earlier audits to support the overall assessment.
- Consider staffing the audits in ways that would ensure continuity in the audit approach and consistency in the assessment process. Well-defined audit programs also could help in this regard.

Audits of the control environment often involve the discussion of sensitive issues, including the actions or inactions of senior management and the board. The internal auditor should consider the following issues during the planning phase:

- Whether specific skills will be required (e.g., requiring the use of internal or external subject matter experts). These skills may be provided through the use of guest auditors from other parts of the organization or from a co-source service provider.
- Whether conversations with senior management and the review of confidential documents require staffing the audit with mature, experienced personnel. In some situations, the CAE may decide to lead the audit and/or personally perform certain aspects (e.g., the review of executive compensation or the results of investigations involving senior management).
- Ensuring, through discussions well in advance of the audit, that the information required to perform the audit (especially any information considered confidential) will be available when required. In addition, the auditor should ensure that everybody asked to support the audit understands the need to provide the audit team with the information required timely. This may require the involvement of the sponsor.

Control Environment Implications for Individual Internal Audit Engagements

Effective management of risks involves evaluating and monitoring not only business process controls but also controls relating to the entity's control environment. If the effectiveness of the control environment is not considered in an audit engagement, there is a risk that the assessment of the adequacy of controls will be incomplete and perhaps even misleading or incorrect.

When defining the scope of any audit, the internal auditor should consider the level of reliance placed on the effectiveness of control environment activities, and the risk of deficiencies in the control environment. In some cases, these risks and the related controls will be included within the scope of the audit. In others, reliance will be placed on separate audits performed of the control environment or one or more of its six elements.

For example, when developing the scope of work for an audit of accounts payable (AP), the auditor should consider risks such as:

- AP staff and managers involved in the AP process (e.g., as approvers of invoices) are not familiar with the organization's expectations for ethical behavior.
- Hiring practices are not effective in staffing key AP positions with experienced personnel.

Audit procedures around these risks might be included within the scope of the AP audit. However, if separate audits are being performed that specifically address these risks — for example, as part of audits of the code of conduct and hiring practices — the auditor might want to make reference to, and rely on the results of, those audits rather than duplicate the work.

When the scope of work for an audit does not include coverage for control environment risks, that limitation should be clearly communicated to management or the executive sponsor during the planning phase and in the final report. The results of separate audits of the control environment should be considered when preparing the audit report:

- When the control environment audit has already been completed, the auditor should consider those results and include them in assessing whether the system of internal control — including those in the control environment — is adequate.
- When the control environment audit has not yet been completed, the auditor should consider acknowledging that fact and make it clear that the assessment of internal controls is based on the assumption that the control environment activities are effective. The auditor should consider revisiting his or her assessment of the adequacy of internal controls should the audit of the control environment result in the identification of deficiencies.

Practical Considerations in Auditing the Control Environment

Discussed below are some of the practical considerations that should be taken into account while planning, executing, and reporting on audits in this area.

Senior Management and Board Support or Buy-in

An audit of the control environment involves assessing controls that in many cases, directly and/or indirectly, are performed by or at the direction of senior management or the board. Whether the audit is of all or only one element of the control environment, consideration should be given during the planning phase as to whether the internal audit team will be challenged in its need for access to the pertinent individuals and required documentation. Actions may be required to mitigate and manage such challenges before the commencement of the audit. These actions might include:

- Discussing the need for access during the development of the audit plan.
- Ensuring that the audit charter provides for appropriate access.
- Obtaining the support and sponsorship of the board and/or the chief executive for the audit. In some cases, the support of the chief financial officer (CFO) or general counsel may be sufficient.
- Written communications from an appropriate member of the executive management instructing the organization to provide the required access and information.
- Attendance by the executive sponsor[4] at the audit's opening meeting.
- Meeting with key members of executive management who are in a position to enable access, early in the audit planning phase. The internal auditor should ensure that the executives understand what information and access is needed and why. Their concerns should be heard, understood, and addressed where possible. Escalation to executive management or the board may be necessary to resolve continued denial of access.

Internal Auditing's Position Within the Organization

The reporting structure for internal auditing also may be an issue. Standard 1110: Organizational Independence states that "the chief audit executive must report to a level within the organization that allows the internal audit activity to fulfill its responsibilities." When the CAE does not report to an appropriate level, his or her ability to perform an audit of the organization's control environment or its elements may be challenged. For example, the CAE may be directed not to assess certain elements of the control environment (e.g., competence of personnel in the finance function), or have only limited access to confidential information (such as board minutes or records containing discussions about allegations against senior management). This may be mitigated if the CAE is able to obtain strong support from the board or executive management, with a clear mandate that the audit team should be provided full access to the information required to perform the audit.

If the CAE is unable to ensure that the audit team will have full access to information necessary to complete an effective control environment audit, or will be unable in fact or perception to be sufficiently objective and independent in its assessment of the control environment, such scope restrictions and other limitations should be promptly reported to the board. The CAE should consider whether to pursue an audit with appropriate scope restrictions communicated in the report per the *Standards*. Such restrictions do not relieve the CAE of her/his obligation to report to the governing board on the importance and need to evaluate the control environment.

Criteria for Assessing the Control Environment

The audit planning process includes consideration of the end-product of the audit, in particular what criteria will be used for the assessment. As with other engagements, options include:

- An assessment of the controls included in scope using the organization's standard rating system, together with opportunities for improvement.
- The assessment of the controls using a defined control maturity model, in addition to the standard rating and opportunities for improvement.
- Assessment of controls as directed by the general counsel with a specific objective in mind.
- Benchmarking (between companies and/or between units/departments in the company).

[4] For the purposes of this Practice Guide "executive sponsor" is a member of the executive team or board who will actively support the completion of the audit.

The CAE should use judgment, in consultation as necessary with the board or executive sponsor or the general counsel, in determining what criteria will be used to measure the effectiveness of the control environment. The CAE should ensure the board, senior management, and management responsible for the area being audited clearly understand how the results will be communicated if they are different from the standard internal audit reporting process.

