– Practice Guide

RELIANCE BY INTERNAL AUDIT ON OTHER ASSURANCE PROVIDERS

DECEMBER 2011

The Institute of Internal Auditors | Global

Table of Contents

Executive Summary

Chief audit executives (CAEs) are charged with providing assurance on the adequacy of governance, risk management, and related internal controls. This gives management and an organization's governing body, including the audit committee, an assessment of risk, governance, and control processes and practices across the organization, rather than a series of audit reports on individual areas of the organization. Since the risk profile is in a perpetual state of change, internal audit functions are challenged in meeting this expectation using traditional, point-in-time, or cycle audit methods and resources.

Ever-increasing compliance requirements and business complexity have driven companies to establish or procure other risk management and assurance functions. They are charged with measuring and reporting risk, identifying control gaps, tracking remediation, and concluding whether control processes are operating effectively in specific areas. Examples of some internal assurance providers are identified as environmental compliance groups, quality management functions that focus on manufacturing activities, internal control teams that assess controls over financial reporting, and IT governance groups. External assurance providers are often engaged to communicate an opinion to another auditor regarding specific control objectives operated by a service provider. These activities provide assurance on the areas they assessed and recommendations to strengthen the related controls, often in areas that are within the scope of internal audit's work.

This practice guide provides guidance to the CAE and internal audit leadership on an approach for relying on the assurance provided by other internal or external assurance functions. A continuum of five principles determines the extent of reliance:

1. Purpose.
2. Independence and Objectivity.
3. Competence.
4. Elements of Practice.
5. Communication of Results and Remediation.

The principles are interdependent. To illustrate, the CAE would place higher value on assurance providers who commit to a common purpose, convey objective expertise, and practice rigor and monitoring to shorten the time to management action. The results of these other assurance providers can be integrated with the work of internal audit to communicate a comprehensive opinion to key stakeholders. The guidance gives a process for valuing the work of others and assessing the reliability of assurance providers. In turn, good coordination attracts greater reliance on internal audit decreasing the cost of compliance and increasing the efficiency for providing assurance.

Introduction

1.1 Introduction

Internal audit is charged by the *International Standards for Professional Practice of Internal Auditing (Standards)* with providing assurance on the adequacy of governance, risk management, and related controls. In many organizations, management has established (or engaged a third party to provide) other assurance functions — such as in the areas of IT projects, manufacturing quality, environmental health and safety, controls over financial reporting, and other regulatory compliance. The purpose of this practice guide is to provide ideas and ways to leverage the work of other assurance providers, whether the assurance is provided internally within the organization or externally to minimize duplication of work and disruption to the operation, provide enhanced coverage, and conserve audit resources for high-risk processes.

STANDARD 2050: COORDINATION
The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimize duplication of efforts.

An added value to the organization of coordinating the activities of the various assurance providers is limiting duplicate work. Multiple audits or examinations of the same risks and testing of the same controls by multiple assurance providers is an unnecessary burden on process owners and an inefficient use of resources. If one assurance provider, such as internal audit, can rely on the work of another, the value is clear.

1.2 Who are assurance providers?

IIA Practice Advisory 2050-2: Assurance Maps describes three classes of assurance providers, differentiated by the stakeholders they serve, their level of independence from the activities over which they provide assurance, and the robustness of that assurance:

A. Those who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management- designated assurance personnel.

B. Those who report to the board, including internal audit.

C. Those who report to external stakeholders (such as external audit assurance, which is a role traditionally fulfilled by the independent/statutory auditor).

The IIA defines assurance as an objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes. The level of assurance desired, and who should provide that assurance, will vary depending on the risk and stakeholder expectations. The scope of the internal audit function covers the entire organization, including risk management processes (both their design and operating effectiveness), and the management of those risks classified as "key" or significant (including the effectiveness of the related controls).

1.3 Benefits

The IIA's Standards define an internal audit activity as:

"A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value and improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes."

It is noteworthy that this definition emphasizes objective assurance and does not reference an expectation for delivering audit reports or ensuring compliance. Traditionally, internal auditors spend a significant amount of time performing direct inspection audits, but there are other ways to provide assurance. The typical organization has a number of different groups who provide risk management, compliance, and assurance activities independently of one another. In many cases these groups are testing controls deeper and with greater frequency than the internal auditor. Without effective coordination and reporting, work can be duplicated or key risks may be missed or misjudged. By adopting a more integrated assurance model that includes the internal auditor relying on the work of others, several benefits accrue to the organization. These include:

- More precise assurance by involving greater subject matter expertise in audit activities. For example, reliance on an environmental compliance group with specialized knowledge and certifications in the field of environmental regulations may improve the level of insight into operations and the quality of assurance provided.
- Reduced redundancy of effort (audit once, audit well) and 'audit fatigue' for the organization.
- Expanded coverage of the enterprise without increasing direct audit hours. (Reliance on others may allow internal audit to reduce the hours spent in that area and allocate them to other risk areas.)
- Shortened time to management action. For example, the other assurance provider may have continuous

monitoring methods in place, or management may have integrated responses to issues detected by other assurance groups into routine business processes.

- Strategic collaboration, transparency, and better governance for meeting organizational objectives resulting in predictable compliance. When all the groups involved in assurance cooperate and share information, insights, and best practices, the quality of the whole effort is likely to rise.

Reliance on other assurance groups may enable the CAE to redirect scarce audit resources to other areas of significant risk to the enterprise. For example, the audit plan may be expanded to include additional strategic risks, or risks in connection with mergers and acquisitions, major IT and other initiatives and capital programs, and research and development processes.

The IIA's Practice Guide, Coordinating Risk Management and Assurance, advises the CAE to help in the creation of an assurance map for the organization to create a more connected assurance and governance community. Assurance maps help identify duplication and overlap in assurance coverage, define scope boundaries and roles for various assurance providers and determine gaps in assurance coverage that need to be addressed.

1.4 Risk

Relying on other assurance providers, however, can add audit risks such as:

- Missing a control weakness or deficiency and reaching the wrong conclusion due to defects in the work or coverage of the other assurance provider.
- Failing to identify issues that are not shared by the other assurance provider due to their lack of independence from management.
- Raising as an exception and issuing a matter out of context that would not ordinarily be considered significant by internal audit, due to differences in risk assessment processes.

Since external and internal assurance providers and the internal auditor may have different purposes, it is important to manage expectations beforehand regarding the purpose of the review, the objectivity and competence of the evaluator, the rigor of the assessment and testing processes, and the timeliness of the conclusion.

1.5 Opportunity

Other sources or forms of assurance can advance innovative models for communicating assurance as an alternative to the traditional inspect-and-report model. Practices such as continuous monitoring, self-reported issues, and macro-assurance planning are designed to assess and strengthen internal controls by identifying issues promptly and reducing the time to management action:

- Continuous Monitoring: Monitoring controls to detect potential failures, or transactions to identify possible errors and defects, enables management to see and respond to risk early, as it emerges. Continuous monitoring reduces the time to action, sustains the resolution, and extends assurance. When management has continuous monitoring practices in place, internal audit may be able to assess the programs and then rely on them as part of a continuous auditing or assurance program.
- Self-reported Issues: This practice empowers management to raise issues and track remediation to advance corrective action. Internal auditors gain comfort when management promptly addresses root causes for the self-reported issues.
- Macro-assurance: Pervasive themes can be highlighted by comparing and trending common issues raised by the governance community. Coordinating principle-based assessments performed by other assurance providers in sequence with internal audit engagements could give an over-arching macro-opinion across multiple entities or processes.

In addition, efficiency and effectiveness of overall assurance activities may be improved when common tools are

used by the internal auditor and other assurance providers. For example, multiple assurance functions can use an integrated platform to manage the assessment process, share results, and track remediation of significant issues.

