Evaluating Internal Controls

Evaluating Overall Effectiveness, Identifying Matters for Improvement, and Ongoing Assessment of Controls
Establishing and maintaining effective internal control is an important management responsibility. Internal control is fundamental to the accurate recording of transactions and the preparation of reliable financial statements. Many business activities involve a high volume of transactions and numerous judgments regarding the related accounting for transactions, estimates, and other events that require recognition in the accounting records and financial statements. Without adequate controls to ensure the proper recording of such items, the resulting financial data may be unreliable and undermine management’s ability to make well-informed decisions, as well as damaging management’s credibility with shareholders, regulators, business partners, and the public.

While companies have long recognized the importance of strong internal control, the Sarbanes-Oxley Act of 2002 (the Act) now makes executive management responsible not just for establishing, evaluating, and assessing over time the effectiveness of internal control over financial reporting and disclosure, but also periodically asserting to its effectiveness. The Act changes the regulatory landscape for public companies and presents serious consequences for those companies that fail to comply with the new requirement. However, this new challenge presents opportunities for companies that not only recognize and accept the new regulatory landscape, but rather view the evaluation of internal control over financial reporting as more than a compliance process and recognize it as an opportunity to reach a higher level of financial reporting integrity and corporate performance.

Our publication, Preparing for Internal Control Reporting—A Guide for Management’s Assessment under Section 404 of the Sarbanes-Oxley Act (The Guide, Ernst & Young SCORE Retrieval File No. EE0677), provides a methodology and framework for completing the evaluation. The methodology outlined in the Guide includes five phases:

- Understand the Definition of Internal Control
- Organize a Project Team to Conduct the Evaluation
- Evaluate Internal Control at the Entity Level
- Understand and Evaluate Internal Control at the Process, Transaction, or Application Level
- Evaluate Overall Effectiveness, Identify Matters for Improvement, and Establish Monitoring System

Guidance on the first two phases of the methodology is provided in the Guide. Detailed guidance on the third and fourth phases is provided in two other Ernst & Young publications, Evaluating Internal Controls—Considerations for Evaluating Internal Control at the Entity Level (Ernst & Young SCORE Retrieval File No. EE0687), and Evaluating...
Internal Controls—Considerations for Documenting Controls at the Process, Transaction, or Application Level (Ernst & Young SCORE Retrieval File No. EE0692). This publication addresses the fifth and final phase.¹

Management’s report on internal control will contain its assertion that the Company maintained, as of the end of the fiscal year, effective internal control over financial reporting, based on an established set of control criteria (e.g., COSO²). “Effective” implies that management was able to conclude that internal control over financial reporting provides reasonable assurance that misstatements (either individually or collectively) caused by error or fraud in amounts that would be material in relation to the financial statements would be prevented or detected and corrected in a timely period by employees in the normal course of performing their assigned functions. In making its assessment, management will need to consider whether the significant controls that have been identified would likely prevent and/or detect a material misstatement relating to each of the relevant financial statement assertions. The approach described herein for making this determination draws upon knowledge and evidence gained from evaluating internal control at the entity level and at the significant process, transaction, or application level, and uses the results of those procedures to make an overall evaluation of the effectiveness of internal control.

A company’s certifying officers must certify each quarter that they have disclosed to the company’s independent auditors and the audit committee of the company’s board of directors all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the company’s ability to record, process, summarize, and report financial information. In this publication we discuss the concepts of significant deficiency and material weakness and describe the matters management should consider in evaluating control exceptions or deficiencies to determine whether they rise to the level of a significant deficiency or material weakness.

The evaluation of the overall effectiveness of internal control is both the end and the beginning of the process. In a dynamic business environment, controls will require modification from time to time. Certain systems may require control enhancements to respond to new products or emerging risks. In other areas, the evaluation may point out redundant controls or other procedures that are no longer necessary. The system of internal control should be self-monitoring and self-correcting. This means a company should establish mechanisms to continually evaluate and maintain the system of internal control and, when necessary, take corrective action in a timely manner. The discussion of the evaluation process and ongoing assessment included in this publication will be useful in establishing such mechanisms.

As always, we would be pleased to discuss the evaluation of internal control over financial reporting with you, and provide our advice and assistance where appropriate.

¹ At the time of publication, the Public Company Accounting Oversight Board had announced plans to issue revised standards and guidance for independent auditors in performing an audit of internal control over financial reporting. The revised standards, when issued, may alter the conditions under which an auditor can perform an audit of internal control over financial reporting and indirectly impact the requirements for management.

² In its report, Internal Control-Integrated Framework, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission provided suitable criteria against which management may evaluate and report on internal control.
Table of Contents

Overview .................................................. 1
   SEC Publishes Final Rule to
   Implement Section 404 ............................... 2

Perform Procedures to Evaluate the
Operating Effectiveness of Controls ............... 4
   Designing Procedures to Evaluate the
   Operating Effectiveness of Controls ............... 5
   Types of Controls ....................................... 6
   Prevent Controls ........................................ 7
   Detect Controls ........................................ 7
   Controls Related to IT Processes ..................... 7
   Testing Controls for Each Component of
   Internal Control ......................................... 8
   Determining the Extent of Tests of Controls ..... 9
   Timing of Tests of Controls ......................... 12
   Other Considerations .................................. 13
      Coordinating Management’s and the
      Independent Auditors’ Procedures to
      Evaluate Operating Effectiveness ............... 13
   Consider Adequacy of Tests Performed
      by Others ............................................. 13
   Fraud Prevention and Detection Programs ....... 14
   Self-Assessment Programs ......................... 14
   Consider Other Sources of Information ........... 15

Evaluate the Results of Procedures and
Identify Matters for Improvement ................... 16
   Determining Whether Control Exceptions Are
   Deficiencies in Internal Control .................... 17
   Significant Deficiencies .............................. 17
   Material Weaknesses .................................. 18
   Updating the Evaluation of Controls to the
   Date of the Assertion ................................ 19
   Documentation Considerations ...................... 19
   Summarize and Evaluate Control Deficiencies .. 19
   Identify Matters for Improvement .................. 20