Whether the assessment will be of the design and operating effectiveness of specific controls or the overall quality of such controls using a particular control maturity model, the criteria for that assessment should be defined during the planning process and clearly explained to the engagement client including appropriate members of senior management. The CAE should consider discussing the criteria to be employed with management and obtaining its agreement if possible. Significant value to the organization can be obtained through such discussion and buy-in prior to beginning the audit.

Consideration of Local Culture and Values

Local culture and values should be considered when determining the criteria for assessing business conduct and other elements of the control environment. Business conduct and other standards and expectations are not uniform around the world, due in large part to differences in legal traditions, social and cultural values, and the structure of capital markets. For example, while there are traditions in some emerging markets for commerce to be enabled by payments to involved individuals and for purchases to be made from related parties, this practice is considered illegal under the U.S. Foreign Corrupt Practices Act (FCPA) and UK Bribery Act. Nations differ in their governance laws and regulations (e.g., on the requirement for independent members of the board and other governing bodies), or in other aspects of the control environment (e.g., some restrict the ability of employers to perform background checks on employees; in some geographies, practices related to the hiring and treatment of minorities are accepted that would be illegal in other countries).

Most multinational organizations have developed and published an organizational code of conduct that applies to all of their operations globally. In such cases, audits of the control environment already have a set standard on which the internal auditors should base their audit scoping, program, assessment, and reporting.

However, not all organizations have adopted global standards, or the global standards may need to be adjusted for the unit being audited to comply with local laws. In these cases, the internal audit team should, in consultation with appropriate management, seek an agreement on what criteria or standard the audit team will follow. This should be clearly communicated to operating management before the start of the audit. If the standards differ in any way from the organizationally published standards, the reasons for variation should be clearly explained.

The CAE should consider variations in culture, values, and practices, as well as the need for language skills,[5] in assessing risks relating to the control environment and in staffing each audit. The team should include individuals who are able to understand the context as well as the practices in each region and enable an objective, balanced, and fair assessment of the adequacy of the control environment practices.

Coordination with External Auditors

While it is clear that internal auditing's evaluation of an entity's control environment, or one or more of its elements, provides much needed assurance to senior management and the board of directors, the internal auditor should be aware that external auditors may not be able to place complete reliance on their work in assessing the control

[5] Lack of familiarity with the local business culture and language may present barriers to developing an effective understanding of differences in culture and behavioral norms from that of internal auditors' host country. Experience in, and understanding of, the local language and culture is likely to improve the auditor's ability to understand and assess compliance or lack thereof with organizational policies, standards, and expectations.

environment with respect to audits of the financial statements and the system of internal control over financial reporting. Depending on the external auditor's assessment, the external auditors may feel compelled to validate certain controls themselves to bolster their independence. Internal auditing should work with the external auditors during annual planning sessions to minimize duplication and ensure the board and other stakeholders understand: (a) the external auditors may only review those aspects of the control environment that relate to a risk of a material misstatement of the financial statements, (b) the external auditors may be required to perform some levels of independent assessment, (c) a review by internal auditing will generally address a greater range of risks (operational and compliance risks in addition to financial reporting risks), and (d) there is an opportunity for internal auditing to contribute to improvements in related processes through its greater understanding of the organization as a whole.

How to Audit the Control Environment

This section elaborates on generic tools and techniques to audit the control environment. The Appendix lists potential audit procedures that might be considered in developing an audit of an entity's control environment or one or more of its elements. The seven elements and attributes are taken from COSO's *Internal Control–Integrated Framework* control environment component.[6] The elements and attributes include financial, compliance, and operating effectiveness control objectives. The Appendix is presented only for illustrative purposes and is not intended to be complete or comprehensive.

An audit of some elements of the control environment will include a review of soft controls, such as those around ethics, integrity, competencies, behaviors, and perceptions. These are considered soft controls because it may be difficult to obtain direct evidence of their effective operation through traditional testing. Instead, self-assessments, surveys, workshops, or similar techniques may be better suited than traditional methods. Specifically:

- Employee surveys are frequently used in evaluating the success of management's efforts in establishing an effective control environment. These surveys provide useful measurements of the effectiveness of one or more control environment elements. Annual employee ethics compliance forms are another example.
- The CAE should use his or her network within the organization. The network is critical in discerning whether communication, tone at the top, management walking the talk, and effective supervision are present on a day-to-day basis.
- The internal auditor's knowledge of the organization's inner-workings is useful to further corroborate the effectiveness of soft controls.
- The value of "auditing by walking around" cannot be overstated. By being present, visible, and observant across the organization, auditors can identify those intangible clues that may lead to deeper assessments. Associates who trust they can provide concerns to auditors with an appropriate degree of anonymity are also valuable.
- Past audit results over control activities and the reaction and remediation from management also are good indicators.
- Internal auditors' participation in committees, taskforces, workgroups, and involvement in ethics and compliance program implementation and assessments provide valuable insights over extended periods of time.

As the above may provide primarily indirect evidence, the auditor must always ensure sufficient evidence is

[6] The seven control elements include the six from the Standards and one additional element — "Importance of the Board" — as defined by COSO.

obtained to support the audit conclusions and assessment. Wherever feasible, the auditor should not hesitate to employ data analytics to filter patterns and anomalies to generate hard evidence.

Controls related to other control environment elements (e.g., publishing an updated and appropriate code of conduct and obtaining references and performing background checks for new employees) may lend themselves to traditional audit techniques.

In planning the audit, the auditor should understand the different nature of soft and other controls, and select the most appropriate techniques.

Evaluating Control Environment Deficiencies

Control environment deficiencies generally impact multiple areas or processes and are essentially pervasive in nature. Deficiencies in control environment might be identified during audits that focus on (1) the organization's control environment, or one or more of its elements; (2) the control environment or one or more of its elements within a business unit, location, or equivalent; and (3) one or more control environment elements as part of other internal audits.