The sharing of schedules and plans, and the results of assessments, can avoid duplicate work. It also can highlight areas of increased risk. For example, multiple compliance issues raised by other assurance groups (such as noncompliance with trade compliance regulations) may indicate a need to address entity-level controls (such as the availability of experts in trade compliance regulations).

Principles for Relying on the Work of Internal or External Assurance Providers

2.1 Prior Guidance

The CAE can look to several authoritative sources for guidance on how the internal auditor may rely on the work of others. The IIA's Practice Guide, Formulating and Expressing Internal Audit Opinions (April 2009), defines other assurance providers and provides guidance for a CAE to assess their competency, independence, and objectivity.

According to The IIA's Practice Advisory 2050-3: Relying on the Work of Other Assurance Providers, the decision to rely on the work of other assurance providers can be made for a variety of reasons:

- To address areas falling outside of the competence of the internal audit activity.
- To gain knowledge transfer from other assurance providers.
- To efficiently enhance coverage of risk beyond the audit plan.

2.2 Five Principles in Determining Reliance

The extent of reliance to be placed on the other internal or external assurance providers depends on the following five principles:

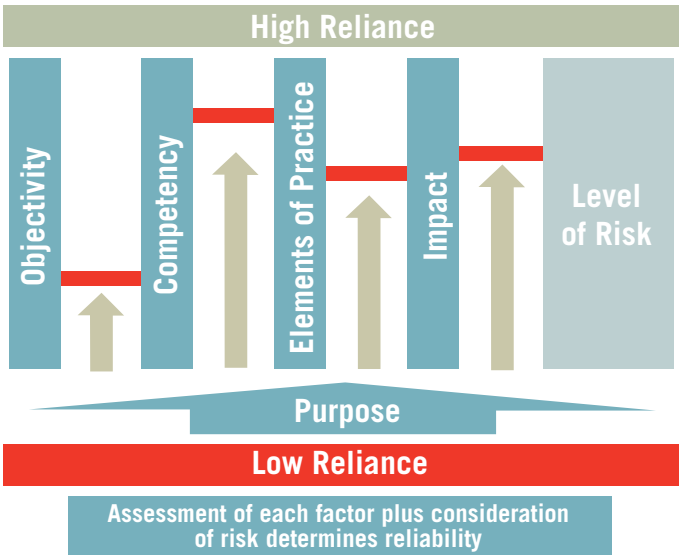
1. **Purpose:** The assurance provider is clear in purpose and committed to providing assurance on a specified risk area and their work is relevant to internal audit's objectives and scope. This is a fundamental principle which must be in place before proceeding further with an evaluation to determine reliability. For internal providers, the purpose should be established in a charter or other similar documentation. For external providers this should be provided for in a contract or statement of work.

2. **Independence & Objectivity:** The professional judgment of the assurance provider is impartial, without inappropriate interference from others. The assurance provider should demonstrate a sufficient degree of objectivity in the course of its work. Although internal assurance providers often report to management and thus are not truly independent, they can be relied on when they demonstrate appropriate objectivity and competence.

3. **Competence:** The assurance provider is knowledgeable of the risks to the organizational processes, how controls are designed to operate in response to the risks, and what constitutes a weakness or deficiency. Characteristics of proficiency for internal or external assurance providers include organizational process expertise, education level, professional experience, relevant professional certifications, continuing education, and the assurance provider's reputation for sound judgment.

4. **Elements of Practice:** The assurance provider has established policies, programs, and procedures and follows them. In execution, assurance work is appropriately planned, supervised, documented, and reviewed. Results are based on persuasive evidence sufficient to support the level of assurance. They also should have the authority to access sufficient information to reach a conclusion.

5. **Communication of Results & Impactful Remediation:** The assurance provider communicates results and ensures management takes timely action. Weaknesses and deficiencies are reported to the person directly responsible for taking corrective actions and to the members of management that have oversight responsibilities. Ongoing monitoring ensures the resolution is sustained as intended. Rigorous process and persuasive and reliable communication results in prompt corrective action. In turn, management action validates an effective assurance process that internal audit can place greater reliance on.



The application of these principles is further described in this diagram. The upward arrows depict a continuum. As the assurance provider puts these principles into practice, the CAE can place higher reliance on the provider's work.

Purpose: When the assurance provider is committed and its purpose is aligned with internal audit's objectives, auditors will find the work more relevant.

Objectivity: The assurance provider can demonstrate credibility and deliver value to the internal auditor even where independence is lacking. The assurance provider's competence, elements of practice and impact are key factors in balancing lower objectivity and establishing reliance.

Competence: Assurance providers can bring a high level of expertise relevant to the specific business process while exercising sufficient objectivity. Although internal auditors provide a high degree of objectivity, they may not have the depth of knowledge needed to provide the desired level of assurance in certain organizational processes or technical areas.

Elements of Practice: The external and internal assurance providers' discipline to practice standard procedures is directly related to their capability for timely and persuasive conclusions. Consistency and rigor in practice should raise the internal auditor's confidence in the assurance provider's work.

Impact: Internal assurance providers who are in close proximity to the business process may communicate risk and influence management to remediate control deficiencies quickly, perhaps more quickly than would a traditional internal audit. By monitoring risk and responding promptly, internal assurance providers may shorten the time to management action.

These principles are interdependent and operate at different levels, proportionate to risk. The internal auditor must evaluate each of these principles in relation to each other and to the overall risk of the relevant processes to arrive at a decision on whether to and how much to rely on another source of assurance provided outside of internal audit. For example, an assurance activity that has a clear purpose and is found to be objective and competent, but does not effectively communicate results or affect constructive change, would likely lead the CAE to rely on it to a much lesser extent. It also is important to note the positive role the internal audit function can play in raising the performance bar for other assurance providers through sharing of best practices and insight into risk management, controls, and audit principles.

Relying on Internal Assurance Providers

3.1 Who are Internal Assurance Providers?

Internal assurance providers (other than the independent internal audit function) are groups that may report to the board, management, or are part of management. These members of the governance community may conduct control self-assessments, continuous monitoring and compliance inspections, quality audits, or a variety of other activities by other names which are designed to provide assurance of achievement of some key organizational objectives or requirements. Organizationally, these individuals and groups may report to the legal department (common for regulatory compliance functions); finance (common for financial reporting control focused or regulatory compliance functions); information security (common for security functions under the chief information officer); environmental, health and safety; or to any operational unit that has decided to invest in a compliance program. All of these are groups the CAE should consider when developing audit plans with the potential to rely on their work.

3.2 Considerations for Internal Assurance Provider

The International Accounting Standards Board (IASB) is an independent accounting standard-setter with the objective of establishing globally accepted financial reporting standards based on clear accounting principles. The IASB gives guidance on using the work of component auditors, internal auditors, and auditor's experts in International Standard on Auditing (IAS) Nos. 600, 610, and 620, respectively. IAS 610 describes the following factors that primarily affect the external auditors' determination for using the work of internal auditors:

- Objectivity.
- Technical competence.
- Due professional care.
- Regular communication.

IAS 620, Using the Work of an Auditor's Expert, names competence, capability, and objectivity as essential factors when considering reliance on the work of others' expertise. Competence relates to the nature and level of expertise of the auditor's expert. Capability relates to the ability to exercise that competence in carrying out the engagement. Objectivity relates to the possible effects that bias, conflict of interest, or the influence of others may have on the expert's judgment.

Similarly, the U.S. Public Company Accounting Oversight Board (PCAOB), a private corporation that oversees the auditors of public companies in the United States, has provided guidance[1] to external auditors on relying on the work of others. The same principles and considerations should be applied in relation to internal audit relying on the work of others. The level of reliance should be based on a careful evaluation of the competence, practices, and objectivity of the persons whose work the auditor plans to rely. A higher degree of competence and objectivity results in greater reliance.