Establish Processes to Evaluate the System
of Internal Control Over Time ......................... 21
   Ongoing Monitoring Activities ...................... 21
   Separate Evaluations ................................ 22

Appendix A—Review of Methodology and Steps to
Evaluate the Design Effectiveness of Controls ..... 23

Appendix B—Evaluate the Effectiveness of
Programmed Controls ................................. 25
   Tests of Programmed Controls ...................... 25
   Benchmarking Programmed Controls ................ 26

Appendix C—Summary of Control Deficiencies ........ 28
Overview

An effective system of internal control is comprehensive and involves people throughout the organization, including many who do not think of themselves as having any accounting or control responsibilities. Of course, it also involves those who keep accounting records, prepare and disseminate policies, and monitor systems as well as members of audit committees and the board of directors, who have ultimate responsibility for oversight of the financial reporting process.

The system of internal control should be under ongoing supervision and monitoring by management to ensure that it is operating as intended and that it is modified appropriately for changes in conditions. The initial evaluation effort necessitated by the Act will establish a baseline from which management can measure the continued effectiveness of internal control in a dynamic environment.

The steps to complete the overall evaluation of the effectiveness of internal control in the final phase of the methodology include:

1. Performing procedures (including testing) to evaluate the operating effectiveness of controls.

2. Evaluating the results of the procedures, taking corrective action in instances where controls do not achieve their control objectives, or otherwise identifying matters for improvement.

3. Establishing processes to evaluate the system of internal control over time.

Procedures to evaluate the operating effectiveness of controls include assessing the results of ongoing monitoring activities that are ingrained in the company’s operations and performed on a real-time basis, and other procedures that focus on evaluating operating effectiveness such as control self-assessments, special reviews by internal audit or third parties, and procedures and tests performed by members of management. Procedures to evaluate the operating effectiveness of controls also might include obtaining and evaluating reports on the operating effectiveness of internal controls at service organizations. These various procedures and tests will be needed to provide an appropriate basis for management to conclude on the operating effectiveness of controls the project team has identified and management relies on to prevent or detect and correct the types of errors or fraud that could occur.

While management is required to make an assertion as of the end of the company’s fiscal year, it ordinarily will be necessary for practical reasons to perform procedures to evaluate the operating effectiveness of controls at one or more points earlier in the year. In addition to addressing logistical issues, this can allow management time to implement corrective actions, if necessary, and re-evaluate
any remediated controls before the assertion date. Further, the Company’s external auditors will need sufficient time to consider the results of management’s procedures and to perform procedures to support their opinion on the Company’s internal control.

Management will need to update its evaluation of controls from the time of the interim procedures through the end of the fiscal year by identifying significant changes in internal control at both the entity level and at the activity/process level. The extent of the procedures management will need to perform likely will increase as the period of time between the interim testing date and year-end increases. When management plans to make significant systems changes prior to the end of the year, it should carefully consider the implications of these planned changes on its assessment of internal control, including the need to incorporate sufficient time to evaluate the operating effectiveness of the revised systems (i.e., those that will be in effect at the reporting date). It is at this juncture in the process that management also should evaluate whether it has performed sufficient procedures to support its overall conclusion as to the effectiveness of internal control over financial reporting.

The final step is for management to make an assertion about the effectiveness of internal control over financial reporting as required by the Act. To accomplish this, management will need to evaluate any control deficiencies or exceptions and determine whether they, either individually or in the aggregate, are deficiencies requiring remediation and/or might need to be disclosed to the company’s independent auditors and the audit committee of the company’s board of directors. Timely evaluation of control deficiencies will allow sufficient time for follow-up remediation and re-evaluation of controls before management must make its assertion. In addition to evaluating control deficiencies or exceptions obtained directly through procedures it performed to evaluate the operating effectiveness of controls, management also should consider information obtained from other relevant sources, including the results from work performed by external and internal auditors, and regulators.

As part of performing the comprehensive evaluation of internal control over financial reporting, the project team should evaluate whether management has implemented appropriate self-monitoring and self-correcting mechanisms, or, where appropriate, it should make reasonably specific recommendations for establishing such mechanisms. Investing in these mechanisms may serve to reduce the ongoing time and cost to comply with the requirements of Section 404 of the Act, and also might provide timely assistance to management in its quarterly certification required by SEC rules implementing Section 302 of the Act.

**SEC Publishes Final Rule to Implement Section 404**

On June 6, 2003 the SEC published its final rule to implement Section 404 of the Sarbanes-Oxley Act of 2002 (the “Act”). The final rule applies to all public companies, except registered investment companies and issuers of asset-backed securities, but including small business issuers and foreign private issuers. For “accelerated filers” (i.e., seasoned U.S. companies with public float exceeding $75 million), management and auditor reporting on internal control over financial reporting is effective for fiscal years ending on or after June 15, 2004. For all other issuers, including smaller companies, foreign private issuers and companies with only registered debt and preferred securities, the rule is effective for fiscal years ending on or after April 15, 2005.

In subsequent fiscal quarters, the rule requires management to evaluate any change that has “materially affected, or is reasonably likely to materially affect, the registrant’s internal control over financial reporting.” However, the rule does not require management to fully evaluate the issuer’s internal control over financial reporting as of the end of each interim reporting period. Instead, the SEC retained the requirement for management to evaluate on a quarterly basis the effectiveness of the issuer’s disclosure controls and procedures (as defined), which would include some, but not necessarily all, elements of internal control over financial reporting. The formal requirement to evaluate material changes in internal control over financial reporting is effective in the first periodic report following the company’s first Section 404
report. However, for periodic reports due on or after August 14, 2003, issuers must disclose any such material changes in internal control over financial reporting.

The final rule clarifies that to the extent a “material weakness” exists at the end of the fiscal year, it must be disclosed in management’s internal control report, and a material weakness would preclude management from concluding that internal control over financial reporting is effective. Further, the SEC points out in the adopting release that an aggregation of significant deficiencies in internal control over financial reporting could also amount to a material weakness that would preclude management from determining that a company’s internal control over financial reporting is effective.