1. *Evaluating deficiencies found during an audit that is focused on the organization's control environment or one or more of its select elements.*

The internal auditor may choose to assess the deficiencies within the context of the control environment audit. In other words, the audit report may limit discussion to whether the individual control environment elements are effective. However, limiting the assessment in this way is likely to result in a failure to understand and act on the pervasive effect of the deficiency. Preferred practice is for the internal auditor to work with management and understand any or all implications for the management of critical risks and the effectiveness of related internal controls.

For example, deficiencies in the hiring process may lead to an inability to hire sufficient, competent personnel in the accounting function. As a direct result, key account analyses, bank reconciliations, and the resolution of unmatched cash receipts may not be completed timely.

When assessing deficiencies in control environment elements, the auditor should be alert to indicators that other affected controls are also failing. These controls may be business process, IT processes, or even other control environment controls. For example, a failure to hire sufficient staff can lead to shortcuts in processes. These indicators may point to a higher level of risk to the organization from the control environment deficiency.

The auditor also should consider the implications of multiple, related deficiencies in control environment elements. Some deficiencies may have a greater effect when they are both present than simple aggregation of their individual risks may suggest. For example, when the absence of new employee training in an organization's code of ethical conduct is coupled with the failure to obtain references and perform background checks on new employees, the risk of hiring potentially incompetent personnel — and even individuals with a criminal record — is exacerbated.

Even if the audit report is limited to disclosure of the deficiencies without consideration of their pervasive effect, the CAE should discuss the implications and related management actions with the board or audit committee.

The corrective actions required to address control environment deficiencies may have to be extended beyond the immediate control environment element; for example, to include greater monitoring of affected controls in business processes.

2. *Evaluating deficiencies found during an audit that is focused on the control environment within a business unit, location, or equivalent.*

In addition to the analyses discussed above, the auditor should determine whether control environment issues identified in a localized audit are indicative of more pervasive issues across the business units, areas, or processes within the organization. For example, if hiring practices in the divisions are deficient, could the related procedures, processes, and systems be deficient in other divisions? If there is a lack of awareness of the organization's code of conduct, is it due to the fact that the current version of the code was not posted on the corporate portal, thereby affecting all parts of the organization? Has the code been translated into local languages, to support all parts of the organization?

The internal auditor and the CAE should discuss the potential implications of local control environment deficiencies on the organization as a whole, and adjust the audit plan accordingly. In some cases, additional audit work may be required to assess whether the deficiencies are widespread rather than confined to the unit, country, etc. covered by the audit.

3. *Evaluating deficiencies found during an audit that focuses on the control environment or one or more of its elements as part of another audit (e.g., an audit of AP that includes assessing the competence of management and staff and awareness of the code of conduct and ethical expectations).*

Many of the issues discussed above also apply here. The internal auditor should confer with the CAE and consider whether the control environment issues that have been identified might extend to other parts of the organization. The audit plan should be adjusted accordingly.

The assessment of the overall system of internal controls for the business risks covered by the audit should consider whether the control environment deficiencies are compensated for or mitigated by other controls that are operating effectively within or outside the business unit/function/area that is being audited.

Communicating Results

When communicating the results of a control environment audit, the auditor should consider:

- Whether the standard audit report format, including the standard assessment scale, should be used. In some cases, senior management or the board may prefer a presentation rather than a standard audit report.
- In many situations, limiting the distribution of the report. This may be achieved in some organizations by clearly marking the report as confidential and thereby limiting its distribution. However, the CAE should clearly understand how and when findings of control environment deficiencies related to the system of internal control over financial reporting need to be communicated to the external auditors.
- Additional safeguards if the audit was performed at the direction of the general counsel, especially when there may be a need to protect the confidentiality of the report under client-attorney privilege or similar protective measures.
- Whether the audit did not include procedures relating to an element of the control environment that is relevant to the assessment. Such a scope limitation should be clearly reported in the final audit report, even if the exclusion is based on the risk assessment as discussed above.
- If the review of the control environment was performed as part of a risk-based business audit in line

with the audit plan, whether to include a discussion of issues related to the control environment as part of the audit or as part of a separate report on the overall control environment.

- Varying the timelines for issuance of the report based on:
  - Significance of the issues identified.
  - Timing of the quarterly attestation on internal controls over financial reporting and compliance.
  - The scope and objective of the audit.
  - The nature or sensitivity of the issues identified.
  - The audience of the audit report.

In addition, the CAE should consider the following specific factors in determining how to communicate the results of control environment audits.

Sensitive Information

In some situations, communication of risks within the control environment due to the nature of the control deficiencies may be considered sensitive or confidential. For example, if there is an issue at the senior management level that could have a potential adverse bearing on the perception of their integrity and represent a potential compromise of organizational values, the CAE should consult with appropriate members of the senior management team, especially the general counsel, and the board to determine the appropriate communication strategy and process — including how corrective action will be documented and monitored.

Identification of Significant Issues

If an audit of the control environment identifies issues of significance, the CAE should review the results of prior internal audits to determine whether earlier assessments should be revised. The results of this review should be communicated to senior management and the board. This may result in changing the audit plan mid-stream because of a potential change in the organization's risk profile.

Nature and Tone of Recommendations

Recommendations in the report should be practical with positive intent and should address the root cause for the identified control environment risk.

Follow-up of Recommendations

Much like other internal audits, the recommendations brought out in these audits should also be followed-up. Given the sensitive nature of the findings, the follow-up may be performed by internal auditing or by others in the organization such as the audit committee and/or the board of directors.