For purposes of relying on the work of others, the PCAOB defines competence as the attainment and maintenance of a level of understanding and knowledge that enables a person to perform assigned tasks. Objectivity means the ability to perform those tasks impartially and with intellectual honesty. When assessing the internal assurance provider's competence, the CAE should evaluate such factors as:

- Educational level and professional experience of staff.

1 Auditing Standard No. 5: An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements; PCAOB Release No. 2007-005A; AU Section 322 — The Auditor's Consideration of the Internal Audit Function in an Audit of Financial Statements

- Professional certification and continuing education.
- Audit policies, programs, and procedures.
- Supervision and review of staff activities.
- Quality of workpaper documentation, reports, and recommendations.
- Evaluation of staff performance.

Assessing the objectivity of other assurance providers can be a challenge as most of these groups report to management and not an independent body such as the audit committee of the board of directors, supervisory board, or head of an agency. There are several factors the CAE may consider when determining if the assurance group demonstrates sufficient objectivity to be relied on:

- The reporting lines for the other assurance group and the level of management to which they report.
- Whether the scope of work, including the tests performed or the assessment and reporting of the other assurance provider are inappropriately influenced by management.
- Policies and practices preventing the assurance provider from auditing areas where the individuals involved have current or recent operational responsibilities.
- The internal auditor's assessment of the quality of work performed by the assurance function, including fact-based conclusions, reporting, and follow-up to identified issues.

3.3 Know When to Rely and Not to Rely

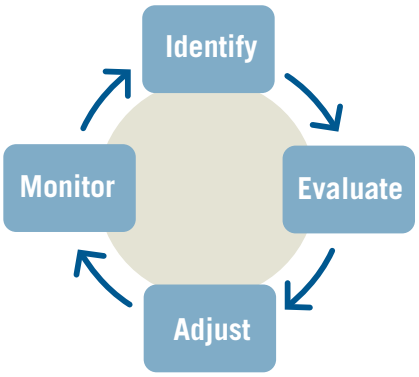
Before investing any significant time in evaluating a particular internal assurance function, the CAE can consider some key factors to determine the extent of potential reliance. These include:

- A charter or similar statement of clear objectives and well-defined responsibilities.
- Objective reporting relationships and/or conflicting operational duties.
- Sufficient expertise regarding the organizational process and risk.
- Disciplined, repeatable processes.
- Communication of results, risks, or control concerns and remediation tracking.

It also is critical to understand the scope of assurance work performed by an internal assurance provider and how it may fit into the internal auditor's assurance objectives and audit plans. Even though internal audit can bring value to the enterprise through objective quality reviews of internal assurance and compliance functions, there is limited value if this work does not extend coverage and help the CAE provide greater assurance to its stakeholders.

3.4 A Process for Relying on the Work of Others

The internal auditor should develop a consistent process for how it will place reliance on the work of others. The following is a basic approach that has been successful for some internal audit functions. It involves the basic steps of identification, evaluation, adjustment, and monitoring.



Identify — Locate internal assurance groups and determine maturity and priority based on preliminary assessment. In large, complex enterprises this can be a challenge. If an organization has an enterprise risk management process, this can be a good single source for identifying additional groups. As other assurance providers are identi-

fied, the internal auditor also must consider how their scope fits into internal audit's own view of the overall risk and control environment and the potential benefits for integrating these assurance activities. Priorities should be based on a measurable value to the organization. This value includes expanding coverage and minimizing fatigue caused by redundant audit activities.

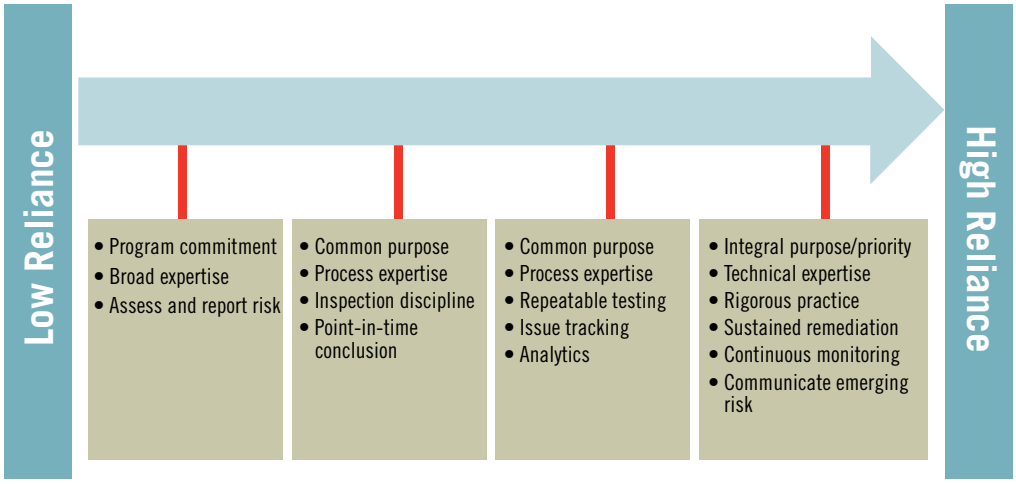
Evaluate — Perform an evaluation of individual groups to determine the extent the internal auditor can rely on the work of others. This is the most critical and time-consuming phase of the reliance model, where internal audit carefully considers the competency and objectivity of the assurance work performed by others. This evaluation also can bring value to the enterprise by providing recommendations to improve the effectiveness of assurance activities. As the evaluation is concluded, there should be a clear communication of how internal audit intends to use the assurance work on an ongoing basis. Additional guidance is provided below on how to evaluate the assurance provider.

Adjust — Modify audit plans and scope to eliminate duplicative testing and expand risk coverage. To realize the full value from a more integrated assurance model, careful consideration must be carried out to determine how these other activities can be used to bolster the independent assurance internal audit provides management, and where there are opportunities to reduce internal audit's own testing. Internal audit should communicate expectations, objectives, and responsibilities in a memo of understanding with other assurance providers regarding the portion of their work that will be relied on.

Monitor — Maintain close communication with each group, sharing risk assessments, audit plans, and results. It is important to establish strong communication and sharing protocol following the evaluation of the assurance providers. This will help ensure the most efficient and effective use of internal audit resources as well as maintain confidence in relying on the work of the other providers. A re-evaluation of the assurance providers should be performed on a periodic basis (see section 3.6).

3.5 Reliance Continuum: Levels of Value

The value the internal auditor can derive from an effective partnership with other assurance groups will vary. There is a continuum of reliance moving from one side of the spectrum, where the auditor determines the work of the other assurance provider is useful but places little reliance, moving across the spectrum to where an assurance provider is fully relied on.



At a minimum, an effective assurance or compliance function should be regularly assessing and communicating risk for its area of responsibility. If the risk assessment process is determined to be sound, it can provide valuable information to help the internal auditor develop audit plans and priorities.

More robust assurance functions, which begin to incorporate periodic testing of controls, may allow the internal auditor to rely on their conclusions at a particular point in time. As these assessments become more frequent and extensive, the internal auditor may be able to place more reliance and further reduce the depth or frequency of its own testing.

Finally, where an effective assurance program is coupled with reliable monitoring mechanisms embedded at the control level, the internal auditor may place the maximum degree of reliance and confidence in the activity.

3.6 Importance of Periodic Evaluation of the Other Assurance Provider

Where internal audit will rely to any measurable extent on the work of other assurance providers, regular assessments should be made of the assurance providers' programs. This is a critical element for internal audit to include in any reliance model to mitigate the risks described earlier (see section 1.4). These assessments should address the continued adequacy of the assurance providers':

- Objectivity.
- Competence.
- Practices.
- Communication that enacts change.