The SEC’s decision to extend the transition period was, at least in part, based on concern about the cost and time it will take to properly implement the new rules. Cost and time factors also largely contributed to the SEC’s decision to not require a full quarterly evaluation of internal control, in the end believing the cost would exceed the benefits. Another contributing factor in the decision to defer the effective dates was the perceived confusion as to the level of work required of management and auditors to comply with the rules. The SEC’s adopting release clarifies that both the scope of management’s assessment of a company’s internal control over financial reporting and the level of required documentation as to the design and operating effectiveness of internal control must be extensive. Given that reporting on internal control over financial reporting is a very significant task, the SEC clearly concluded that additional time beyond the originally proposed implementation date will be required to complete it in a high quality manner. The extended transition period demonstrates that the SEC listened to the concerns expressed by commenters as to the short implementation period provided in the SEC’s proposed rule. However, management should not take this as an opportunity to delay their efforts to document and evaluate their internal control or they run the risk of not benefiting from the added time the SEC is allowing them to get ready.
Perform Procedures to Evaluate the Operating Effectiveness of Controls

In previous steps of the evaluation methodology, the project team determined whether one or more controls address the significant risks identified as “what can go wrong” questions. They also determined whether the controls that address the identified risks are adequately designed to prevent or detect errors of importance or fraud. Appendix A provides a description of the steps the project team should follow to document the design of controls identified over specific processes. The project team should be satisfied that it has addressed these steps for each significant process before designing procedures to evaluate the operating effectiveness of controls, as it would be inefficient to perform procedures to evaluate the operating effectiveness of controls that are not adequately designed or have not been placed in operation.

At this point, the project team may ask itself, “Why do we need to perform procedures to evaluate the operating effectiveness of controls?” The answer is quite simply that management’s assertion as to the effectiveness of internal control over financial reporting needs to address the operating effectiveness of the controls as well as their effective design.\(^1\)

While identifying controls that address each of the significant risks and walking through them will confirm their design and confirm whether they have been placed in operation, other procedures are needed to provide management with assurance that the controls operate effectively to reduce the risk of material misstatements in the financial statements.

Management will need to perform procedures to evaluate the operating effectiveness of controls for each significant account balance, class of transactions, and disclosure each year so as to have a basis for its annual assertion. This requirement suggests that management should, to the extent feasible, seek to implement methods to evaluate operating effectiveness that are part of the normal recurring operations of the entity.

The extent of testing and verification management needs to support its assertion is a judgmental determination. In determining the extent of necessary procedures to verify operating effectiveness, it may be practical to focus on the objectives of the procedures. The objectives of the procedures generally include determining whether the controls:

- Operated according to the way the project team understood (and documented) they would be operated.

\(^1\) In its adopting release implementing rules addressing the requirements of Section 404 of the Act, the SEC specified, “The assessment of a company's internal control over financial reporting must be based on procedures sufficient to both evaluate its design and to test its operating effectiveness.”
Were applied on a timely basis by the person(s) specified in the design of the control.

Encompassed all applicable transactions.

Were based on reliable information (i.e., information used in the performance of the control is complete and accurate).

Resulted in the timely correction of any errors identified by the controls being relied upon by management.

Management may be able to determine that controls are operating effectively through direct and on-going monitoring of the functioning of controls. This might be accomplished through regular management and supervisory activities, monitoring adherence to policies and procedures, and other routine actions such as comparisons and reconciliations, supplemented by internal audit or other compliance functions that test, monitor, and evaluate the functioning of controls, or by various self-assessment programs.

As a technique, management could ask, from the top-down, “How do we know a particular control is operating effectively?” This question may help identify current procedures in place that management can potentially rely on as a basis for its assertion that a particular control operates effectively. One example is a self-assessment program designed to monitor the operating effectiveness of one or more controls. Self-assessment programs are discussed later in this section. If management cannot identify current procedures that provide a basis for concluding the control operates effectively, it should develop procedures to test and evaluate the operating effectiveness of the controls.

**Factors management should consider in designing a testing strategy include:**

- The nature of the control and its significance in achieving the control criteria and whether more than one control achieves a particular objective.
- Whether significant changes in the volume or nature of transactions might adversely affect control design or operating effectiveness.
- Whether there have been changes in the design of the control.
- The degree to which the control relies on the effectiveness of other controls (for example, the control environment or information technology (IT) general controls).
- Whether there have been changes in key personnel who perform the control or monitor its performance.
- Whether the control relies on performance by an individual or is automated.
- The complexity of the control.

**Designing Procedures to Evaluate the Operating Effectiveness of Controls**

For certain controls or groups of controls, management may determine the most effective approach for evaluating operating effectiveness is for management, internal audit or others, under the direction of management, to design and execute procedures to test the functioning of the controls. Management is not constrained by statistical sampling or typical sample sizes used by independent auditors. The testing strategy should be sufficient to provide management with adequate information to conclude that a particular control or group of controls operates effectively.

The project team’s evaluation of the entity’s risk assessment and monitoring processes may affect its selection of the reporting units or business locations included in the assessment, the procedures performed, the controls tested, and the timing of the procedures. However, all significant reporting units or business locations and all significant controls must be evaluated in connection with each annual assessment of the effectiveness of internal control.

Procedures to evaluate the operating effectiveness of controls ordinarily include inquiry of appropriate personnel, inspection of relevant documentation, observation of the specific operations, and testing the operation of the control in the processing of selected transactions (e.g., reapplication, reperformance). The usefulness of these procedures and any other procedures that help the project team arrive at a conclusion on the effectiveness of controls depends on whether such procedures help satisfy the project team that the control in question operates as intended.
Ordinarily, some combination of procedures to evaluate controls will be needed to provide assurance that the control operated as intended. For example, the project team may observe the procedures for opening the mail and processing cash receipts to test the operating effectiveness of controls over cash receipts. Because an observation is pertinent only at the point in time at which it is made, the project team may supplement the observation with inquiries of appropriate personnel and inspection of documentation about the operation of such controls at other times. The inquiries might address: (1) whether deviations from the procedures observed ever occur and with what frequency, (2) whether errors or exceptions are ever identified, and (3) how errors or exceptions are handled.