Appendix

The following is an example of audit procedures that use seven basic principles for a broad-based audit that assesses the control environment. The principles, as well as the elements and attributes, are adapted from COSO's *Internal Control–Integrated Framework* control environment component.[7] The elements and attributes include financial, compliance, and operating effectiveness control objectives.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS[8]
1. **Integrity and Ethical Values:** ***Basic Principle — Sound integrity and ethical values, particularly of senior management, are developed and set the standard of conduct for doing business.***		
Developed — senior management develops a clearly articulated statement of values or ethical behaviors that are understood by key executives and the board.	Senior management conveys the message that integrity and ethical values cannot be compromised, both in words and in actions. Senior management has developed a code of ethics that emphasizes the organization's expectation that employees will act with integrity in all actions related to their scope of employment. Senior management has developed a code of business conduct that emphasizes the organization's commitment to fair and honest dealings with customers, suppliers, and other external parties. Performance expectations and incentives are designed so as to not create undue temptations to violate laws, rules, regulations, and organization policies and procedures.	Conduct periodic, anonymous "pulse" surveys of employees as to the ethical attitude communicated by senior management. Review the existence and content of the organization's code of conduct and ensure a process exists for periodic updating of the code. Review the existence and content of the organization's code of business conduct and ensure a process exists for periodic updating of the code. Review the mix between fixed and variable elements in employee compensation plans, and the relative weighting on short-term financial performance in compensation plans. Review senior management's compensation system to understand if it unduly incents excessive risk-taking and the override of the entity's system of internal control.

[7] Adapted from "Internal Control over Financial Reporting-Guidance for Smaller Public Companies: Volume III, Evaluation Tools." COSO, 2006, pages 25-31 for Control Environment Principles, Attributes and related summary of Entity-wide Controls and Management Documentation. Auditors should consider obtaining and reviewing the COSO literature found at www.COSO.org for more in-depth guidance and methodology tools.