The assessment should include performing tests sufficient to provide objective evidence supporting the reliance placed by internal audit. Opportunities for improving the work of the other assurance provider should be reported, consistent with standard internal audit practices.

Considerations for the CAE – A Case Study

Complex and business critical processes compel an approach for relying on other assurance providers:

A global provider of computer products and services relies on a complex and multichannel sales process involving thousands of third-party distributors around the world. Effectively managing this mix of sales channels can be a competitive advantage and is essential for the long-term success of the business. Management has implemented numerous control processes to mitigate a range of risks inherent in this area. Some examples of risk include compliance (e.g., doing business with restricted parties), financial (e.g., unprofitable sales discounting), and operational (e.g., non-standard and inefficient processes).

Based on management's assessment of the risks and identified control weaknesses, management has invested in a compliance program that includes regular self-assessments by trained, objective assessors outside of internal audit, who test the operating effectiveness of key controls, report findings, and recommend corrective actions. Internal audit provided consultation to help management develop the control framework and key compliance program elements with the intent to rely on this work. This model promoted management ownership of risk and control and more frequent monitoring and testing of controls than the internal audit function could realistically provide due to resource constraints and other enterprise risks to be monitored.

Once the compliance program was implemented and stabilized, internal audit performed a review to validate that it was operating as intended, providing factual and objective assurance and driving positive change in the business. As part of the review, internal audit also connected the compliance program scope with the audit plan and determined how and when the work would be leveraged, and agreed with management on how the two groups would communicate on a regular basis, share information, and collaborate to form a trusted partnership.

Internal audit has significantly reduced the frequency and depth of their control testing, which is now covered by management's compliance process, and has been able to focus on other areas historically not audited such as product lifecycle management, strategic sourcing, and IT project management.

Relying on the Work of External Assurance Providers

4.1 Introduction

A wide variety of external groups provide assurance services to organizations worldwide to ensure that internal controls and risk management procedures are in place and operating effectively. External assurance providers also provide these services at third-party service organizations for the benefit of the service organization and their respective business clients. The purpose of this section is to examine some of the services offered by external assurance providers and discuss key areas that the CAE should consider before placing reliance on their work.

4.2 Who Are External Assurance Providers?

Common external assurance providers include public accounting firms, government auditor general offices, consulting companies, legal firms, security organizations, and internal audit departments of third-party service providers. The following provides a description of each.

Public accounting firms – provide many assurance services such as opining on the fairness and accuracy of financial statements; performing International Organization of Standards (ISO) certification reviews to ensure that an organization conforms to the requirements specified in an ISO standard; conducting reviews of compliance with laws and regulations; assessing the effectiveness of internal controls over financial reporting; reporting on a service provider's privacy program and assessing the protection of personal information; and attest engagements covering system security, availability, processing integrity, confidentiality, and privacy.

Government auditor general offices – provide services similar to public accounting firms; however, they are usually government appointed functions that report to the overall government rather than to shareholders. They provide many assurance services such as opining on the fairness and accuracy of financial statements; performing performance audits to give assurance that appropriate value for money is being achieved from various activities and projects; conducting reviews of compliance with laws and regulations; assessing the effectiveness of internal controls over financial reporting; and attest to engagements covering system security, availability, processing integrity, confidentiality, and privacy.

Consulting companies – provide many services similar to those of public accounting firms mentioned above. However, they are not licensed or registered to issue an opinion on the fairness of financial statements.

Legal firms – provide services to help organizations and third-party service providers to assess compliance with various laws and regulations in jurisdictions where they do business. Legal firms also bring a wealth of knowledge when assisting organizations in completing privacy and legal risk assessments.

Security organizations – provide specialized assurance services such as validating compliance with requirements of the Payment Card Industry Data Security Standards (PCI-DSS) as a qualified security assessor (QSA), conducting network penetration assessments, and performing system vulnerability assessments for security patches, viruses, and fixes. They also provide services related to fraud and IT risk assessments.

The internal audit function of service providers — like other internal audit departments, provide many auditing and consulting services to ensure that internal controls are working effectively and efficiently, and verify that management has programs in place to address significant IT infrastructure risk, application risk, and business process risk relevant to the organization.

Internal audit functions of user entities – often the service organization is contacted by internal audit functions of their customers, user entities, to provide assurance regarding a particular service or organizational pro-

cess or to gain visibility throughout a specific time period. It's not unusual for the service organization to be audited by multiple user entities. Analyzing the audit results and issues raised through assessments conducted by user entities can provide the service organization with common themes providing a unique view to its capability for carrying out control activities consistently.

Specific services provided by external assurance providers can be found in appendix A.

4.3 Considerations for the CAE When Relying on External Assurance Providers

It is important for management and the CAE to understand the relevance of assurance work completed by external assurance providers within the organization. It also is important for management and the CAE to have the same understanding if the organization is outsourcing key business processes to third-party service providers. The CAE also must assess the impact their assurance work may have on the internal audit function.

For information on the role of the CAE in sharing information and coordinating activities with other providers of assurance and consulting services, refer to The IIA's Practice Guide on Co-coordinating Risk Management and Assurance.

Some common questions are outlined below, along with points for consideration:

1. Are the external assurance providers sufficiently qualified, objective, and independent to perform the necessary assurance work? How much reliance should the CAE place on the work of external assurance providers?

   The CAE should:

   - Determine if the external assurance provider is subject to professional performance standards and guidance such as those prescribed by The IIA, the International Federation of Accountants (IFAC), the International Organization of Supreme Audit Institutions (INTOSAI), and other similar governing bodies.
   - Ensure that the external assurance provider is in good standing with their respective governing body and place greater reliance on the work of compliant external assurance providers compared to those not subject to professional standards.
   - Determine if the external assurance provider is subject to professional ethics requirements to ensure the assurance work is performed by qualified individuals, and done in an objective and independent manner.
   - Confirm that due diligence was performed on the external assurance provider that includes background checks, financial stability, years in business, confidentiality agreement, references, and a review of resumes of provider's engagement employees.
   - Obtain evidence, as necessary, to confirm that the individuals performing the work meet competency and experience requirements, that the work is performed and supervised consistent with quality standards, and that the assessment and report are free from inappropriate influence from management. Consideration should be given to whether the assurance provider performs other consulting work for management which might influence their assurance activities, including whether there is either a real or perceived independence and objectivity issue.

2. What is the impact to the annual internal audit plan if the CAE either places reliance or does not place reliance on the work of external assurance providers?

   The CAE should:

   - Be aware of the scope, objectives, and findings of the external assurance engagement to determine the impact to the annual audit plan.

- Determine if there is duplication of audit coverage as a result of the engagement. Alternatively, the CAE should determine if there are coverage gaps in the engagement that may require additional audit work by internal audit.
- If the engagement is performed at the organization, determine if there is an opportunity to co source the engagement, or at a minimum, participate in the tracking of audit findings and resolutions.
- If the engagement was conducted by the organization's third-party service provider, reach out to the service provider to obtain information about the engagement.
- Consider the need for any preliminary audit work prior to the start of the engagement.

3. Do the objectives and scope of work performed by external assurance providers address key risks of the organization?

   The CAE should:

   - Carefully review and understand the scope and objectives of the external assurance engagement before determining the impact it may have on internal audit.
   - Keep in mind that an external assurance engagement typically will not cover all the business risks, key controls, and concerns.

4. Should internal audit complete additional assurance work to supplement the work of external assurance providers?

   - An external assurance engagement typically will not cover all the risks and exposures related to the organization. As such, the CAE and internal audit may have to perform additional audit work based on its risk assessment.
   - Consider the scope, objectives, and results of the engagement before finalizing any additional audit work.
   - Before additional audit work is planned by the organization's third-party service provider(s), identify the right-to-audit clauses contained in the service agreement with the service provider.

