Management’s assessment of the effectiveness of internal control over financial reporting under Section 404 of the Sarbanes-Oxley Act…
## Index

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Management's responsibilities</td>
<td>4</td>
</tr>
<tr>
<td>Auditor's responsibilities</td>
<td>5</td>
</tr>
<tr>
<td>Preliminary considerations</td>
<td></td>
</tr>
<tr>
<td>Establishing a project team</td>
<td>6</td>
</tr>
<tr>
<td>Determining what documentation should be produced</td>
<td>6</td>
</tr>
<tr>
<td>Communicating with external auditors</td>
<td>7</td>
</tr>
<tr>
<td>Management's evaluation process</td>
<td></td>
</tr>
<tr>
<td>Planning the project</td>
<td>8</td>
</tr>
<tr>
<td>Controls design analysis</td>
<td>13</td>
</tr>
<tr>
<td>Testing controls</td>
<td>14</td>
</tr>
<tr>
<td>Reporting</td>
<td>17</td>
</tr>
</tbody>
</table>
Introduction

According to Section 404 of the Sarbanes-Oxley Act of 2002 (“Section 404”), management must report on the effectiveness of the company’s internal control over financial reporting (“internal control”). In addition, the entity’s external auditor (“the auditor”) must issue an attestation report (“audit of internal control”) on management’s assessment of internal control.

This document provides guidance on management’s assessment process. The document incorporates current rules issued by the Securities and Exchange Commission (“SEC”) and auditing standards issued by the Public Company Accounting Oversight Board (“PCAOB”) as of March 9, 2004. This guidance may change as a result of future rulemaking by the SEC or PCAOB.
Management’s responsibilities

Before an audit of internal control can be performed, management must perform its own assessment of the effectiveness of internal control. Accordingly, management must:

- Accept responsibility for the effectiveness of internal control
- Evaluate the design and operating effectiveness of its internal control using a suitable, recognized control framework
- Support its evaluation with sufficient evidence, including documentation and testing of controls
- Provide a written assessment of the effectiveness of its internal control over financial reporting as of the end of its fiscal year

In the United States, the Committee of Sponsoring Organizations (COSO) introduced the most widely accepted framework for evaluating controls over financial reporting. COSO defined internal control as a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations.

There is a direct relationship between the objectives, which are what an entity strives to achieve, and internal control components, which represent what is needed to achieve the objectives.

COSO identified the following five interrelated internal control components:

- **Control environment** - sets the tone of an organization, influencing the control consciousness of its people; the foundation for all other components of internal control, providing discipline and structure
- **Risk assessment** - the entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed
- **Control activities** - the policies and procedures that help ensure that management directives are carried out
- **Information and communication systems** - support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities
- **Monitoring** – a process that assesses the quality of internal control performance over time
Auditor’s responsibilities

The auditor evaluates management’s assessment process and obtains sufficient evidence about whether the company’s internal control is **designed** and **operating** effectively. This evaluation provides the auditor with a basis for expressing an opinion on the company’s internal control over financial reporting. The auditor’s report will be appropriately modified if the auditor concludes that management’s assessment process is inadequate or if management’s report is inappropriate.

**Design effectiveness** involves evaluating whether internal control is suitably designed to prevent or detect material misstatement on a timely basis. Controls will not be designed effectively if there are missing controls, or if implemented controls do not meet the appropriate control objective.

**Operating effectiveness** involves evaluating whether internal control is operating as designed. (Was the control performed? Was the control consistently performed? Was the control performed by a person who had the necessary authority and qualifications to perform the control effectively?)
Preliminary considerations

There are some initial considerations that management needs to address before beginning its evaluation process. These include:

- Establishing a project team
- Determining what documentation should be produced
- Communicating with external auditors

Establishing a project team

Management should appoint a project leader who will assist in choosing a project team. The project team should consist of individuals from internal audit, accounting and financial reporting, information technology, legal, human resources and operations. Project team members should have the appropriate skills and knowledge of financial reporting and controls. The project team should report to the CEO and CFO, although in smaller entities, the CEO and/or CFO will likely be a member of the project team. The team should develop policies and procedures for the documentation and testing plan, and for internal communications of the project’s progress and findings. Roles and responsibilities for each member of the project team should be clearly defined. The audit committee should approve the project plan.

If the entity does not have the appropriate resources or expertise, third parties may be added to the project team to assist with documentation and/or testing internal control. If third parties are employed, management remains responsible for evaluating and reporting on the design and operating effectiveness of the entity’s internal control.