Another example might be a project team that is testing the reconciliation of cash. The procedures might include the following techniques:

- **Inquiry** – The project team may ask the employee who prepares the cash reconciliation how reconciling items are identified, the reasons for them, and the procedures in place to ensure that the accounting records are corrected on a timely basis when there are reconciling items that require correction. The project team may also ask management how it assures itself that the reconciliations are prepared correctly and on a timely basis.

- **Observation** – The project team may observe the preparation of the cash reconciliation. However, project team members should be aware that employees might perform procedures more diligently when they know they are being observed.

- **Reperformance and Inspection of Physical Evidence** (e.g., the cash reconciliation itself) – The project team might trace the amounts on one or more of the cash reconciliations to the related records or to other documents (e.g., a bank statement) to gain assurance that the procedures were properly performed (reperformance). The project team may read or review some or all of the cash reconciliations for other periods and examine the reconciling items to determine whether the reconciliation detected errors, and whether those errors were appropriately addressed (inspection).

In designing a strategy to test the operating effectiveness of controls, the project team might determine that it need not test all controls that have been identified. For example, if the project team believes that a particular assertion is likely to be supported by more than one control, it does not need to test all of the controls; rather the project team might decide to test only the key controls on which management intends to base its assertion. The choice of the controls to test depends on the team’s evaluation of (1) whether the controls to be relied on are likely to be effective in supporting the related financial statement assertion, and (2) whether the controls can be tested more effectively and efficiently than the other controls. If the project team believes that one control supports more than one assertion, the project team may test that control once to support achievement of all of the related assertions.

Inquiry is a procedure that typically is used extensively throughout the evaluation process and usually is complementary to performing other procedures. Inquiry consists of seeking information of knowledgeable persons and may range from formal written inquiries to informal interviews. Often the information obtained through inquiry is corroborated by other inquiries (both written and oral). Evaluating responses to inquiries is an integral part of the process. Inquiry alone generally will not provide sufficient evidence to support the operating effectiveness of controls.

### Types of Controls

Controls can include any procedures used and relied on by management to: (1) prevent material misstatements, whether caused by error or fraud, from occurring during transaction processing or (2) detect and correct on a timely basis material misstatements that may occur in processing transactions. Two broad types of controls and their descriptions are listed below.

<table>
<thead>
<tr>
<th>Control Types</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Controls</td>
<td>Policies and procedures designed to prevent an error or fraud. Prevent controls are normally applied to individual transactions.</td>
</tr>
<tr>
<td>Detect Controls</td>
<td>Policies and procedures that are designed to detect and correct errors or fraud that might preclude the achievement of the relevant process objectives. Detect controls generally are applied to groups of transactions.</td>
</tr>
</tbody>
</table>
Prevent Controls

To be effective, systems of internal control should include strong prevent controls (either programmed or manual) in addition to detect controls. For example, where there is a high volume of transactions, a lack of prevent controls, such as edit or validation checks, on the input of transactions before they are recorded significantly increases the risk of errors and increases the need for particularly sensitive detect controls. In the absence of prevent controls, a high number of errors can render detect controls ineffective in detecting and correcting errors in a timely manner. Prevent controls often are programmed controls and can take a myriad of forms. In addition to edit or validation checks, prevent controls may include approvals, segregation of duties, file or transaction transmission controls, automated postings to ledgers, and automated functionality (e.g., translation, mapping, calculations).

The type of prevent control also often affects the type of evidence available to support the functioning of the control. For example, an effective manual prevent control (e.g., the shipping staff’s comparison of picked merchandise to the bills of lading) may not result in any physical evidence indicating whether the control was performed, by whom, or how well.

In other cases, there may be evidence that indicates performance of the control, but evidence regarding the effectiveness of the controls may not be available. For example, a signature on a voucher package to indicate that the signer approved it does not necessarily mean that the person carefully reviewed it before signing; the package may have been signed based on only a cursory review (or without any review). As a result, the quality of the evidence regarding the effective operation of a prevent control evidenced by a signature or initials may not be sufficiently persuasive to become satisfied that the control operated effectively without testing of the validity of the data. The project team may need to look to other available evidence, such as interviews with supervisors or other evidence of supervisory oversight, to corroborate that the signatures are evidence that the prevent control is functioning. Thus, when the control is a checking routine (e.g., checking prices, extensions, additions) evidenced by a signature or initials, the project team should reperform the checking routine as part of the test of the control.

Tests of controls normally should not take the form of tests of individual transactions to infer the effectiveness of controls, unless it is not otherwise practical to design direct tests of the controls to support their proper functioning. For example, it generally is not appropriate for the project team to simply test a sample of cash disbursement transactions to determine that transactions are properly recorded in the accounting records and then infer that all controls associated with initiating, recording, processing, and reporting those transactions function as intended.

Detect Controls

In contrast to manual prevent controls that are often accompanied only by evidence suggesting that the control operated (e.g., initials, signatures), detect controls, such as a monthly reconciliation, are often accompanied by physical evidence of their performance (e.g., a completed reconciliation). The project team normally should examine evidence that the reconciliation was properly completed (including tracing certain amounts for agreement) and that the appropriate reviews and follow-ups were carried out.

Evaluating detect controls also can be more efficient than manual prevent controls because detect controls often are applied to groups of transactions rather than on a transaction-by-transaction basis, and they are performed less frequently than prevent controls. Management may place more emphasis on prevent controls on the premise it is more efficient to prevent errors or misstatements, however, no system of controls can be expected to be totally effective and should incorporate an appropriate mixture of prevent and detect controls.