5. Should internal audit reperform audit work completed by external assurance providers?

   - The level of expertise brought to the engagement and the rigor practiced by the other assurance provider will determine the extent of diligence conducted by internal audit to accept their audit work. In most cases internal audit would not reperform testing; rather, the CAE should conduct a suitable analysis to determine if the audit work completed was commensurate with the assertions as intended based on risk, scope, and competence of the external service providers.
   - For specialist reviews like penetration and network vulnerability engagements or income tax consulting, the CAE should understand that this area is technical in nature, so the skill set of each auditor should include a solid background in network and information security, income taxes, or the relevant specialty.

6. Should the CAE pursue co sourcing arrangements with external assurance providers?

   - The CAE should consider separate (from management) co sourcing arrangements with the external assurance provider that would provide the appropriate skill sets and add to the efficiency and effectiveness of the audit engagement.

Co sourcing arrangements may include preliminary audit work prior to the start of the engagement, conducting some audit work during the engagement under the supervision of the external service provider, and completing post-audit work to validate on-going compliance and remediation efforts.

Appendix

Appendix A: Services Provided by External Assurance Provider

The types of services offered by external assurance service providers include AICPA/CICA SysTrust, ISO/IEC 27002:2005 certifications, SSAE 16/ISAE 3402 reviews, internal audit cosourcing, PCI-DSS assessments, network penetration security assessments, vulnerability management reviews, and many other types of services. A description of some of these common services follows:

AICPA/CICA SysTrust

For example, in North America, SysTrust is a branded assurance service offering licensed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Trust Services Principles and Criteria (Trust Services). Trust Services are professional attestation and advisory services based on principles and criteria that address risks and opportunities of IT-enabled systems and privacy programs. Specific areas covered in Trust Services guidance include:[2]

- Security – the system is protected against unauthorized access (both physical and logical).
- Availability – the system is available for operation and use as committed or agreed.
- Processing integrity – system processing is complete, accurate, timely, and authorized.
- Confidentiality – information designated as confidential is protected as committed or agreed.
- Privacy – personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles issued by the AICPA and CICA.

As a licensed offering, SysTrust engagements are conducted by certified public accountants (CPAs) or chartered accountants (CAs). Many organizations, particularly third-party service providers, request this type of engagement to demonstrate to their clients that they are concerned about protecting the information assets entrusted to them, and addressing business risks and controls associated with complex IT systems. These reports also can be used by the service organization in marketing its services to potential clients/customers.

ISO/IEC 27002:2005

The ISO/IEC 27002:2005 – Code of Practice for information security management is one of a set of Information Security Management System (ISMS) standards published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Through the use of these standards, organizations can develop and implement a framework for managing the security of their information assets such as financial information, intellectual property, and customer and employee personal information. The ISMS family of standards consists of the following international standards, under the general title of Information technology – Security techniques:[3]

- ISO/IEC 27000:2009, Information security management systems — Overview and vocabulary.
- ISO/IEC 27001:2005, Information security management systems — Requirements.
- ISO/IEC 27002:2005, Code of practice for information security management.
- ISO/IEC 27003, Information security management system implementation guidance.
- ISO/IEC 27004, Information security management — Measurement.

2 Trust Services Principles and Criteria – An Overview, January, 29, 2009, www.aicpa.org/InterestAreas/InformationTechnology/Resources.

3. ISO/IEC 27000:2009, Information technology – Security techniques – Information security management systems – Overview and vocabulary, First edition 2009-05-01, ISO/IEC. This material is reproduced from ISO/IEC 27000:2009 with permission from the American National Standards Institute (ANSI) on behalf of the International Organization for Standardization (ISO). No part of this material may be copied or reproduced in any form, electronic retrieval system or otherwise or made available on the Internet, a public network, by satellite or otherwise without the prior written consent of the ANSI. Copies of this standard may be purchased from ANSI, 25 West 43rd Street, New York, NY 10036, (212) 642-4900, http://webstore.ansi.org.

- ISO/IEC 27005:2008, Information security risk management.
- ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management system.
- ISO/IEC 27007, Guidelines for information security management systems auditing.
- ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.

ISO/IEC 27002 provides guidance on the implementation of 11 commonly accepted security control objectives along with best practice controls that can be applied to achieve the objectives. The standard also includes comments on risk assessment and treatment. Specific areas covered in the standard include:

- Security policy.
- Organization of information security.
- Asset management.
- Human resources security.
- Physical and environmental security.
- Communications and operations management.
- Access control.
- Information systems acquisition, development, and maintenance.
- Information security incident management.
- Business continuity management.
- Compliance.

Many organizations, particularly third-party service providers, who have adopted the ISO/IEC 27002 information security management standard, choose to be certified compliant with the standard through a formal independent audit. Third-party service providers often use this certification to demonstrate to current and future business clients that they have good security practices in place to protect the information assets that are entrusted to them.

ISO does not audit or assess an organization to validate that its standards are being implemented in conformity with the requirements. An external independent certification body or ISO registrar conducts the audit to determine if the organization conforms to the requirements specified in the standard to obtain certification. There are numerous certification bodies (assurance service providers) worldwide that carry out certification assessments. External service providers performing this type of service include public accounting firms, consulting companies, and sole practitioners.

SSAE 16/ISAE 3402

Third party assurance reviews are normally performed for organizations that process financial transactions for their clients or customers. The resulting report is typically used by internal and external auditors and can potentially reduce the amount of work required in their audits. The reports describe the service offerings and the control environment surrounding the processing of customer transactions.

ISAE 3402

The International Standard on Assurance Engagements No. 3402 (ISAE 3402), Assurance Reports on Controls at a Service Organization, was issued in December 2009 by the International Auditing and Assurance Standards Board (IAASB) under the International Federation of Accountants (IFAC). ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.[4] The effective date for this standard applies to periods ending on or after June 15, 2011.

4 2011 IAES3402.com, http://isae3402.com/ISAE3402_overview.html

SSAE 16

Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, was finalized by the Auditing Standards Board of the AICPA in January 2010. SSAE 16 replaced Statement on Auditing Standards (SAS) No. 70, Service Organizations, as the authoritative guidance for reporting on controls at service organizations. SSAE 16 was formally issued in April 2010 with an effective date of June 15, 2011.[5] SSAE 16 is based on the IAASB assurance standard for service auditors ISAE 3402. It should be noted that the requirements for auditing the financial statements of entities that use service organizations remains in the auditing standards in a new SAS, Audit Considerations Relating to an Entity Using a Service Organization.

The AICPA is establishing three reporting options to provide a framework for CPAs to examine controls and to help management understand related risks. The Service Organization Control 1 (SOC 1) report addresses controls for financial statement audits with guidance provided by SSAE 16. SOC 2 reports on controls related to compliance or operations with guidance provided by Attestation Standard (AT) Section 101, Attest Engagements. Both SOC 1 and SOC 2 reports are restricted use reports. SOC 3 reports are the same as a SOC 2 report but general use.

The AICPA SSAE 16 or ISAE 3402 allows for two types of reports:

Type I: Reports on controls placed in operation

A service auditor's report on a service organization's description of the controls that may be relevant to a user organization's internal controls, whether such were suitably designed to achieve specified control objectives, and whether they had been placed in operation as of a specific date. These reports may be useful in providing a user auditor with an understanding of the controls necessary to plan the audit, as well as design effective tests of controls and substantive tests at the user organization. However, they are not intended to provide a basis for reducing assessments of control risk below the maximum.

Type II: Reports on controls placed in operation and tests of operating effectiveness

A service auditor's report on a service organization's description of the controls that may be relevant to a user organization's internal controls, whether such controls were suitably designed to achieve specified control objectives, whether they had been placed in operation as of a specific date, and whether the controls that were tested were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the related control objectives were achieved during the period specified. Such reports may be useful in providing the user auditor with an understanding of the controls necessary to plan the audit and may also provide the user auditor with a basis for reducing his or her assessments of control risk below the maximum.