Determining what documentation should be produced

The nature and extent of documentation will vary depending on the size, nature and complexity of the entity. Documentation may consist of policy manuals, process models, questionnaires, flowcharts, job descriptions, documents and forms. The documentation should include:

- The design of controls for all five COSO components of internal control
- Controls relevant to financial statement assertions
- Information about how transactions are initiated, recorded, processed and reported
- Information about the flow of transactions to enable the identification of where material misstatements could occur
- Controls designed to prevent or detect errors or fraud, including who performs the control and the related segregation of duties
- Controls over the period-end financial reporting process
- Controls over safeguarding of assets
- Controls over processes that require significant judgments or estimates
• Key decisions in management’s evaluation process (materiality assessment, locations to include in the evaluation)

• Results of management’s tests and evaluation

**PCAOB auditing standards clearly state that management’s failure to adequately document internal control is a deficiency that may also be a material weakness.**

**Communicating with external auditors**

Although management determines the nature and extent of documentation and testing, it is important to discuss these decisions with the auditor to minimize the impact of unforeseen issues e.g., which locations to include in the evaluation or the nature of control tests. Management should discuss the overall assessment process, project plan and progress with the auditor.
Management’s evaluation process

Management’s evaluation process consists of the following phases:

- Planning the project
- Controls design analysis
- Control testing
- Reporting

Planning the project

In planning the project, management assesses materiality and the risk of material misstatement of the financial statements, determines which locations or business units to include in its evaluation and determines which controls to document. These assessments must be documented.

Assessing materiality and the risk of material misstatement

Management should begin its assessment process by determining materiality and assessing the risk of material misstatement of the financial statements. These materiality assessments will enable management to determine which locations, transaction cycles and processes to document and test, and will also provide a means of evaluating the impact of identified controls deficiencies, if any, on the financial statements.

In assessing the risk of material misstatement, management considers the susceptibility of one or more financial statement assertions to material misstatement, and the risk of material misstatement due to fraudulent financial reporting or misappropriation of assets.

SEC Staff Accounting Bulletin (SAB) 99 is the SEC’s definitive statement on issues related to materiality as it relates to the preparation of public company financial statements. SAB 99 requires management to consider both the quantitative and qualitative factors when evaluating the materiality of a potential financial statement misstatement.

Determining locations or business units to include

Management should evaluate which locations or business units to include in its evaluation by identifying locations or business units that:

- Are individually significant
- Contain specific risks that could create a material misstatement
- Are significant, if aggregated with other locations or business units
The process to determine which locations to document and test is illustrated in the following table.

**Multi-location documentation and testing considerations**

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is location or business unit individually significant?</td>
<td>Document and test controls at each location or business unit</td>
<td>No further work is required</td>
</tr>
<tr>
<td>Are there specific significant risks?</td>
<td>Document and test controls over those risks</td>
<td>No further work is required</td>
</tr>
<tr>
<td>Are there locations or business units that are important when aggregated with others?</td>
<td>No further work is required</td>
<td>No further work is required</td>
</tr>
<tr>
<td>Are there documented company-level controls over this group?</td>
<td>Document and test company-level controls</td>
<td>Test internal control at individual locations or business units</td>
</tr>
</tbody>
</table>

**Determining controls to document**

Management should document governance and activities-level controls.

**Governance** or **company-level** controls are the foundation of all other controls. They are applicable to all entities, regardless of size. Governance controls are very dependent on senior management, the board of directors and audit committee and include controls to monitor operations and oversee the control environment and risk assessment process. They have a pervasive impact on controls at the activity-level.
Governance controls include:

- **Control environment** including the tone of the organization, management’s philosophy and operating style, organizational structure, assignment of authority and responsibility, human resource policies and procedures, anti-fraud procedures, such as code of conduct and ethics hotline/whistleblower program, and oversight by the board of directors, audit committee and others charged with governance

- **Risk assessment process** including how management identifies risks relevant to the preparation of the financial statements

- **Monitoring controls** including monitoring the results of operations, assessing the quality of internal control performance over time and the activities of the internal audit function

- **Information and communication controls** including roles and responsibilities pertaining to financial reporting and the information and financial reporting system

- **Information technology controls** including the management and organization of the IT department, controls over the acquisition and maintenance of operating systems, database systems and applications, security policies and procedures, and security controls to protect data and enforce segregation of duties, limit external access to the entity’s systems and protect the entity’s physical assets

---

**Effectiveness of the audit committee**

Management should evaluate the effectiveness of the audit committee’s oversight of the company’s external financial reporting and internal control. The evaluation should consider the independence, experience and capabilities of the audit committee members. This evaluation should consider how audit committee members are nominated and selected, the committee’s compliance with Sections 301 and 407 of the Act and applicable stock exchange listing standards, the level of interaction with internal and external auditors, and the amount of time that the audit committee devotes to control issues. In unique or complex industries such as financial services or technology, particular attention should be paid to the level of industry experience represented on the audit committee. The evaluation should be documented.