Controls Related to IT Processes

We anticipate that, except in certain rare instances, the project team will determine that management is relying on IT programmed controls (i.e., controls performed by a computer) or that identified controls are dependent on IT-generated data (i.e., electronic evidence). The project team will need to evaluate the effectiveness of controls that management relies upon to ensure that the programmed controls or the electronic evidence relied upon in the performance of other controls continue to operate effectively over time. Ordinarily companies that rely heavily on IT applications have implemented IT general controls that are applied above the computer application (i.e.,
Perform Procedures to Evaluate the Operating Effectiveness of Controls

Illustration 8.1—Evaluate the Effectiveness of Programmed Controls

The project team should evaluate the operating effectiveness of significant controls for each of the components of internal control in each annual assessment. Project teams may have difficulty identifying the type (or nature) of tests of controls they should design and execute to evaluate the operating effectiveness of certain components of internal control. It generally will be easier to design and execute tests of controls within control activities and information and communication components since many of these controls operate at the significant account, class of transactions, or disclosure level. The project team may find it more difficult to design and execute tests to evaluate controls for the

Certain aspects of the company’s electronic information may exist only at a certain point in time, or such information may not be retrievable after a specified period of time. Therefore, the project team will need to consider the time during which information exists or is available in determining the nature, timing, and extent of their tests of controls. For example, the project team might determine that it will need to perform a portion of its planned procedures to test controls over transaction processing at various times throughout the year.

Appendix B—Evaluate the Effectiveness of Programmed Controls provides additional examples of procedures the project team might perform to evaluate the operating effectiveness of programmed controls.
control environment, risk assessment, and monitoring components since many of the controls comprising these components operate as entity-wide controls and therefore evidence gathered about their operating effectiveness generally will be less conclusive and require more subjective judgment on the part of the project team.

Entity-wide controls are controls the company has implemented to monitor the operations at various locations or business units and therefore operate over controls at the various locations or business units and may encompass a number of aspects of the control environment, risk assessment, and monitoring components of the entity’s overall internal control. These entity-wide controls are important because they might have a pervasive effect on controls over individual processes at individual locations or business units, and increase or decrease the likelihood that such controls will continue to operate as intended.

Entity-wide controls ordinarily include a combination of the following:

- Management’s assignment of authority and responsibility, use of consistent policies and procedures, and implementation of entity-wide programs such as codes of conduct and fraud prevention that apply to all locations and business units.
- Centralized processing and controls, including shared service environments.
- Monitoring results of operations.
- Monitoring of controls, including activities of the internal audit function and self-assessment programs.

Entity-wide controls relating to the risk assessment component of internal control might include management’s identification of the risks of material misstatement in the significant accounts, classes of transactions, and disclosures and related assertions in the financial statements and its implementation of controls to prevent or detect errors or fraud. For example, the risk assessment process may address how management considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements. Management’s assessment may result in it assigning levels of authority for transactions based on perceived risk. Risks relevant to reliable financial reporting also relate to specific events or transactions. The project team should consider whether previous failure to identify such risks or to control them is a deficiency that should be addressed.

Entity-wide controls relating to the information and communication component generally are the same systems and processes covered by the audit of financial statements (e.g., accurate and timely financial information, controls over systems development, access to IT resources and data, and business continuity/disaster recovery planning). This component also includes controls that ensure the safeguarding of assets and processes for authorization of transactions and the maintenance of records.

Entity-wide controls relating to the monitoring component extends to management’s monitoring of the functioning of the significant controls, including control activities, that management has designed to prevent or detect errors of importance in significant accounts, classes of transactions, and disclosures and related assertions in the financial statements. Controls relating to the monitoring component also include the role and functioning of internal audit and management’s processes for responding to internal control recommendations and correcting known deficiencies.

Because of their potential pervasive impact on the effectiveness of other controls, the project team should evaluate entity-wide controls closely. The relative strength of entity-wide controls is one of several factors the project team should consider in determining the extent of testing of individual controls at the process, transaction, or application level.

**Determining the Extent of Tests of Controls**

Management can evaluate the operating effectiveness of controls by designing and executing tests of the controls or through regular management or supervisory activities, robust control self-assessment programs, or other routine actions. The project team may vary from year to year the nature, timing, and extent of its procedures to evaluate controls however, management will need to gather evidence as to the operating effectiveness of controls for each significant account balance, class of transactions, and disclosure in each annual assessment. For example, the
The project team may test the controls at a different interim period; increase or reduce the number of tests performed; or change the combination of procedures used. The tests of controls should be designed to provide evidence to enable management to conclude whether the company’s system of internal control over financial reporting (i.e., including the controls in all five components) is operating effectively. The project team also should be mindful that varying the extent of testing in a particular year potentially could affect the external auditor’s determination of the nature, timing and extent of its procedures to evaluate the operating effectiveness of controls.

Because the internal control components are interrelated, the evidence produced from the combination of tests of each component provides better evidence that the company’s internal control is operating effectively than evidence from tests of only a single component. Similarly, tests of more than one control related to a significant account provide better evidence than a test of a single control for a significant account. Accordingly, in addition to testing the entity-wide controls related to significant accounts (that is, the control environment, risk assessment, and monitoring controls), the project team also should perform some tests of control activities for each significant account balance, class of transactions, and disclosure in each annual assessment.

The project team will need to use judgment to determine the extent of procedures (i.e., testing an individual control) necessary to support management’s assertion as to operating effectiveness. There are a number of factors the project team should consider which are listed below:

- **How often the control is performed.** The less frequently the manual control is performed (e.g., a manual control applied monthly compared to a manual control applied on a transaction-by-transaction basis) the fewer number of times the test needs to be performed in order for the project team to be satisfied regarding the effective operation of the control. Likewise, if the control is a programmed control the testing may be less extensive since the control will always function in the same manner until the program is changed.

- **The degree to which management plans to rely on the control as a basis for its assertion.** The higher the degree of reliance the more extensively the project team should test the control to provide the desired assurance. When other controls, related to one of the assertions, are also in place and tested, the level of assurance that might be needed from any one control need not be as high as would be the case where management is placing reliance solely on the one control.

