

# Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control

IIA Web Site – <http://www.theiia.org/>

# **Practical Considerations Regarding Internal Auditing**

## **Expressing an Opinion on Internal Control**

### Table of Contents

<u>Topic</u>	<u>Page</u>
Introduction	3
Evaluation Criteria and Structure	4
Scope Description	5
Defining Responsibility for Internal Controls	6
Types of Audit Opinions	6
Interaction with Section 404	9
Practical Considerations (Q&A)	11
Related Standards	15
Additional Resources	16

# **Practical Considerations Regarding Internal Auditing Expressing an Opinion on Internal Control**

## **Introduction**

The chief audit executive (CAE) may be requested to issue an opinion on the adequacy of internal controls within the organization. This request is becoming more common with the advent of new financial reporting legislation and regulation. The *International Standards for the Professional Practice of Internal Auditing* (The *Standards*), specifically Standard 2410.A1 indicates, “Final communication of engagement results, where appropriate, contain the internal auditor’s overall opinion and or conclusions.” The need for such an opinion, and the ability of a CAE to express such an opinion, depends on individual circumstances. This paper provides guidance in those situations where a CAE does express an opinion on internal controls.

Some internal auditors have not expressed opinions on the adequacy of controls in the past, either on individual audits or for organizations as a whole. Instead, only specific weaknesses in internal control have been reported. This leaves the responsibility up to the reader to interpret the importance of the issues reported and the reader may often assume areas with no issues reported were “perfect.” If a CAE issues an opinion, the CAE needs to consider the scope of the audit work, the nature and extent of audit work performed, and evaluate what the evidence from the audit means concerning the adequacy of internal controls. Such an opinion should express clearly:

- The evaluation criteria and structure used.
- The scope over which the opinion applies.
- Who has responsibility for the establishment and maintenance of internal controls.
- The specific type of opinion being expressed by the auditor.

The CAE should be careful that the opinion expressed is consistent with the internal audit activity's charter as approved by the board and supported by sufficient amount of audit evidence. A CAE should resist expressing an opinion related to a subject that is inconsistent with the charter. In addition, a CAE should not express an opinion that is not supported by sufficient audit evidence.

The CAE should also understand fully the reason and proposed use of any opinion that he or she is requested to issue. For example, does management intend to share the opinion with third parties or does management intend to place reliance on the opinion as a basis for any management attestation on controls? The CAE must ensure that any opinion is appropriate for its intended use and audience.

### **Evaluation Criteria and Structure**

An opinion is best expressed when using a defined criteria and evaluation structure. Opinions can be very poorly defined, which leads to misunderstanding of what an opinion is saying. Using a defined evaluation structure allows the reader to better

understand the opinion being expressed and helps to ensure the internal auditor is consistent in his or her formulation of an opinion across different audit areas and different time periods.

The *Internal Control-Integrated Framework*, published in 1992 and 1994 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is the most common framework for assessing internal controls.



The COSO report defines an internal control structure along five elements (control environment, risk assessment, control activities, information and communication, and monitoring) and three components/objectives (financial

reporting, operations and compliance), with identification of the areas/activities audited (e.g., geographic unit, business unit, process).

Other comprehensive structures have been developed and can be equally as useful. Governing law or other special circumstances should be considered in selecting the evaluation structure to be used.

A defined evaluation structure is especially useful to understand the scope of the audit work. For example, an opinion using the COSO framework can define whether the opinion extends to all three components of internal control and whether the audit work addressed controls along all five elements.

Many organizations have adopted their own criteria and policies on internal controls. Depending on the sophistication and detail of these policies, the CAE may use compliance with internal policies as his or her evaluation criteria. If the CAE uses, or is asked to use, an internal policy as evaluation standards, the CAE should ensure that the policies are sufficiently detailed and appropriate to serve as an evaluation standard.

## **Scope Description**

The scope over which the opinion extends should be communicated clearly in the opinion document. Common elements defining the scope over which the opinion applies are descriptions of the portions of the organization being covered (e.g., specific departments, geographic areas, or subsidiaries) or processes (e.g., financial reporting, purchasing, or IT operations), as well as the control components/objectives covered by the audit (e.g., which financial, operational, or compliance objectives were addressed). The time period over which the opinion is expressed is also a critical element of the scope (e.g., an opinion as of a point in time or an opinion regarding controls operating during a specified time period).