Some common misconceptions about SSAE 16 reports the CAE should be aware of include:

1. All SOC reports contain the same control objectives. (Control objectives are defined specifically for the environment been attested.)
2. SOC reports are "forward-looking" documents.
3. Type I vs. Type II reports don't really make a difference to my audit planning. (Type I only covers control design effectiveness and is point in time. Type II covers control operating effectiveness for an opinion period.)
4. Exceptions are not reported. (Any exceptions to the controls are clearly identified in the test tables even if it does not rise to the level of being a qualified report.)
5. Exceptions have no impact on my audit plan.

5 2011 SSAE16.com, http://ssae16.com/SSAE16_overview.html

(Further testing or compensating controls should be considered for exceptions.)

6. Since SOC reports are intended for external auditor-to-auditor communication, the report is not relevant to internal audit planning. (Using/relying/further testing of controls covered in the SOC report should be discussed at planning.)

7. As a professional courtesy, a copy of the SOC opinion need only be referenced in the audit planning file. (A thorough understanding of the scope, coverage, nature, timing, and extent of testing within a SSAE 16 engagement is essential.)

The CAE of the organization that utilizes third-party service providers should consider adopting the following practices when evaluating the impact of SSAE 16 engagements to the organization and the audit plan:

- Obtain all relevant SSAE 16 SOC reports.
- Determine the exact nature of the environment in scope for the report as large service providers can potentially have many reports.
- Understand "carve-outs" of environments as the standard allows service providers to exclude areas or parts of the environment from the scope of work and resulting audit opinion.
- Review the independent service auditor's opinion type (qualified/unqualified).
- Review the date of the report(s) and period(s) covered.
- Determine whether the report is a Type I or Type II.
- If the SSAE 16 report is older than six months, a more current report should be requested. If a more current report is not yet available, then management and the CAE should consider the need to perform other audit procedures to obtain comfort over the controls at the service provider or request a letter from the service provider to bridge the interim.
- Document the comfort level with the SOC report and the impact to the organization and the CAE's audit plans
- Determine if control risk will be assessed as low, moderate, or high.
- Gain an understanding and test user control considerations defined in the report.

Payment Card Industry – Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of 12 technical and operational requirements established by the PCI Security Standards Council (PCI SSC) to protect cardholder data. The standards apply to all organizations that store, process, or transmit cardholder data. The PCI SSC also provides guidance for software developers and manufacturers of applications and devices used in those transactions. The Council is responsible for managing the security standards, while compliance with the standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard, and VISA, Inc.

The PCI-DSS Security Audit Procedures (SAPs) contains more than 230 comprehensive requirements. The auditing responsibility is distributed between merchants, qualified security assessors (QSAs), approved scanning vendors (ASVs), and acquirers. PCI SSC allows two acceptable forms of auditing of the requirements by either a qualified security assessor (QSA) or internal security assessor (ISA).

QSA companies are organizations that have been qualified by the PCI SSC to perform detailed SAP assessments and reports on compliance on behalf of the merchant. The primary reasons merchants may select a QSA rather than performing the assessment internally may include transaction volume, breadth of industry knowledge, depth of technical expertise, and an independent view of the environment. Other reasons merchants may not use internal resources may include lack of technical competence, lack

of resources, and to focus resources on more strategic vs. compliance efforts.

ISA is a certification required for organizations performing internal assessments by their internal audit staff, beginning in 2011. The purpose of the ISA certification is to ensure internal auditors are provided the same training as the QSAs to improve the quality, consistency, and competency of the assessments.

Penetration Tests and Network Vulnerability Management

Organizations continue to be impacted from malicious breaches resulting in compromised credit card information, social security numbers, medical information, and other loss of internal and external customer information at the hands of hacker attacks. Key to proactively combating these attacks within an organization is to ensure a strong program for penetration tests and vulnerability assessments.

Penetration testing, sometimes called "ethical hacking," mimics the role of a hacker to deliberately attempt to break into the network infrastructure to determine vulnerabilities of key components of the company infrastructure that could lead to a compromise of critical/sensitive information. The penetration test should stop short of actually negatively impacting the environment.

Penetration tests are not only an imperative practice for a strong information security program, but are required to comply with several regulations and requirements. For example, PCI-DSS requires third-party penetration tests to be performed annually. Some organizations require annual penetration testing as a key IT general control to meet the requirements of the U.S. Sarbanes-Oxley Act of 2002. External penetration testing provides organizations the opportunity to have an independent third party determine the risks (or weak links) in their network and systems.

Vulnerability management is the processes and technologies that an organization employs to identify, assess, and remediate IT vulnerabilities — weaknesses or exposures in IT assets or processes that may lead to a business risk or security risk. One of the most common attack vectors today is via weak or insecure web application programs. Hackers exploit these weaknesses to gain access into the unsuspecting organization's network and systems environment. Awareness and secure coding training is crucial to help mitigate this risk. All programmers, especially web application developers, should be properly trained on secure coding techniques.

Penetration tests and vulnerability assessments could potentially disrupt an organization. Therefore, organizations should determine what is needed to adequately test with the potential of "breaking" or disrupting a component of the infrastructure. A strong program for penetration testing and vulnerability management is imperative for an organization to mitigate internal and external threats.

In conclusion, services offered by external assurance providers can be leveraged to provide broader coverage of the organization's key risks when carefully considered beforehand to be relevant to the enterprise. As outlined in the first principle of "purpose," both external and internal assurance providers are committed to reliance and their work is relevant to the objective of internal audit, which applies to operational, regulatory, or financial reporting. It is vital to communicate expectations, objectives, and responsibilities with the other assurance provider regarding the portion of their work that will be relied upon.

Appendix B: Guide for Internal Auditors to Assess the Reliability of Other Assurance Providers

The following is a sample audit guide for internal audit to assess the reliability of another internal assurance provider. These procedures should help the auditor evaluate the extent the assurance provider meets the principles for reliance described in section two of this practice guide. In evaluating the competency and objectivity of the assur-

ance provider, the assessment process is organized around four major areas:

Governance and Objectives – A charter or objective statement provides authority and scope of assurance activities and establishes intent for internal audit to rely on the work product of the assurance provider. Adequate staff is in place (numbers and competency) and objectivity is provided for.

Risk Assessment and Planning – Assurance activities are guided by appropriate policies and procedures and should include audit plans that incorporate an assessment of risk.

Assurance Execution – The assurance provider has a demonstrated performance history of delivering to the established objectives and producing competent and reliable results. Documentation should be maintained as evidence of performance to relevant professional standards.

Reporting and Follow-up – The results of assurance activities are reported to an appropriate level of management and issues are tracked until they are mitigated.

Purpose and Governance – A charter or objective statement provides authority and scope of assurance activities and establishes intent for internal audit to rely on the work product of the assurance provider. Adequate staff is in place (numbers and competency) and objectivity is provided for.	
Characteristic	**Verification Procedures or Method of Demonstrating**
Charter	1. Does the assurance provider have a written charter that includes the following elements: mission and scope of work, accountability, roles and responsibilities, responsibility, and authority? 2. Is the charter published, easily accessible, and has been communicated to all applicable staff? 3. Is the charter periodically reviewed and updated in accordance with the changing risk environment and approved by an appropriate leadership level?
Written policies and procedures	Does the assurance provider maintain documented policies and procedures that include the following: 1. Procedures to identify, document, and evaluate the relevant risks and their associated controls. 2. Risk-based procedures to evaluate the effectiveness of internal controls. 3. Procedures to document internal control monitoring and testing procedures including supervisory review. 4. Procedures to report on the effectiveness of internal control to appropriate management. 5. Procedures to monitor and report actions to remediate control weaknesses.
Personnel performing assurance activities have appropriate skill and objectivity	1. Obtain staff bios and look for appropriate background, experience, and education to perform audit activities. Evidence may include formal education, direct experience, professional certifications, and relevant training courses. 2. Review and evaluate the assurance provider's functions/responsibilities beyond their review activities and ensure that these tasks do not impair their independence. 3. Evaluate the management supervision process of staff and determine if there is appropriate oversight to ensure the quality of work.