- **The persuasiveness of the evidence produced by the control.** If the performance of a control activity results in little or no direct evidence that the control or control activity operated effectively, then testing it — no matter how extensively — may not provide the necessary assurance. Conversely, if direct evidence regarding the effective operation of a control is available, the project team might decide that they only need to examine a limited amount of the evidence to be satisfied regarding its effective operation.

- **The relative importance of the possible errors that could result if the control is not functioning.** Matters to consider in assessing the amount of assurance needed from the test include:
  - The materiality of the transactions being processed.
  - The complexity of the transactions.
  - The volume of transactions.

- **Other factors that relate to the likelihood that the control operated as intended.** In determining the extent of tests, the project team also should consider several other factors that affect the likelihood that the control is operating as intended. Such factors may include:
  - The competency of the person who performs the control. The apparent competence and integrity of the employees performing the control, their objectivity about the related processing procedures, the degree to which the employees are supervised, and the extent of employee turnover all contribute to the likelihood that the control operates as intended.
  - The effectiveness of internal control at the entity level. The effectiveness of internal control at the entity level may influence (either positively or negatively) the
operating effectiveness of a specific control, and it also may influence the project team’s determination of the extent of testing. For example, in deciding on the extent of testing, the project team should consider:

- The likelihood that a control is bypassed during peak processing periods.
- The potential for management override of a control.
- The potential risk of fraud.
- The extent to which the controls have been subjected to on-going monitoring activities throughout the year.
- The likelihood that a control will continue to operate as intended until year-end (i.e., the date of management’s assertion). Effective internal control at the entity level provides a basis for expecting that controls tested during the year will continue to operate as intended until year-end.

Changes in the related processes. When there are changes in the related processes during the year, the project team might consider whether a control continues to be effective after changes to the process have been implemented. This can be especially true when implementing a new IT application.

Even though one or more of the factors just described may reduce the expectation of errors, the procedures to evaluate the operating effectiveness of controls need to be sufficiently extensive to provide appropriate evidence that the controls are operating effectively. The project team will need to exercise judgment in determining the appropriate sample size, and, regardless of the size of the test, it should plan to investigate all control exceptions (i.e., control did not function as designed). Generally, in situations where the project team is performing tests of more than one control related to a significant account, class of transactions, or disclosure, and where deviations from designed controls are not expected and the likelihood of material errors is considered low, the samples need not be large. In situations where deviations from designed controls are expected, the likelihood of errors or override is considered other than low, or the control is the primary or only control related to a significant account, class of transactions, or disclosure, larger sample sizes may be appropriate. There may be other circumstances, for example when a control is applied by a number of different personnel at various reporting units, where larger sample sizes also may be appropriate.

The project team may need to exercise additional judgment in determining the extent of its testing of a control which functions over a common process that is applied throughout numerous locations or reporting units of a company. For example, company policy may require that operations personnel obtain a credit check from an external source before extending terms to a customer. On one hand, the control is designed to function similarly across all locations or reporting units. However, different personnel execute the control at each of these locations or reporting units, and therefore the control may not function with the same operating effectiveness, or the control may be overridden.

In addition to considering the factors discussed previously (e.g., importance of the control to management’s assessment, control is one of a combination of controls, competence of those who perform the control), the project team also should consider whether management has implemented procedures to monitor the terms extended to customers at the various locations or reporting units, and monitor the functioning of the controls. In this example, routine monitoring of the terms extended to customers by management, or internal audit procedures to determine that the control is functioning as part of ongoing monitoring activities, may allow the project team to evaluate the

**Sample Sizes**

While the extent of testing is a judgment, statistically based sample sizes can be useful in promoting a consistent approach to testing individual controls across an organization. Generally, a sample of 25, without the occurrence of exceptions, provides a statistical reliability of 90% that the error rate does not exceed 10%. In situations where the project team is testing a number of controls to evaluate the effectiveness of internal controls that are responsive to one or more assertions, sample sizes of 25 or more generally would provide a sufficient basis for concluding a control operated effectively. The project team should consider larger sample sizes when the control it plans to test is the only control identified for one or more significant assertions. Sample sizes of 60 or more provide a statistical reliability of 95% that the error rate does not exceed 5% when no exceptions are found.
effectiveness of these higher level controls and limit the number of times it plans to test the functioning of the individual control (i.e., obtaining a credit report). In the absence of these monitoring activities, the project team likely will determine that it needs to expand the number of times it plans to test the functioning of the control across the various locations or reporting units to support management’s evaluation.

When a project team is determining the extent of its tests of a control, it should consider the work it undertook as part of its earlier walk-through of the process to verify its understanding of the related controls. In certain cases, a walk-through might provide sufficient evidence of operating effectiveness. For instance, a walk-through of a computer process and the related programmed control may, in some cases, allow the project team to conclude that the control is operating effectively. This conclusion might be based on the premise that a programmed control is systematic and if successfully tested once, and IT general controls are effective, it will work the same way repeatedly unless the program is changed.

If the project team observes an exception, it should be careful not to dismiss the exception as a random (non-systematic) occurrence. Accordingly, if a sample was selected for testing based on the expectation of not finding any exceptions, the detection of one control exception should result in the project team:

- Performing a qualitative analysis to determine the cause for the control exception.
- Extending the test (in anticipation of determining that, while control exceptions exist, the rate of occurrence is acceptable to management).
- Amending its decision to rely on that control.
- Considering whether another control is available that can be substituted for the one being tested.

If the project team extends its testing and additional control exceptions are observed, they should either address how to correct the control so the error does not continue to occur, or they should identify another control that addresses the assertion. The other control is a different control or set of controls that achieve the same control objective as the original control. Timely evaluation of control exceptions and follow up remediation of deficiencies or identification of other controls will enable management to take advantage of the point-in-time nature of its assertion on internal control. If addressed early, management can allow sufficient time to re-evaluate the control and conclude whether it operates effectively.