[8] The suggested control testing in many instances asks the internal auditor to obtain certain documentation. In practice the auditor may encounter situations where the documentation may be missing or may not exist. It is important that this lack of documentation be listed when appropriate as a significant audit finding by the auditor.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
1. Integrity and Ethical Values: *Basic Principle — Sound integrity and ethical values, particularly of senior management, are developed and set the standard of conduct for doing business.*		
Communicated — senior management communicates its commitment to ethical values through words and actions.	New employees receive a copy of the organization's code of ethics and code of business conduct and are trained as to how these guidelines apply to specific factual situations common to the organization's business environment. Existing employees are provided with updated copies of the organization's code of ethics and code of business conduct at least yearly, and receive periodic retraining on the application of these guidelines to the organization's business environment. Customers, vendors, and other external parties receive a copy of the organization's code of business conduct at least yearly, by inclusion in other mailings to these parties. Contractual arrangements with these parties should include requirements for adherence to the organization's code of ethics and code of business conduct.	Review the signed employee representation that they have read and understood the codes of ethics and business conduct and, for existing employees, their certification that they have not violated the codes during the past year and are aware of no other such violations (or, if they are aware of such violations, they have 1) communicated these violations as directed by their compliance or ethics office training and 2) if based on their perspective the violations have not been resolved, communicated the potential violations via their company's ethics hotline. Review organization training courses, including the process for ensuring that all employees attend these courses on the codes of ethics and business conduct. Review the organization's policy for including the code of business conduct in a yearly mailing to customers, vendors, and other external parties. Verify that the code of business conduct is included in mailings.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
1. Integrity and Ethical Values: *Basic Principle — Sound integrity and ethical values, particularly of senior management, are developed and set the standard of conduct for doing business.*		
Reinforced — the importance of integrity and ethical values is communicated and reinforced to all employees in a manner suitable for the organization.	The organization's newsletter (and other internal communication devices) highlights: a. Ethical dilemmas often arising in the organization's industry and how management expects employees to act in these situations. b. Ethical failures (with names disguised) and the consequences of these failures for both the organization and the employees involved. c. Ethical successes (with names retained and highlighted) with the situation described, the employee behavior, and why the behavior was consistent with organization guidelines.	Review editions of the organization's newsletter during the year to examine whether coverage of ethical dilemmas, ethical failures, and ethical successes are included.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
1. **Integrity and Ethical Values:** *Basic Principle — Sound integrity and ethical values, particularly of senior management, are developed and set the standard of conduct for doing business.*		
Monitored — processes are in place to monitor the organization's compliance with principles of sound integrity and ethical values.	All new employees are required to sign the code of ethics and business conduct indicating that they have read and understand these codes. All existing employees are required to sign an annual contract acknowledging that they have read the most recent versions of the code of ethics and business conduct and that they understand and are in compliance with these codes. HR or hiring department management monitor whether new and existing employees have completed the required training on the codes of ethics and business conduct. The organization has established a hotline — a reporting mechanism that permits anonymity, and preferably staffed by an internal group with a direct reporting relationship to the board or by an outside vendor — for receiving reports of suspected violations of the organization's codes of ethics and business conduct and publicizes the existence of the hotline.	Review the signed employee representation that they have read and understood the codes of ethics and business conduct and, for existing employees, their certification that they have not violated the codes during the past year and are aware of no other such violations (or, if they are aware of such violations, they have communicated these violations via the hotline). Review organization training courses, including the process for ensuring that all employees attend these courses, on the codes of ethics and business conduct. Review the existence of the hotline — including the organizational unit responsible for managing and overseeing the hotline. Examine the organization's efforts to publicize the hotline. Review a sample of calls received on the hotline and examine the appropriateness of investigation and resolution of allegations.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
1. **Integrity and Ethical Values:** ***Basic Principle — Sound integrity and ethical values, particularly of senior management, are developed and set the standard of conduct for doing business.***		
Deviations Addressed — deviations from sound integrity and ethical values are identified timely and are addressed and remediated at appropriate levels within the organization.	A senior executive, preferably with a direct reporting relationship to the board, is responsible for oversight of the organization's ethics and compliance function. Allegations of violations of the organization's codes of ethics and business conduct are appropriately investigated, and the necessary corrective, disciplinary, and remedial actions happen timely. This includes hotline reported matters.	Review the organizational unit, and related reporting relationships, responsible for oversight of ethics and compliance. Examine the appropriateness of investigations of allegations of violations of the organization's code of ethics and business conduct, including corrective, disciplinary, and remedial actions taken. Review the organization's investigation policies and practices to ensure that appropriately qualified personnel are performing the investigations. Evaluate the qualifications of the investigators and ascertain that there is good segregation of duties between investigations, operating management, and the discipline decision makers.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
2. Importance of Board*: Basic Principle — The board understands and exercises oversight responsibility related to financial reporting, applicable laws and regulations, operating effectiveness and efficiency, and related internal control.*		
Evaluates and Monitors Risk — the board actively evaluates and monitors: • The risk of management fraud via override of internal controls. • Risks affecting the achievement of internal control objectives.	The board develops governance principles and included among these principles is the board's responsibility for evaluating and monitoring risks, especially the risk of fraud by senior management. The board actively, or by delegation of the audit committee, evaluates and monitors the risk of management fraud by overriding of internal controls. The board actively evaluates and monitors the risk of not achieving internal control objectives.	Review the board's governance principles, and that among these principles is the board's responsibility for evaluating and monitoring risks. Inquire of the board, senior management, the CAE, and the external auditor as to the board's processes for evaluating and monitoring risks. Review board agenda, minutes, and information packets for evidence that the board evaluates and monitors the risk of fraud by senior management via management's override of internal controls. Inquire of the board, senior management, the CAE, and the external auditor as to board processes for evaluating and monitoring the risk of management fraud and management override of internal controls. Review board agenda, minutes, and information packets for evidence that the board evaluates and monitors the risk of not achieving internal control objectives. Inquire of the board, senior management, the CAE, and the external audit partner as to the board's processes for evaluating and monitoring the risk of not achieving internal control objectives.
Oversees Quality and Reliability — the board provides oversight for the effectiveness of the system of internal control.	The board charter vests oversight responsibility for the organization's internal control system with the board. The board receives periodic reports on the effectiveness of internal control.	Review the board charter to verify that the board has responsibility for oversight of the internal control system. Review board meeting agenda and minutes denoting substantive board attention to this issue. Review board meeting agenda, minutes, and information packets for evidence of reporting to the board on the effectiveness of internal control.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
2. **Importance of Board***: Basic Principle — The board understands and exercises oversight responsibility related to financial reporting, applicable laws and regulations, operating effectiveness and efficiency, and related internal control.*		
Oversees Audit Activities — the board oversees the work of all audit functions, including internal and external auditing, and interacts with regulatory auditors, as necessary. The board has the exclusive authority to hire, fire, and determine the compensation of the external audit firm and the CAE.	The board charter vests the audit committee or the similar governing body with the authority to oversee the: • Financial reporting and external audit processes, and the exclusive authority to hire, fire, and determine the compensation of the external audit firm. • The internal audit activity, and the authority to hire and fire the CAE and to approve the budget for the internal audit activity.	Review the audit committee charter to verify that the audit committee is vested with the authority to oversee the: • Financial reporting and external audit processes, and with the exclusive authority to hire, fire, and determine the compensation of the external audit firm. Inquire of board members, senior management, and the external auditors as to the board's role in overseeing the financial reporting and external audit processes, including responsibility for selecting the audit firm and determining the audit fee. • Internal audit group, and with the authority to hire and fire the CAE, and to approve the budget for the internal audit activity. Inquire of board members, senior management, and the CAE as to the board's role in overseeing the internal audit activity, including responsibility for selecting the CAE and approving the internal audit budget.
Independent Critical Mass — the board has a critical mass of members who are independent of management.	The organization's charter or bylaws requires a critical mass of independent directors on the board, and is appropriate given the organization's size, industry, and regulatory environment.	Review charter or bylaw provisions requiring independent directors on the board, and evaluate the number of independent directors given the organization's size, industry, and regulatory environment. Review director backgrounds for those directors classified as independent.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
2. Importance of Board*: Basic Principle — The board understands and exercises oversight responsibility related to financial reporting, applicable laws and regulations, operating effectiveness and efficiency, and related internal control.*		
Financial Expertise[2] — the board has one or more members who have financial expertise.	The board charter requires at least one member to have financial expertise and requires all members to be financially literate. At least one member on the board has substantive experience in accounting (e.g., certified public accountant, CFO, or controller).	Review the backgrounds, including education and experience, of board members to evaluate the nature of their financial expertise and literacy.
Frequency — the board meets regularly, often in executive sessions, and devotes sufficient time and resources to adequately carry out its functions.	The charter for the board requires it to meet no less frequently than quarterly. The board holds an executive session at every meeting. The board allocates time to meet alone with the partner from the registered public accounting firm and with the CAE at every meeting. The board devotes sufficient time to carry out its responsibilities (e.g., as a rule of thumb, the board should meet for 1-2 days at each meeting and the audit committee should meet for 3-4 hours at each meeting). The chairman of the board, if independent, or, if not, the lead independent director is primarily responsible for developing the agenda for board meetings. Other directors, the CAE, senior management, and external auditors have input to the agenda-setting process.	Review the charter for these provisions. Evaluate whether the board was in compliance with this aspect of the charter. Inquire of board members as to whether the number of meetings was sufficient (separately for independent and non-independent directors). Review board minutes, and inquire of board members as to whether an executive session was held at every meeting. Review board minutes, and inquire of audit committee members as to whether the board had the opportunity to meet alone with the audit partner from the registered public accounting firm and with the CAE at every meeting and does so on multiple occasions throughout the year. Review board minutes as to the length of board meetings. Inquire of board members as to whether the number of meetings was sufficient (separately for independent and non-independent directors).