Typical internal audits focus heavily on internal controls related to transactional processes. Care should be taken to define whether the opinion being expressed is limited to these types of transactional controls, or if it extends to broader aspects of internal controls. For example, did the internal audit consider “soft” aspects of the control environment, like tone at the top,

adequacy of training, etc? Also, did the audit consider not only controls related to transactional accuracy, but also compliance with laws over data privacy and regulatory reporting requirements? An opinion with a well defined scope will not leave the reader guessing as to the relevance, focus of the opinion, or time period to which it applies. Many internal audit activities use a risk-based audit plan. In some situations it might be difficult to issue an opinion on internal controls as the audit work performed may not cover a clearly definable portion of the organization.

### **Defining Responsibility for Internal Controls**

Consideration should be given to clarifying within the opinion who has the responsibility for establishing and maintaining the internal controls audited. Internal controls should be the responsibility of process owners. Internal auditors provide assurance on the design and effectiveness of those controls, but are not responsible for them. This separation of responsibility and assurance is an underlying

assumption of the definition of internal auditing developed by The Institute.

### **Types of Audit Opinions**

There are two different types of opinions, positive assurance and negative assurance, and each conveys different meanings to the reader and provides different levels of assurance by the auditor. The opinion should describe the scope of work performed and the evaluation criteria and structure used. Expressing an opinion requires gathering sufficient competent supporting evidence, in conformity with the *Standards*. Different opinions likely require different levels of audit evidence. The alternative to expressing an opinion is to formally *disclaim* an opinion. This would be used when the auditor has not gathered, or is unable to gather, sufficient audit evidence to express any form of opinion and decides to clearly state that fact.

*Positive assurance* is one of the strongest types of audit opinions. In providing positive assurance, the auditor is taking a position on the strength of the

internal controls. Varieties of a positive assurance opinion are:

- Binary – internal controls are or are not appropriate in the situation, for example: internal controls are satisfactory or unsatisfactory, effective or ineffective, meet expectations or don't meet expectations, etc.
- Graded – the effectiveness of internal controls is rated using a grading system, for example: red-yellow-green, 1-2-3-4-5, etc.
- Directional – provides additional information about the direction of the opinion since a previous report, for example “Satisfactory, but diminished since last year.”

A positive assurance opinion requires the highest level of evidence as it implies not only whether controls are adequate, but also that sufficient evidence was gathered to be reasonably certain that evidence to the contrary, if it exists, would have been identified. The auditor takes full responsibility for the sufficiency of the audit procedures to find what should have been found.

Positive assurance opinions provide the reader a high level of information, which

generally brings a higher level of confidence or comfort in the accuracy of the opinion. CAEs typically are requested to provide positive assurance opinions.

The CAE should ensure that a sufficient amount of audit evidence is obtained to express their opinion. For example, work often is performed on a rotation basis across many audit units, with the scope of the work performed based on work in multiple audit units. Giving a positive assurance opinion on each of the individual units may not be possible if the amount of work done in each unit is insufficient.

A grading scale can be useful in providing sufficient information to build a positive assurance opinion. Use of a grading scale would generally require a well-defined evaluation structure. In addition, the more detailed the grading scheme, the more evidence is required to support the grades. Thus, a grading scale can provide more precision in the positive assurance opinion being expressed. For example, an opinion that merely states that internal controls meet a minimum defined criteria would not require the same amount of evidence as an opinion that stated how much better

or worse internal controls are than a defined benchmark. Increased precision in the information provided in an opinion normally increases the amount of evidence needed to support the opinion. Providing a grade as part of a positive assurance opinion may provide useful information to the reader, but sufficient evidence is needed to support that finer level of detail given in the opinion.