Performance measurements	1. Does the assurance provider measure its own performance? This could include use of a balanced scorecard, surveys of key stakeholders, etc. 2. Identify key stakeholders of the assurance provider assurance activity and interview to understand their view of the value being provided, the areas of focus, quality, and timeliness of reporting, etc.
Risk Assessment and Planning – Assurance activities are guided by appropriate policies and procedures and should include audit plans that incorporate an assessment of risk.	
Characteristic	**Verification Procedures or Method of Demonstrating**
Defined assurance universe	1. How has the assurance universe been defined? Determine the appropriateness of the size and number of the entities making up the audit universe (e.g., too detailed or general, too many or too few, logical division, etc).
Risk assessment	1. Review the risk assessment process. Understand the key risk components considered. Evaluate if these are reasonable and comprehensive, considering both qualitative and quantitative factors. Is the risk assessment updated at least annually? 2. Determine if the assurance provider follows a structured approach to create and document risk-based reviews. Does the approach include input from an appropriate range and level of business leaders? 3. Interview the audit team and process owners of the associated business units/support functions and assess how risks are updated for changes such as acquisition, reorganization, change in Job responsibilities, etc.
Assurance plan	1. Obtain the current period and long range audit plan(s). Determine the following: - How is the assurance plan developed? - Is it based on results of the risk assessment? - Are plans reviewed and approved by an appropriate level of leadership? - Does the plan provide for appropriate coverage of the assurance universe? - Does the plan include appropriate time for follow-up activities to validate corrective actions of prior issues? 2. Inquire as to how the planning process factors in changes that occur, such as new regulations, organization changes, etc. 3. Compare current staffing levels with the audit plan to determine if sufficient resources are available (i.e. are they on track to finish their scheduled reviews).
Assurance Execution – The assurance provider has a demonstrated performance history of delivering to the established objectives and producing competent and reliable results. Documentation should be maintained as evidence of performance to relevant professional standards.	
Characteristic	**Verification Procedures or Method of Demonstrating**
Engagement planning	Select a sample of assurance engagements and review for the following: 1. Does the engagement have a documented scope, objectives, timeframe, and deliverables? 2. Do the scope and objectives tie to the overall risk assessment and assurance plan? 3. How is the scope determined? Is it based on some preliminary assessment and understanding of risks relevant to the activity being reviewed? 4. Does the scope appear adequate in light of the identified risks?

Documentation	1. Are work programs documented to achieve engagement objectives? These should establish the procedures for identifying, analyzing, evaluating, and recording information during the engagement. 2. Is the work performed documented? Review the workpapers and assess whether they are sufficient, relevant, and reliable in meeting IIA standards. 3. Assess if it is feasible for a third party to re-perform the work based on the audit work papers. 4. Are appropriate samples selected for the controls tested? 5. Are issues or findings adequately documented, with root cause clearly identified? 6. Is there evidence of an appropriate review and approval of assurance work? 7. Are workpapers appropriately secured and retained according to company record retention requirements?
IT considerations	1. Review for evidence of appropriate use of technology in assurance activities, i.e., use of analytical review techniques, computer aided audit tools (CAATS), etc. 2. Are IT risks and controls adequately considered and addressed in the assurance/audit activities?
Reporting and Follow-up – The results of assurance activities are reported to an appropriate level of management and issues are tracked until they are mitigated.	
Characteristic	**Verification Procedures or Method of Demonstrating**
Reporting	1. Are the results of assurance activities formally reported? Select a sample of assurance reviews completed in the past 12 months and review for the following: - Are they documented and presented in a standard format? - Are they provided to an appropriate distribution of leadership? - Are findings presented in a reasonable time following the review activities? - Are issues and recommendations clearly presented and rated according to assurance provider procedures? 2. Do findings include elements of effective issues (5 C's – criteria, condition, cause, consequence, corrective action)? 3. Do all issues have an appropriate owner identified?
Issues are identified and tracked	1. Is there a process to monitor issues and status of corrective actions? Is status regularly reported to appropriate leadership? 2. Is there a process to validate corrective actions taken in response to audit issues?

Glossary

The American Institute of Certified Public Accountants (AICPA) – the voice of the accounting profession since 1887. The AICPA prides itself on its serving the certified public accounting (CPA) profession and the public interest to which it is profoundly committed. AICPA members work in all sectors of the business and financial services profession, including public accounting, financial planning, tax, business and industry, law, consulting, education, and government.

http://www.aicpa.org/About/Pages/About.aspx

Assessment – the act of assessing; appraisal; evaluation.

Auditing Standard No. 5 (AS No. 5): An Audit of Internal Control Over Financial Reporting That Is Integrated with An Audit of Financial Statements – Issued by the PCAOB, the report is based on PCAOB inspections that examined portions of approximately 250 audits of internal control over financial reporting (ICFR) by the eight largest domestic registered firms in 2007 and 2008. AS No. 5 became effective for audits for fiscal years ending on or after Nov. 15, 2007, and replaced the PCAOB's previous ICFR standard, AS No. 2.

http://pcaobus.org/News/Releases/Pages/09242009_AS5_Report.aspx

Board – A board is an organization's governing body, such as the board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report.

Chief Audit Executive (CAE) – describes a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the Definition of Internal Auditing, the Code of Ethics, and the International Standards for the Professional Practice of Internal Auditing (Standards). The CAE or others reporting to the CAE will have appropriate professional certifications and qualifications. The specific job title of the CAE may vary across organizations.

https://www.globaliia.org/standards-guidance/mandatory-guidance/Pages/Standards-Glossary.aspx

The Canadian Institute of Chartered Accountants (CICA) – represents Canada's chartered accountants (CA) profession both nationally and internationally. CAs are Canada's internationally recognized profession of leaders in senior management, advisory, financial, tax, and assurance roles.

http://www.cica.ca/about-the-profession/cica/index.aspx

Compliance Community Member – an individual or group with responsibility for developing, administering, and monitoring internal programs to ensure compliance with applicable federal and state laws and regulations. Alternate titles: compliance manager, risk and compliance officer.

Continuous Auditing – Continuous auditing is a method used to perform control and risk assessments automatically on a more frequent basis. Technology is key to enabling a continuous auditing approach. Traditionally, internal audit's testing of controls has been performed on a retrospective and cyclical basis, often many months after business activities have occurred. The testing procedures have often been based on a sampling approach and included activities such as reviews of policies, procedures, approvals, and reconciliations. Today, however, it is recognized that this approach only affords internal auditors a narrow scope of evaluation, and is often too late

to be of real value to business performance or regulatory compliance. See GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment.

Continuous Monitoring – encompasses the processes that management puts in place to be sure that the policies, procedures, and business processes are operating effectively. It addresses management's responsibility to assess the adequacy and effectiveness of controls. This involves identifying the control objectives and assurance assertions and establishing automated tests to highlight activities and transactions that fail to comply. See GTAG 3.

Co-sourcing – Many CAEs must confront the possibility of outsourcing some of their work to ensure everything with which they are tasked is completed in a timely and competent manner. Co sourcing presents a CAE with a broad range of outside capabilities to supplement in-house talent.

Chartered Accountant (CA) – Professional member of a country's Institute Of Chartered Accountants. He or she must work (and be trained) in the office of a practicing chartered accountant for three years, and pass exhaustive written tests to qualify. On completing the requirements, the trainee is awarded the Associate of the Institute of Chartered Accountants (ACA).

http://www.businessdictionary.com/definition/chartered-accountant-CA.html

Certified Public Accountant (CPA) – a statutory title of qualified accountants in the United States for one who has passed the CPA examination administered by the licensing body of the AICPA.