[9] Although COSO's Small Business Guidance focuses on internal controls over financial reporting, it is important to note that boards need and have other experts (e.g., risk management, etc.) as members on various committees. In such cases, it is expected that educational background and related experience of such individuals also be evaluated.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
2. Importance of Board*: Basic Principle — The board understands and exercises oversight responsibility related to financial reporting, applicable laws and regulations, operating effectiveness and efficiency, and related internal control.*		
	The board has input into the packet of information received before board/committee meetings. The information packet is received at least three days before the meeting. Board members spend sufficient time reviewing the pre-meeting information packet. The charter for the board authorizes the board to retain outside advisers or counsel as needed.	Inquire of the chairman of the board (lead independent director) and other board members as to the process for setting the board agenda. Confirm that board members have an opportunity to review and provide input into the setting of the agenda. Inquire of board members as to their involvement in determining the content of the information packet and appropriateness of the advanced distribution for review prior to the meeting. Inquire of board members, senior management, the audit partner, and the CAE as to board preparedness for meetings. Review the annual board peer evaluation process, ascertaining that board preparedness is evaluated. Review the charters for provisions allowing the board to retain outside counsel and advisers as needed. Inquire of board members as to

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
3. **Management's Philosophy and Operating Style: Basic Principle** — ***Management's philosophy and operating style support achieving effective internal control.***		
Set the Tone — management's philosophy and operating style emphasize high-quality and transparent internal and external reporting, and the importance of effective internal control and risk management.	Management emphasizes the importance of meeting internal control objectives through both its words and actions.	Inquire of relevant employees as to their perception of the importance of complying with internal control objectives. Review criteria for employee performance reviews, ascertaining whether employees are held accountable for meeting internal control objectives. Review speeches and presentations to internal and external parties that may reflect the tone and style of leadership. Independently observe or inquire with attendees of executive and/or board meetings to confirm that the extent and depth of conversations regarding risk, controls, and compliance matters is appropriate given the matters facing the organization. Review employee survey results where questions concerning the culture and leadership have been asked.
Articulate Objectives — management establishes and clearly articulates internal control objectives.	Internal control objectives over financial reporting, compliance with applicable laws and regulations, efficiency and effectiveness of operations, and safeguarding of assets are communicated to relevant individuals throughout the organization.	Review organization operating and accounting manuals and other means of disseminating internal control objectives throughout the organization. Inquire of relevant individuals as to their understanding of internal control objectives.
Select Principles and Estimates — management follows a disciplined, objective process in developing internal control objectives.	The organization follows a periodic, disciplined process for establishing internal control objectives over financial reporting, compliance with applicable laws and regulations, efficiency and effectiveness of operations, and safeguarding of assets and involves senior financial and operating management.	Review documentation of the organization's process for establishing internal control objectives. Inquire of senior financial and operating management as to their involvement in establishing internal control objectives.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
4. Organizational Structure: Basic Principle — *The organization's organizational structure supports effective internal control.*		
Establishes Responsibility – management establishes internal reporting responsibilities for each functional area and business unit in the organization.	The organization designs a structure that is appropriate given its size, industry, age, and business risks. Management establishes reporting responsibilities for all organizational units.	Review the entity's organizational structure. Compare the organizational structure to other companies of similar size, industry, and age. Review established reporting responsibilities and written evidence of the discharge of these reporting responsibilities during the period. Inquire of key operating, financial, and legal personnel as to their understanding of, and compliance with, reporting responsibilities. Review whether the risks associated with the organization's structure have been discussed by senior management and the board (e.g., risks associated with legal entity complexities, centralization vs. decentralization, span of control, pace of business change and whether the organizational structure is adapting, etc.). Review whether the organization's structure facilitates the flow of risk information upwards, downwards, and across the organization.
Maintains Structure — management maintains an organizational structure that facilitates effective reporting and other communications about internal control among various functions and positions of management.	The organization develops and maintains an organization chart that establishes roles and reporting responsibilities for all employees. The organization develops and maintains job descriptions for key positions.	Review the organizational chart, including delineation of roles and reporting responsibilities, and review the organization's process for updating the organizational chart. Inquire of key employees in the internal control structure as to their understanding of roles and responsibilities. Review job descriptions for key employees, including the organization's process for updating job descriptions. Inquire of key employees in the internal control structure as to their understanding of their job description.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
4. Organizational Structure: Basic Principle — *The organization's organizational structure supports effective internal control.*		
Maintains Processes — management's lines of reporting recognize the importance of maintaining processes for objective verification of information generated from the organization's information system.	The organization has established processes for periodically validating the reliability of its information system and the accuracy, completeness, and timeliness of the information generated from that system.	Review the organization's process for periodically validating the reliability of its information system and the accuracy, completeness, and timeliness of the information generated from that system, and reports generated as a result of this process. Review deficiencies identified, and the organization's investigation, resolution, and remediation of identified deficiencies.
5. Commitment to Competence: Basic Principle — *The organization retains individuals competent in financial reporting, internal control, and risk management, and related oversight roles.*		
Identifies Competencies — competencies that support effective financial reporting, internal control, and risk management are identified.	A clear and transparent competency strategy/plan exists that is aligned to the organization's business strategy and objectives. The strategy has been approved by executive management and communicated. The strategy/plan should include the competency requirements for activities that have been outsourced. The plan should include methods for acquiring the competencies required. Plans are in place to ensure the appropriate level of staffing. Formal job/role descriptions exist that define tasks and competencies for each position. Job/role descriptions (and experience) should include both skills and behaviors necessary to complete the assigned work. For each competency, the desired level of competency should be articulated.	Obtain and review the competency strategy/plan to verify that it exists, aligns to business strategies and objectives, has been approved by executive management, and has been communicated as appropriate. Review staffing levels and organization charts and inquire with management to understand the methodologies used to assess that there is sufficient staff to execute strategies and operating plans. From the organization charts, select a sample of positions and review the job/role descriptions to ensure that the right level of competencies have been articulated to fulfill the assigned tasks of the position. Do the skills seem appropriate and competencies (and experience) reasonable and consistent? It is recommended that the sample include key leadership, management, and supervisory positions particularly as they relate to financial reporting, risk, and control.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
5. **Commitment to Competence: Basic Principle** — ***The organization retains individuals competent in financial reporting, internal control, and risk management, and related oversight roles.***		
Retains Individuals — the organization employs or otherwise utilizes individuals who possess the required competencies in financial reporting, internal control, compliance, and risk management.	Individuals are placed in positions based on the fit of their competencies (and experience) to the job requirements as defined by the job descriptions. In filling key management positions, broad functional experience should be a goal. Consideration is given to competency of service providers when outsourcing activities. There should be a plan to cross train management and staff to provide understanding of other functions impacting their specific duties and for back-up. Plans are in place to ensure adequate staffing levels are maintained. Succession plans for key positions exist and individuals identified in those succession plans have the required competencies or plans exist to develop those competencies. There is a process in place to obtain assistance for highly complex technical matters. Hiring of individuals includes background checks and references, etc.	For recent hires, obtain the incumbents' curriculum vitae or résumés to ascertain that there is an appropriate match of their competencies to the job position. Consider competencies, background, education, and experience. Inquire with management about the adequacy of the selection process. In reviewing the key management job descriptions of incumbents, ascertain that there is broad functional experience rather than over-weighting from one or two functional areas. Inquire with management about the alignment of current skills and competencies of incumbents given ongoing business changes, risks, and current operational performance. Review outsource agreements/arrangements to ascertain that competencies were given due consideration in selecting the service provider (pre-qualification). Ensure that provisions exist requiring the service provider to maintain the necessary competencies. Assess whether the process for monitoring competencies is effective. Obtain training plans and ascertain that cross training is being included in training plan strategies. Inquire of external auditors their perception of capabilities and staffing levels within the financial reporting and key governance functions within the organization. Review audits completed by external parties (regulators, contract, environmental, etc.).