*Negative assurance* is a statement that nothing came to the auditor's attention that would indicate inadequate internal controls. The auditor takes no responsibility for the sufficiency of the audit scope and procedures to find all concerns or issues. Such an opinion is less valuable than a positive assurance opinion as it provides limited assurance that sufficient evidence was gathered to determine whether internal controls were inadequate. A negative assurance opinion merely states that the internal auditor has not seen problems based on the work performed.

An opinion can be *qualified* with specific findings that contradict the overall opinion. Qualified opinions can be useful in situations where there is an exception to the general opinion. For

example, the opinion may indicate that controls were, "Satisfactory, with the exception of accounts payable controls, which require significant improvement."

The *Standards* provide guidance for determining the adequacy of evidence and documentation. The CAE must ensure that any opinion expressed can be fully supported with sufficient audit evidence. The CAE should determine the level of audit evidence required to support an opinion on internal controls. This determination relies heavily on the judgment of the CAE based on the scope of the opinion and the risks in the organization being addressed by the internal controls. Some internal audit activities have sufficient resources to gather enough audit evidence to provide very definitive and descriptive opinions. Other internal audit activities do not have sufficient resources to gather enough audit evidence to provide any type of opinion other than negative assurance qualified with a clear explanation of the limited amount of testing performed.

Care must be taken with wording used in any opinion. The CAE must ensure the

wording of an opinion is clear and appropriately defined for the reader. Using general terms such as “satisfactory,” “effective,” or “adequate” alone may not sufficiently define their meaning. For example, the term “effective” usually refers to controls being effective both in design and in operation. It should be clear in the opinion whether both meanings are included. Another example is use of the general term “internal controls” which could be confusing without some definition of the type or extent of controls covered. Finally, in certain jurisdictions words have been assigned specific meanings. For example, in the United States, the terms “material weakness” and “significant deficiency” have very specific definitions and ramifications. CAEs should avoid using these defined terms unless they are reporting in accordance with the applicable regulations in that jurisdiction.

### **Interaction with Section 404 of the U.S. Sarbanes-Oxley Act of 2002**

Most organizations who file financial statements with the U.S. Securities and Exchange Commission are required to

comply with the requirements of Section 404 of the Sarbanes-Oxley Act of 2002. This section requires management to state its responsibility for establishing and maintaining adequate internal controls over financial reporting and include in the annual report an assessment by management as to the effectiveness of these internal controls.

A number of CAEs have been asked to sign an attestation stating that internal auditing has evaluated the effectiveness of internal control over financial reporting and whether they were found to be effective, or whether there were material weaknesses or significant deficiencies. Often, these attestations are drafted based on the attestation to be signed by the CEO and CFO of the organization for inclusion in the annual filings with the SEC.

CAEs should carefully consider the wording of the attestation before signing it. Signing such an attestation is expressing an opinion and the concerns discussed above come into play. Specific issues to consider include:

- If internal audit work is performed in accordance with an annual audit plan approved by the audit committee, the

objectives and scope of that plan may not provide enough audit evidence specifically related to internal controls over financial reporting to give a positive assurance opinion. By signing the attestation, the CAE is assuming responsibility for the sufficiency of the audit work done to express a positive assurance opinion. A negative assurance opinion, with reference to the scope of the internal audit plan, may be more appropriate if the amount of audit testing in this area is inadequate.

- A statement that there are no material weaknesses assumes that all areas within the organization that could have material weaknesses have been audited thoroughly enough to conclude they do not exist within the organization. If the audit plan did not cover all these areas, the opinion should be limited to the areas audited.
- The attestations drafted for signing by the CAE may refer to the adequacy of internal controls over which the signer has responsibility.

Internal auditors have no responsibility for internal controls, but only the monitoring of these controls. Any opinion expressed in support of Section 404 should not imply that the CAE has any management responsibility for internal controls.

- If the internal audit activity has performed work related to the organization's readiness for compliance with Section 404 that impairs the independence and objectivity of the internal audit activity, the impairment should be noted in the opinion expressed. The Institute has published separate guidance concerning internal auditing's role in Section 302 and 404 of the Act that discusses situations where independence and objectivity may be impaired.

### **Practical Considerations**

The following question and answer section applies the concepts described above in various situations.