AICPA Board of Examiners (BOE) – a senior committee of the AICPA that sets policy for the Uniform CPA Examination in accordance with legal and psychometric standards as they apply to licensure examinations. Members of the BOE are CPA volunteers from every segment of the profession — public accounting, business and industry, and the academic community — the majority of whom currently also have regulatory (state board) experience.

http://www.aicpa.org/BECOMEACPA/CPAEXAM/EXAMOVERVIEW/GOVERNANCE/Pages/default.aspx

Internal Security Assessor (ISA) – A certification program offered by the Payment Card Industry Security Standard Council (PCI SSC), an international organization that manages the Payment Card Industry Data Security Standard (PCI-DSS). ISA is designed to help companies comply with their continually evolving rules and regulations. The ISA program offers training to merchants, banks, and processors. This certification program trains select individuals on the basics of implementing an ongoing security discipline, and works to remove the "check the box" mentality that can sometimes arise with compliance programs. ISA program benefits include: an opportunity for internal auditors to learn the same techniques taught to QSAs; the chance for merchants to verify their internal staff have a common understanding of the PCI-DSS requirements; the ability for merchants to hear the intent of the requirements directly from the Council; and a potential reduction in compliance costs by teaching ISAs to develop security strategies before and beyond the annual PCI-DSS validation.

http://www.scmagazineus.com/how-you-are-changing-the-pci-standards-in-2010/article/170374/

International Organization of Supreme Audit Institutions (INTOSAI) - a worldwide affiliation of governmental entities. Its members are the Chief Financial Controller/Comptroller General Offices of nations.

International Standard on Assurance Engagements (ISAE) 3402 –deals with assurance engagements undertaken by a professional accountant in public practice to provide a report for user entities and their auditors on the controls at a service organization. The service is likely to be relevant to user entities' internal control as it relates to financial reporting.

http://web.ifac.org/download/b014-2010-iaasb-handbook-isae-3402.pdf

Information technology–Security techniques–Code of practice for information security management (ISO/IEC 27002:2005) — an information security standard published by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) originally as ISO/IEC 17799:2000. ISO/IEC 27002 provides best practice recommendations on information security management for use by those responsible for initiating, implementing, or maintaining Information Security Management Systems (ISMS). The current standard is a revision of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British Standard (BS) 7799-1:1999.

Key Performance Indicators (KPIs) – KPIs are important measures of a business's performance and progress toward goals (dictionary.com). They are metrics related to critical success factors.

Key Risk Indicator (KRI) – a measure used in management to indicate how risky an activity is. According to The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Guidance on Monitoring Internal Control Systems, key risk indicators are forward-looking metrics that seek to identify potential problems, thus enabling an organization to take timely action, if necessary. Reprinted with permission from COSO, copyright 2004-2011. COSO. All rights reserved.

Macro Assurance – Pervasive themes can be highlighted by comparing and trending common issues raised by the compliance community. Planning principle-based assessments performed by other assurance providers in sequence with internal audit engagements to provide an overarching macro-opinion across multiple entities or processes.

Other Assurance Provider (internal/external facing) – Internal Other Assurance Providers are evaluators who report to management and/or are part of management (management assurance), including individuals who perform control self-assessments, quality auditors, environmental auditors, and other management-designated assurance personnel. External Other Assurance Providers are evaluators who report to external stakeholders (external audit assurance), a role traditionally fulfilled by the independent/statutory auditor.

U.S. Public Company Accounting Oversight Board (PCAOB) – The PCAOB is a nonprofit corporation established by the U.S. Congress in 2002 to oversee the audits of public companies to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports. The PCAOB also oversees the audits of broker-dealer compliance reports under federal securities laws.

http://pcaobus.org/Pages/default.aspx

Payment Card Industry Data Security Standard (PCI-DSS) – created by the leading credit card companies to ensure customer data is safeguarded.

Payment Card Industry Security Standards Council (PCI SSC) – offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to

help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI-DSS, which provides an actionable framework for developing a robust payment card data security process — including prevention, detection, and appropriate reaction to security incidents.

https://www.pcisecuritystandards.org/security_standards/index.php

Penetration Testing – A penetration test is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for any potential vulnerability that could result from poor or improper system configuration, from known and unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. The intent of a penetration test is to determine the feasibility of an attack and the amount of business impact of a successful exploit, if discovered.

Qualified Security Assessor (QSA) – The Payment Card Industry (PCI) QSA designation is conferred by the PCI Security Standards Council to those individuals that meet specific information security education requirements, have taken the appropriate training from the PCI Security Standards Council, are employees of an Approved PCI Security and Auditing Firm, and will be performing PCI compliance assessments as they relate to the protection of credit card data. The term QSA also may be implied to identify an individual qualified to perform PCI compliance auditing and consulting. The primary goal of an individual with the PCI QSA certification is to perform an assessment of a firm that handles credit card data against the high-level control objectives of the PCI Data Security Standard (PCI-DSS).

Reliance – confident or trustful dependence (dictionary.com).

Statement of Auditing Standards No. 70 (SAS 70) – SAS 70 is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). SAS 70 demonstrates that data centers have adequate controls and safeguards in place to host or process data related to their customer base. SAS 70 is not a certificate, but an opinion on the nature of those controls.

http://www.c7dc.com/articles/sas-70-faq.htm.

Self-reported Issues – This practice empowers management to raise issues and track remediation to advance corrective action. Auditors gain comfort when management promptly address root causes related to the self-reported issues.

Service Provider – any company that provides the following services to another organization: executes and maintains accountability of transactions, records transactions and processes information, and impacts the client's financial reporting. Typical service companies include application service providers, claims processors, clearinghouses, credit processing companies, and data center hosting facilities.

http://www.c7dc.com/articles/sas-70-faq.htm

Statement on Standards for Attestation Engagements (SSAE) No. 16 – In April 2010 the AICPA Auditing Standards Board (ASB) issued SSAE 16, Reporting on Controls at a Service Organization. The SSAEs also are known as attestation standards. SSAE 16 is applicable when an entity outsources a business task or function to another entity (usually one that specializes in that task or function) and the data resulting from that task or function is incorporated in the outsourcer's financial statements. In SSAE 16 an entity that performs a specialized task or function for other entities is known as a service organization and an entity that outsources the task or function to

a service organization is known as a user entity.

http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/SOC/DownloadableDocuments/QAs_Serv_Orgs_Apr_26_2010.pdf

User Entity (Client Organization) – an entity that outsources a business task or function to another entity (usually one that specializes in that task or function) and the data resulting from that task or function is incorporated in the outsourcer's financial statements. In SSAE 16 an entity that performs a specialized task or function for other entities is known as a service organization and an entity that outsources the task or function to a service organization is known as a user entity.

http://www.aicpa.org/InterestAreas/AccountingAndAuditing/Resources/SOC/DownloadableDocuments/QAs_Serv_Orgs_Apr_26_2010.pdf

Vulnerability Management – the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems.

Authors:

Bradley C. Ames, CPA, CISA

Ken Askelson, CPA, CITP, CIA

Hussain T. Hasan, CISSP, CISM, CGEIT, PCI-QSA

David Strealy, CIA

David Williams, CISA

Reviewers and Contributors

Gary E. Eymer, CIA

Carrie Gilstrap, CISA

Mark Harrison

Steve Hunt, CIA

Steve Jameson, CIA, CCSA, CFSA, CRMA

Donald E. Sparks, CIA, CISA

Steven Stein, CIA, PMP, CISA, CISSP, CFE, CGEIT

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.globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors | *Global*

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

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