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
5. **Commitment to Competence: Basic Principle** — *The organization retains individuals competent in financial reporting, internal control, and risk management, and related oversight roles.*		
		Were competencies evaluated and if so what were the conclusions/ recommendations? Review succession plans for key positions. Ensure that training development plans and competencies of potential succession planning candidates generally align to job/role requirements. Inquire with finance staff and independently with external auditors to determine how past needs for technical assistance/confirmation of accounting procedures were handled.
Evaluates Competencies — needed competencies are regularly evaluated and maintained.	There is a competency assessment approach and guidance that is documented and updated regularly. The approach is designed to identify competency gaps and establish written development plans to address gaps within a reasonable timeframe and a monitoring/ reporting system to ensure that the gaps are addressed. For individuals in key financial reporting, risk, and control functions, the board annually assesses their competencies. Annual assessments of competencies and performance of both organization and outsourced service provider employees is in place. Skills noted in job descriptions are part of the regular annual employee performance review.	Obtain and review the adequacy of procedures for assessing individual competencies. Select a sample of management and staff and review assessments, plans to address gaps, and progress made to date. Review the reporting system, and conclude on whether people collectively are progressing adequately in addressing competency gaps. For key individuals, review documentation that this was completed. Review those business processes where surprise risk events, material weakness, or deficiencies occurred to determine if competency assessments were properly carried out. Review a sample of performance appraisals to determine whether skills noted in job descriptions are indeed part of employees' annual performance appraisal and whether compensation adjustments differ for employees performing the same skill at various levels of competency.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
6. Authority and Responsibility: Basic Principle — Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.		
Board Oversees Internal Control and Risk Management — the board oversees management's process for defining responsibilities for internal control and risk management.	Legal entity board and committee structures, bylaws, and/or charters set forth responsibilities for the oversight and evaluation of management's principal roles and responsibilities for risk management and internal control. Board meetings should regularly include discussions on the effectiveness of management's roles and responsibilities for risk management and internal control. As a result of discussions, the board should make recommendations on realignment where necessary.	Obtain and review the organization's legal documents to ensure that proper oversight roles exist and are documented. Review board meeting agenda and minutes to ascertain that appropriate oversight discussions are taking place.
Defined Responsibilities — assignment of responsibility and delegation of authority are clearly defined for all employees involved in the internal control and risk management, compliance, and financial reporting processes.	The board delegates authorities and responsibilities to the CEO who in turn delegates authority and responsibilities to appropriate individuals in the organization. These delegated authorities and assigned responsibilities should be formally documented. For key management positions, the board reviews and approves descriptions of the positions' responsibilities and authorities, and considers how those positions affect the strength of internal control. The evidence for assignment of authorities can be in the form of a delegated authorities matrix, written job descriptions, or individual authority grant letters. Employees should clearly understand their authorities and responsibilities.	Review completeness of process for defining responsibilities and delegating authorities. Evaluate appropriateness of criteria for delegating authorities. Through inspection, verify that key management has appropriate documented authorities. By interview, ascertain that management understands its authorities and responsibilities. Verify that authorities are reviewed and adjusted where appropriate periodically. Review employee surveys (or conduct a survey if not conducted by others) to determine whether authorities and responsibilities were clearly communicated and understood.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
6. Authority and Responsibility: Basic Principle — Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.		
	When management assigns authority and responsibilities to key individuals, it considers the impact on the effectiveness of the control environment and the importance of maintaining effective segregation of duties. A defined set of criteria should exist upon which management bases level of authority. When delegating levels of authority and responsibility, management establishes an appropriate balance between the authority needed to "get the job done" and the need to maintain adequate internal control over key business processes. Authority levels should be reviewed periodically to ensure they are appropriate. Employees are empowered to correct problems or implement improvements in their assigned business processes as deemed necessary. Empowerment to take these actions is accompanied by pre-approved levels of responsibility and authority. Management considers the nature of employee positions within the organization when assigning responsibilities to individuals or determining certain levels of authority for positions.	

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
6. Authority and Responsibility: Basic Principle — Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective internal control.		
Limit of Authority — assignment of authority and responsibility includes appropriate limitations.	As part of granting authorities, the organization process includes clear lines of authority for approving transactions over a specific dollar amount or in meeting certain described characteristics. As dollar threshold increases, additional approvals from senior management are required, with the highest dollar thresholds reserved for CEO and board approval. There is a process in place to monitor compliance to authority levels and a remediation process in those cases where authorities are exceeded.	Include verification of authority limits in testing above. During the review period for any significant events/ transactions, verify that the appropriate approval process and levels of approval were followed.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
7. Human Resources: Basic Principle — ***HR policies and practices are designed and implemented to facilitate effective internal control.***		
Establish HR Policies — management establishes HR policies and procedures that demonstrate its commitment to integrity, ethical behavior, and competence.	HR policies and procedures exist. These are reviewed and approved by the board and implemented by management. The policies and procedures are documented and thus provide evidence of the control process. HR policies and procedures are periodically reviewed, updated where necessary, and signed off/approved by appropriate individuals. An effective policy exists for disseminating the HR policies and procedures and employees understand them. Newly hired employees receive a copy of the policies and procedures and all employees receive updates. Periodic employee surveys are conducted to assess employee understanding of HR policies and procedures and whether they have been effective in achieving HR objectives.	Obtain and review the organization's HR policies and procedures to ensure that they are complete, current, and approved appropriately. Review most recent employee survey content. Did it ask employees to evaluate quality/effectiveness of the policies, procedures, and practices? Where improvement opportunities exist, what is the status of the actions? Were the results summarized and reviewed with senior management and the board?