**Q. Why can't I just say that "internal controls are adequate"? This is a short and clear message and I know what it means.**

A. The auditor may know what this means, but the reader may not. Such a brief statement, with no explanation of context, leaves the reader to assume a lot. For example: Does this opinion cover all regulatory aspects of the organization? Was the tone of the executive team evaluated as to its impact on internal controls and did the auditor document the evidence collected? Did the auditor test every control that exists in the organization?

**Q. How do I express in my opinion that I have sufficient basis to make this opinion?**

A. The *Standards* include discussion of the need for sufficient evidential matter to support the conclusions of an internal auditor. If the auditor's opinion states that the auditor complies with the *Standards*, the reader should be able to understand the basis for the auditor's opinion.

**Q. I don't know what type of opinion my audience requires (e.g., positive binary, positive with grading scale, or negative). What should I do?**

A. The CAE of an internal audit activity must understand the needs of the organization, which includes the needs of the reader of an opinion expressed. If the CAE does not know what type of opinion is required or what the opinion is to be used for, he or she should raise the issue with the key stakeholders, educating them on the different types of opinions possible, the effort required to express these opinions, and their relative value to the stakeholders. The results of that discussion should clarify the opinion needed from the CAE. If the readers of audit reports typically do not understand the

different types of audit opinions, an explanation could be provided as an attachment to the audit report or by reference to policy statements of the internal audit activity.

**Q. Why do I need to deal with the bureaucracy of something like the COSO framework? If I audit payroll, everyone knows what I audited.**

A. Internal controls can include financial reporting, operational, and compliance objectives and involve a range of elements from detailed control activities to the tone at the top of an organization. The COSO framework was created in part because the context of a discussion regarding internal controls is not always that clear. In the example of a payroll audit, using the COSO framework clarifies whether the audit covered items such as:

- Risk assessment activities, including management’s process for assessing the likelihood of the risk of fraudulent employees, errors in pension accounting, loss of confidential data, etc.
- Compliance with regulations regarding data privacy in all jurisdictions.
- Efficiency of handling employee-initiated changes in benefit plans elections.
- Sufficiency of training of payroll clerks.
- Adequacy of communications with employees.

A proper definition of the scope of the audit in terms of a framework like COSO would clarify these types of questions.

**Q. When would a negative assurance opinion be appropriate?**

A. A negative assurance opinion is used when the auditor does not take responsibility for the sufficiency of the audit scope and procedures to find all concerns or issues. This is a lower level of assurance than a positive assurance opinion and should only be used when a lower level of assurance accomplishes the needs of the reader. Situations where a negative assurance opinion may be appropriate include:

- Work is being performed on a rotation basis across many audit units with the scope of the work performed based on work in multiple audit units. In this case, a negative assurance opinion may be appropriate on the individual units. However, the combination of the evidence from all the units may be sufficient to express a positive assurance opinion on the group of units.
- Resources devoted to the audit were limited such that the amount of audit evidence required to support a positive assurance opinion was not obtained. In this case, the negative assurance opinion should clearly state the extent of work performed.

**Q. Don't "unsatisfactory" opinions require less audit evidence than "satisfactory" opinions?**

- A. It may be true that an internal auditor will be able to quickly, and with little effort, establish that internal controls do not meet a defined or expected level of effectiveness. In this case, expressing an "unsatisfactory" opinion may not require a large amount of audit evidence. However, in some cases, it may not be clear whether the internal controls meet or fall short of the threshold required for "satisfactory." The CAE must ensure that, with whatever opinion is expressed, sufficient audit evidence was collected to fully support that opinion.

**Q. Do all opinions need to be written? What about oral opinions?**

- A. The substance of an opinion is the same whether it is written or oral. The concerns discussed above are as applicable to oral opinions as they are to written opinions. Internal auditors should be cautious when using only oral opinions. Oral opinions are more subject to misinterpretation, are less reliably communicated to other parties, and are subject to differences in recollection at a later time. If oral opinions are used, documentation of the opinion expressed would normally be desirable in the internal audit files.