---

**Activities-level controls** are controls performed at the process level within a transaction cycle. They are the controls over the origination, processing, and recording of transactions. Processes are the action steps that are performed by every entity when conducting their business. The following control objectives are applicable to activities-level controls: authorization, completeness, accuracy, integrity, budgetary, reconciliation and safeguarding.
Typically activities-level controls consist of:

- Controls to check the accuracy, completeness and authorization of transactions
- Segregation of duties
- Performance reviews (reviews of actual versus budgets, forecasts and prior period performance, ratio analysis)
- Physical controls to safeguard assets
- Reconciliation controls

**Activities-level control attributes**

- Documented or undocumented
- Automated or manual
- Preventative or detective
- Foundational, operational or monitoring
  - *Foundational* controls provide an overall context or environment to ensure that the execution of activities and controls is consistent with management objectives (policies and procedures)
  - *Operational* controls provide the front line of defense in preventing, detecting, and correcting errors (comparing batch totals to predetermined numbers)
  - *Monitoring* controls ensure that all other controls are operating as designed (observation of operational controls, review of business metrics)

Management should:

1. Identify the **transaction cycles** that comprise the company’s financial reporting process

   **Transaction cycles** are groupings of various income and expense and balance sheet accounts and reflect normal business processes, double entry bookkeeping, and the functioning of accounting systems (e.g., revenue, payroll, inventory purchasing, treasury)

2. Match all **significant accounts** and **disclosures** to the identified transaction cycles

   The majority of significant accounts and disclosures are contained within the transaction cycles. However, significant accounts sometimes exist that do not pertain to any transaction cycle (for example, an environmental liability). These accounts must be evaluated separately.
3. Determine what **activities** and **processes** are performed within each transaction cycle

Ordering, shipping, invoicing and customer collections are **activities** in the revenue cycle.

Extending customer credit, maintaining the customer masterfile and generating a sales invoice are **processes** in the ordering **activity**.

Depicted as: Cycles → Activities → Processes → Controls

4. Document the processes in a manner where a person not involved in the process can understand the general flow of information (high level flow charts and brief narratives are often useful for this purpose)

5. Determine the significance of each process by assessing its relative risk (e.g., materiality, complexity, past problems, recent changes) in relation to the financial statements and disclosures (ask “What can go wrong?”)

6. Document activities-level controls in all **significant** processes, including who performs the process and the control

7. Document controls established for significant accounts and disclosures that cannot be matched to a transaction cycle

8. Document the controls over the period-end financial reporting process

Walkthroughs involve tracing individual transactions through processes from their initiation until they culminate in the financial statements. Performing walkthroughs can help management assess whether the documentation accurately reflects the company’s processes and implemented controls.

**Using service organizations**

A service organization provides services to an entity that are a part of that entity’s information system. A service organization is considered part of a company’s internal control when it provides services that affect:

- How the entity initiates transactions,
- How the entity’s transactions are processed and reported in its accounting records, supporting information, and specific financial statements accounts,
- How the entity’s transactions are processed from the initiation of the transaction to its inclusion in the financial statements, or
- How the financial reporting process is used to prepare the financial statements

Management should identify service organizations that it uses, and evaluate and document whether these service organizations are considered part of its internal control. Management should obtain the latest service organization auditor’s report on controls placed in operation and tests of operating effectiveness (a “SAS 70 Type II report”). Management should use this report to evaluate the service organization’s controls. This evaluation should be documented. If a SAS 70 report is out of date or
is not available, or if management concludes that additional evidence about the service organization’s controls is needed, management could request that a service auditor be engaged or could visit the service organization and perform the necessary procedures.

Controls design analysis

The controls design analysis phase consists of documenting governance and activities-level controls and determining whether controls are designed effectively to prevent or detect material misstatements. In evaluating design effectiveness, management considers factors such as:

- Missing controls
- Missing control objectives
- Incompatible duties
- Inappropriate mix of control attributes (lack of monitoring controls, too many undocumented controls)
- Inadequate governance controls

The design effectiveness evaluation should be documented. Management should view the entire internal control process and not just focus on one or two areas. Management may conclude that despite the existence of control deficiencies identified in its evaluation process, its internal control objectives are met due to other controls that are implemented. Management should determine whether deficiencies identified rise to the level of significant deficiencies or material weaknesses.