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
7. Human Resources: Basic Principle — *HR policies and practices are designed and implemented to facilitate effective internal control.*		
Recruiting and Retention — employee recruitment and retention for key positions are guided by the principles of integrity and by the necessary competencies associated with the positions.	Management establishes and enforces standards for hiring qualified individuals consistent with job description requirements. Policies over conflicts of interest regarding employment relationships such as those involving family members or personal relationships among co-workers are in place and enforced. Recruiting practices include formal, in-depth employment interviews. Screening procedures, including reference checks, resume review, and background checks are employed for job applicants, particularly those applying for key management positions. Interview and screening practices comply with local employment, human rights, and privacy laws/regulations. The organization develops and maintains position descriptions that reflect its values and the competencies needed to fulfill the position requirements. The job descriptions contain specific references to control related responsibilities. The organization performs exit interviews with those leaving the organization and inquires about any concerns related to internal control. Retention strategies include formal succession plans. The organization should have a documented succession plan for key management positions. Succession plans should be updated periodically and approved by the CEO and board.	Include review of recruiting/retention procedures when completing above review. Verify that screening procedures are being followed. For recent hires into key positions, verify that the new hire meets the position requirements. Review exit interview documentation. Verify that follow-up action was appropriate. Obtain and review succession plans for key positions. Ensure they are periodically reviewed and approved. Review turnover statistics and trends. Were results outside reasonable range analyzed and discussed at an appropriate level? Assess whether HR or another management area reviews turnover levels. Independently review turnover data regarding overall turnover, turnover of recent hires, and turnover of key positions or competencies. Inquire further about potential root cause of excessive or unexpected or unexplained turnover.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
7. Human Resources: Basic Principle — *HR policies and practices are designed and implemented to facilitate effective internal control.*		
Adequate Training — management supports employees by providing access to the tools and training needed to perform their roles.	Training programs exist to enforce and promote ethical behavior and internal control. A training program should include identification of the knowledge, skills, and competencies necessary to perform their roles. Individual training needs should be documented in a training plan. The ongoing training process enables people to effectively deal with evolving business environments. Training includes development and coaching in leadership and interpersonal skills. Management supports employees by providing them the tools and resources necessary to perform their jobs.	Obtain and review training and development programs to ensure they address key elements. Verify that the program includes steps to evaluate employee effectiveness and to set a plan to close any identified gaps. Inspect training plans for several key management team members to verify existence. Evaluate progress in closing "gaps." Review budgets to ensure that there are adequate resources (e.g. time, people, funds, equipment) to achieve the development plans. Review actual spending to ensure that the employees are availing themselves of the training. Review the organization's supplemental education program if one exists. Sample employees regarding the adequacy of internal training and the value add of the training for enhancing skills and competencies.

ELEMENTS AND ATTRIBUTES	CONTROL DESIGN (METHODS TO ACHIEVE CONTROL ENVIRONMENT PRINCIPLES, ELEMENTS, AND ATTRIBUTES)	CONTROL TESTING CONSIDERATIONS
7. Human Resources: Basic Principle — *HR policies and practices are designed and implemented to facilitate effective internal control.*		
Performance and Compensation — employee performance evaluations and the organization's compensation practices, including those affecting senior management, support the achievement of internal control objectives.	A performance management process that includes objective setting, assessment, and reward exists. The organization's compensation/incentive plan for senior executives is balanced among achievement of financial and non-financial goals and is not over-weighted to achievement of quarterly financial results. The performance management process includes steps to confirm awareness of an employee's progress to achievement of objectives during the performance period. Performance reviews are conducted annually and signed by the employee and respective manager. The documented review is evidence of the performance review and is retrievable. Performance evaluations and compensation to include incentive compensation for key management are reviewed by the board before administration/payout. Compensation programs are benchmarked in the market and by industry periodically. The board is apprised of such benchmarks. The board is assured of the integrity of incentive program information systems and that information used to award incentive compensation is reliable.	Obtain and review organization's documented performance management process. Verify that key elements exist. For key management (particular emphasis on executive) verify that performance management process was performed as required. Review board meeting minutes and other documentation to support its review and approval of performance and rewards. Verify that compensation changes, incentive comp awards, and stock grants made are consistent with board approved amounts. Review information packages to the board to ensure that it is getting appropriate information for benchmarking compensation and awarding incentives. Review processes used to develop and compile compensation information and identify that assurance activities cover all important activities. Review actual compensation paid and incentive awards made to approved amounts and pay guidelines.

Authors

Parveen P. Gupta

Philip D. Bahrman, CIA

Joseph Carcello, CIA

Princy Jain, CIA, CCSA

Norman Marks

James A. Rose, CIA

Erich Schumann, CIA

Natarajan Girija Shankar, CIA

Reviewers

Carlos Alberto Reyes, CIA

Maria E. Mendes, CIA, CCSA

Lynn C. Morley, CIA

David W. Zechnich, CIA

Douglas J. Anderson, CIA

Steven E. Jameson, CIA, CCSA, CFSA

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes. For other authoritative guidance materials provided by The IIA, please visit our website at www.theiia.org/guidance.

Disclaimer

The IIA publishes this document for informational and educational purposes. This guidance material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends that you always seek independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this guidance.

Copyright

The Institute of Internal Auditors

GLOBAL HEADQUARTERS
247 Maitland Ave.
Altamonte Springs, FL 32701 USA

T: +1-407-937-1111
F: +1-407-937-1101
W: www.theiia.org