**Timing of Tests of Controls**

The period of time over which controls should be evaluated is a matter of judgment, however, it should vary with the nature of the controls being evaluated, the frequency with which specific controls operate, and the specific policies that are applied. Some controls operate continuously (e.g., controls over sales), while others operate only at certain times (e.g., controls over the preparation of financial statements, controls over physical inventory counts). The project team should evaluate controls over a period of time that is adequate to determine whether the controls necessary for achieving the relevant assertion are operating effectively.

As a matter of necessity, the project team will need to evaluate controls before the end of the fiscal year and, therefore, the project team will need to update its evaluation of controls from the time of the original procedures through fiscal year end. The project team will need to determine what additional evidence should be obtained for the remaining period. In making that determination, the team should consider the specific controls that were originally tested, the degree to which evidence about the operating effectiveness of those controls was obtained, and the length of time from the original date of testing to the end of the year. Generally, the extent of the procedures the project team performs to update its evaluation should increase as the period of time between the original testing date and year-end increases. For example, the performance of control testing in June would require more extensive procedures to update the evaluation than the performance of testing in October for a company with a December year end. The project team also should obtain evidence about the nature and extent of any significant changes in internal control at the entity level and at the activity/process level that occurred subsequent to the original evaluation procedures.

Some controls over financial reporting may only operate after the date of management’s assertion (i.e., end of the company’s fiscal year). For example, many aspects of the financial
statement close process only function after year end. The project team will need to ensure that its procedures to evaluate the operating effectiveness of controls includes those significant controls that only operate after year end.

Other Considerations

Coordinating Management’s and the Independent Auditors’ Procedures to Evaluate Operating Effectiveness

The entity’s independent auditors may consider the results of the entity’s procedures to evaluate the operating effectiveness of controls in determining the nature, timing and extent of their procedures. However, the independent auditors will need to obtain the principal assurance as to the overall effectiveness of the entity’s internal control from tests they have performed. Similarly, the independent auditors should not rely solely on the results of procedures performed by others (i.e., internal audit) as evidence of the operating effectiveness of controls over significant account balances, classes of transactions, and disclosures. Generally, this means the independent auditors will need to reperform or perform independent tests of controls for each significant account balance, class of transactions, and disclosure to corroborate the results of any tests performed by others that it plans to rely on. The independent auditors may not use the results of tests performed by others in evaluating evidence about the control environment, including fraud related programs and controls, and additionally must limit the use of the work of others in evaluating:

- Controls that have a pervasive effect on the financial statements (such as IT general controls on which the operating effectiveness of other controls depend).
- Controls over significant non-routine and non-systematic transactions (such as accounts involving judgments and estimates).
- Controls over the period-end financial reporting process, including controls over procedures used to enter transaction totals into the general ledger; to initiate, record, and process journal entries in the general ledger; and to record recurring and nonrecurring adjustments to the financial statements (for example, consolidating adjustments, report combinations, and reclassifications).

These requirements may limit the extent to which testing procedures performed by internal audit and other groups may be used by the independent auditors to reduce the required extent of their work. While management cannot rely on the results of the independent auditors’ testing in forming its conclusions, there may be complementary testing strategies that result in an appropriate and efficient testing of the operating effectiveness of controls.

Consider Adequacy of Tests Performed by Others

Procedures to evaluate the operating effectiveness of controls might include testing performed directly by management personnel (including control self assessment processes) or by internal audit or third parties under the direction of management. Procedures to evaluate the operating effectiveness of controls also might include service organization reports that include procedures to determine if controls are operating effectively. Regardless of who performs the tests to evaluate operating effectiveness of controls, the project team must satisfy itself that the nature and scope of the various tests provide sufficient evidence to support management’s assertion as to the overall effectiveness of internal control, and those persons performing the tests or other evaluative procedures are objective and competent to do so.

If a service organization is part of the entity’s information system and, accordingly, is part of the entity’s internal control, the project team should consider the activities of the service organization, including obtaining an understanding of the controls at the service organization that are relevant to the entity’s internal control and determining that those controls are operating effectively. Performing procedures at the service organization or obtaining a service auditor’s report may provide such evidence. If a service auditor’s report on controls placed in operation and tests of operating effectiveness is available, the project team may consider whether this report provides sufficient evidence to support management’s assertion. The items the project team should consider include: the scope of the examination and applications covered, the controls tested and how they relate to the entity’s internal controls, the results of those tests of controls, the service auditor’s opinion on the operating effectiveness of the controls, and the time period covered by the service auditor’s tests of controls and its relation to the date of management’s assertion. A service auditor’s report that does not include tests
Perform Procedures to Evaluate the Operating Effectiveness of Controls

of controls and the service auditor’s opinion on operating effectiveness (i.e., “report on controls placed in operation”) does not provide evidence of operating effectiveness.

When the period of time covered by the tests of controls in the service auditor’s report significantly precedes the date of management’s assertion (e.g., service auditor’s testing performed through June 30 and management’s assertion is as of December 31), the project team should perform additional procedures, including making inquiring of appropriate personnel within the company who are responsible for the company’s relationship with the service organization. The inquiries should focus on whether management has identified any changes in the service organization’s controls subsequent to the period covered by the service auditor’s report (e.g., changes communicated to the company through communications from the service organization, changes in personnel at the service organization with whom company personnel interact, changes in reports or other data received from the service organization, changes in contracts or service level agreements with the service organization, errors identified in the service organization’s processing). If such changes are identified, the project team should perform procedures to evaluate the effect of such changes on the assessment of internal control.

Fraud Prevention and Detection Programs

Management also should consider evidence about the operating effectiveness of its fraud prevention and detection programs in evaluating the overall effectiveness of the entity’s internal controls over financial reporting. Generally, the steps that management implements to prevent, deter, and detect fraud include:

- Creating and maintaining a culture of honesty and high ethics.
- Evaluating the risks of fraud and implementing processes, procedures, and controls needed to mitigate the risks and reduce the opportunities of fraud.
- Developing an appropriate oversight process.