**Q. I perform audits of almost all of the transactional processes in an entity in my organization. Based on this work, can I express an opinion on the internal controls of the entity as a whole?**

A. The audit work on the processes within the entity provides an excellent foundation for an overall audit opinion. However, this work alone may not be enough to provide the overall opinion. For most entities, aspects of internal controls like the control environment, risk assessment, information flows and monitoring are not performed solely within the transactional processes, but also operate separately at the entity level. An overall opinion of the entity would need to include audit work on these entity-level controls.

**Q. Do internal controls need to meet some level defined by COSO to be adequate? Where does cost come into play when deciding whether internal controls are adequate?**

A. In most cases, internal controls are not expected to eliminate all risk of error or problems. Internal controls are expected to reduce risk to a level justified when considering the cost of the control versus the benefit from the risk reduction. These concepts are all involved in the auditor's judgment as to whether or not internal controls are satisfactory. The CAE must clearly understand the risks of an organization in assessing the adequacy of internal controls. Because risks, and the cost of controls, differ by organization, no pre-defined level of controls can be applied across all organizations. COSO does not establish any defined level of control in an organization; it only provides the framework to make that evaluation.

**Q. An external party wants an opinion from internal auditing on compliance with certain terms of the contract my organization has with that third party. Can I express an opinion in this situation?**

A. It does not sound like this is an audit of internal controls, but an audit of compliance with a contract. Most internal auditors would have the competency to perform this

work. However, there are important concerns to keep in mind when deciding whether to express this opinion to an external party:

- Is the opinion clear as to the work performed, the scope of the opinion, and time period to which it applies?
- Is the wording of the opinion consistent with the level of assurance the audit evidence provides?
- Does performance of this type of work fall within the scope of the internal audit activity as described in the approved charter?
- Has legal counsel been appropriately engaged to ensure expression of this opinion does not subject the organization to improper legal exposure? Practice Advisory 2400-1 gives guidance in this respect.

**Q. Will I be subject to criminal or civil liability if it turns out the opinion I expressed is wrong?**

A. The *Standards* delineate basic principles that represent the practice of internal auditing, provide a framework for performing these activities, establish a basis for evaluating the performance of internal audit activities, and foster continuous improvement in internal audit activities. The *Standards* do not establish or define legal liability or the lack of such liability. This is determined by the laws and regulations in the country of the internal auditor.

**Related Standards and Practice Advisories**

- |         |                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2410.A1 | Final communication of engagement results, where appropriate, contain the internal auditor's overall opinion and or conclusions.                        |
| 2410.A3 | When releasing engagement results to parties outside the organization, the communication should include limitations on distribution and use of results. |

- 2120.A1 Based on the results of the risk assessment, the internal audit activity should evaluate the adequacy and effectiveness of controls encompassing the organization's governance, operations, and information systems. This should include:
- Reliability and integrity of financial and operational information.
  - Effectiveness and efficiency of operations.
  - Safeguarding of assets.
  - Compliance with laws, regulations, and contracts.
- 2420 Communications should be accurate, objective, clear, concise, constructive, complete, and timely.
- Practice Advisory 2060-2 Relationship with the Audit Committee, covers the internal auditor's interactions with the audit committee.
- Practice Advisory 2120.A1-1 Assessing and Reporting on Control Processes, discusses the evidence needed to assess a system of internal controls and form an opinion.
- Practice Advisory 2120.A1-3 The Internal Auditor's Role in Quarterly Financial Reporting, Disclosures, and Management Certifications, provides guidance on the requirements of Sarbanes-Oxley and related SEC rules.
- Practice Advisory 2400-1 Legal Considerations in Communicating Results, gives cautions regarding the degree of assurance and the associated liabilities, focusing on U.S. law.
- Practice Advisory 2410-1 Communication Criteria
- Practice Advisory 2420-1 Quality of Communications.

**Additional Resources:**

1. Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Internal Control - Integrated Framework (IC-IF).
2. Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management – Integrated Framework (ERM-IF).
3. A Framework for Internal Auditing's Entity-wide Opinion on Internal Control.
4. Internal Auditing's Role in Section 302 and 404 of the U.S. Sarbanes-Oxley Act of 2002.

IIA Guidance Web Page: <http://www.theiia.org/guidance>