<table>
<thead>
<tr>
<th>Internal control deficiencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>The PCAOB categorizes deficiencies as:</td>
</tr>
<tr>
<td><strong>Inconsequential</strong> – The identified deficiencies are deemed to be negligible or insignificant, individually.</td>
</tr>
<tr>
<td><strong>Significant deficiency</strong> - An internal control deficiency that adversely affects the entity’s ability to initiate, record, process or report information reliably in its financial statements in accordance with GAAP. A deficiency (or a combination of deficiencies) should be classified as a significant deficiency if, by itself or in combination with other deficiencies, it results in more than a remote likelihood of a misstatement of the entity’s financial statements that is more than inconsequential will not be prevented or detected.</td>
</tr>
<tr>
<td><strong>Material weakness</strong> - A significant deficiency should be classified as a material weakness if, by itself or in combination with other significant deficiencies, it results in more than a remote likelihood that a material misstatement in the entity's financial statements will not be prevented or detected.</td>
</tr>
</tbody>
</table>
Testing controls

After determining that controls are designed effectively, management must test the operating effectiveness of governance and activities-level controls to obtain sufficient evidence to support its assessment. All significant controls over financial reporting need to be tested. Tests of controls are concerned with how the control was applied, the consistency with which it was applied and who applied it. These tests must be documented. Control testing should be performed throughout the year so that management can evaluate operating effectiveness “as of” the end of the fiscal year.

Testing operating effectiveness involves:

1. Identifying controls to test (key controls)
2. Selecting a testing strategy
3. Designing testing procedures, determining the number of items to test and the period that testing should cover
4. Performing control tests and evaluating the impact of any deviations found
5. Determining whether deficiencies rise to the level of material weaknesses

Management should determine how key controls will be tested. The types of control tests that can be performed include:

- Inquiry and observation
- Sampling
- Computer assisted-auditing techniques (CAAT)
- Reperformance
Tests of control considerations

When performing inquiry and observation procedures management assesses performance of the control through inquiry of appropriate entity personnel and through observation of the application of the control. Inquiry and observation alone is typically not sufficient to support a high level of assurance. Undocumented controls can only be tested with inquiry and observation.

**Sampling** is a testing method used to test the operating effectiveness of documented manual controls in a larger population. Sampling is generally not appropriate for testing a control that is performed monthly or at regular periodic intervals. In those circumstances, reperformance is used (see below). When sampling is used, the work performed on each sample item covers both control performance and the correctness of the information subject to the control. Control performance is tested by reviewing the documentation. The correctness of the information is tested by reperforming the control procedure.

In an automated environment, computer assisted-auditing techniques (CAAT) can be used to test controls. CAAT procedures vary, but always involve interrogating electronic data using a software application such as IDEA or ACL.

**Reperformance** is a testing method ordinarily applicable to manual controls that operate on an infrequent basis (monthly, quarterly, annually). When reperformance is used as a testing method, the management reperforms the control to test control performance.

Management’s testing should be sufficient to support a high level of assurance about the operating effectiveness of its internal control. This is the same standard that auditors have to achieve. While management should determine for itself how many items to test to achieve this high level of assurance, it generally is not acceptable for management to test fewer items than the auditor. Also, management will likely identify more key controls than the auditor.

It is management’s responsibility to determine the extent of testing needed to support their assessment that internal control is operating effectively. The extent of testing is determined primarily by the importance of the processes where controls are established. The more important the process, the greater the need for controls to be operating effectively. Consequently, the extent of testing for very important processes is greater than that used for somewhat important processes.
Management may find the following table useful as a guide to determine the appropriate number of items to test.

<table>
<thead>
<tr>
<th>Control frequency</th>
<th>Type of test to employ</th>
<th>Somewhat important processes</th>
<th>Very important processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Every transaction</td>
<td>Sampling</td>
<td>20-30</td>
<td>40-50</td>
</tr>
<tr>
<td>Daily</td>
<td>Sampling</td>
<td>20-30</td>
<td>40-50</td>
</tr>
<tr>
<td>Weekly</td>
<td>Reperformance</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Monthly</td>
<td>Reperformance</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Quarterly</td>
<td>Reperformance</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Annually</td>
<td>Reperformance</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

This table considers that assurance about the effectiveness of internal control is assessed in total and not on the operation of any one control. In those rare situations where a single manual documented control prevents or detects errors for a material account balance or in a very important process in a significant transaction cycle, management should consider increasing the number of items to test. When sampling, typically this increase would be at least 20 items.

**Attribute sampling** is the sampling technique applied to tests of control. As opposed to other sampling techniques used in making conclusions about specific account balances or dollar amounts, attribute sampling looks for the presence or absence of certain attributes, such as the number of times a control was appropriately performed. A population size in excess of 100 to 200 items has very little impact on the sample size when using attribute sampling.

**Evaluating deviations and concluding on effectiveness**

Operating effectiveness involves evaluating whether the control is operating as designed. As controls are designed and implemented to operate effectively all the time, a deviation is evidence that the control is not operating effectively. After considering the nature and cause of deviations found in control tests, management should determine whether the deficiency rises to the level of a **significant deficiency** or a **material weakness** by evaluating the:

- Likelihood that a misstatement could occur
- Magnitude of the potential misstatement
Evaluating internal control deficiencies

**Reporting**

Management should communicate the progress of the project and any findings to the audit committee and the auditor. Management should report significant deficiencies and material weaknesses in the design or operation of controls to the audit committee and auditor as soon as practicable.