The steps management undertakes to create and maintain a culture of honesty and high ethics most likely are rooted in a strong set of core values that provides the foundation for employees as to how the organization conducts its business. These steps should include:

1. Setting the tone at the top.
2. Creating a positive workplace environment.
3. Hiring and promoting appropriate employees.
4. Training about the entity’s values.
5. Periodic confirmation of accountability.
6. Disciplining incidents of fraud or wrongdoing.

Management generally can evaluate the operating effectiveness of these steps through its assessment of the control environment component of internal control over financial reporting. Specific activities that the project team might evaluate include oversight processes of the audit committee, the board of directors, and management:

1. Reinforcing the entity’s commitment to creating the appropriate tone and high ethical values,
2. Providing mechanisms for employees to report concerns about unethical behavior, actual or suspected fraud, or violations of the entity’s code of conduct,
3. Demonstrating proactive involvement and oversight of financial reporting activities,
4. Proactively investigating indicators of fraudulent activities.

Self-Assessment Programs

Management may be able to use the results of robust control self-assessment programs to, at least in part, evaluate the operating effectiveness of various controls. Self-assessment programs are becoming a popular method of incorporating the real-time nature and efficiency of ongoing monitoring activities into separate evaluations that provide an explicit, documented assessment and reporting to management.

Companies that have implemented one or more control self-assessment processes will want to determine the extent these processes can be leveraged to evaluate the operating effectiveness of controls over financial reporting. The degree to which these programs can be effectively leveraged will depend on the focus of the self-assessment processes and the nature and extent of the assessment procedures. If the control self-assessment processes focus on business processes,
efficiency and effectiveness of operations, or compliance
with various laws and regulations, and only indirectly on
assessing the effectiveness of controls over financial
reporting objectives, they likely will not provide a basis for
evaluating internal control over financial reporting. In such
cases, management should consider expanding the focus of
these processes to include assessment of key controls that
assure achievement of financial reporting objectives.

Similarly, some self-assessment programs involve only
survey or inquiry of those who operate the control(s). Inquiry
alone does not adequately evaluate whether the controls are
operating effectively and will need to be supplemented with
other procedures to provide an appropriate basis to support
management’s assessment. In the absence of objective
verification procedures to evaluate operating effectiveness,
self-assessment processes generally function as part of
management’s risk assessment or monitoring processes by
creating awareness of poorly designed or missing controls.

Consider Other Sources of Information
The project team should consider other relevant sources of
information in addition to its own documentation and
testing to provide management with all of the information
it will need to make its assertion about the effectiveness of
internal control. The following sources of information
might be relevant to management’s assessment:

- **Work Performed by External Auditors**—The external
  auditors may identify errors and weaknesses in performing the
  financial statement audit. Among the items that could
  provide information with respect to errors or weaknesses are
  legal letters and other substantive audit procedures
  (e.g., confirmation requests returned noting differences).

- **Internal Audit Reports**—Internal audit reports issued
during the year may include discussions of weaknesses in
internal control and related matters.

- **Service Organization Reports**—Situations may arise
  where a service organization report indicates weaknesses in
  the controls, either at an outside service organization
  that is part of the entity’s internal control, or at the entity
  when the subject of the service organization report is one
  or more operations of the entity (e.g., trust operations of a
  bank holding company, investment operations of an
  insurance company). These weaknesses in the controls of
  the service organization also may affect the controls of
  the company.

- **Regulatory Reports**—Recent regulatory reports of
  examination, supervisory memorandums, or reports of
  regulatory actions to which the company has been
  subject may provide information with respect to errors or
  weaknesses.
The project team should document and accumulate all control exceptions encountered in performing tests of operating effectiveness of controls. A control exception or deviation occurs when procedures used to evaluate operating effectiveness indicate that a control did not operate as intended.

For example, the project team might find that key information was not reconciled, reconciling items were not investigated in a timely manner, or the error identified by the control was not corrected in a timely manner. The project team also may find that higher-level monitoring controls did not result in appropriate follow up, or that the follow up was not effective in achieving the relevant assertions. When the project team identifies a control exception, it should consider the results in relation to management’s overall evaluation of internal control and determine whether the exception potentially indicates there is a deficiency in the design or operating effectiveness of the control, or both. The project team also should attempt to identify the underlying cause of the error, if possible, to determine whether the error is due to specific circumstances (e.g., the person that normally applies the control was on vacation and the control did not work). If the project team determines the error and its cause have been corrected, and is satisfied the control is now working as designed, the control is likely to be effective as of the date of management’s assertion.

Other procedures the project team should perform when control exceptions are found include:

- **Confirm its understanding of the control**—Upon further investigation, the project team may determine that its earlier understanding of the process and the related controls was incorrect. Therefore, the controls previously documented by the project team are not functioning and they should determine whether other controls are in place and, if so, identify, evaluate and test the other controls.

- **Consider the cause and implications for each exception**—Knowing the cause of a control exception aids in determining the potential for errors of a similar type and the need for changes in procedures to evaluate controls. For example, the project team might consider whether the exception is systematic (one that can be expected to occur in every similar circumstance) or apparently random. The project team also should consider whether the control exception is intentional or unintentional.

- **Determine the accounts and processes affected**—The project team should understand all the significant financial statement accounts affected by the control exception. For example, a control exception indicating that cash disbursements may not be appropriately recorded in the general ledger has implications for many financial statement accounts.

- **Consider the potential effect on management’s assertions**—If the identified controls are not in place or are not effective in preventing and/or detecting material misstatements in an account balance, class of transactions, or disclosure and related assertion, additional or different manual or programmed controls may need to be identified and evaluated.
Determining Whether Control Exceptions Are Deficiencies in Internal Control

The project team will need to analyze and evaluate the errors and control exceptions identified in testing the operating effectiveness of controls, and from other sources, to determine whether they represent deficiencies in internal control, and their effect on management’s assertion. A design deficiency exists when either a necessary control is missing or an existing control is not properly designed to achieve the desired control objective. An operating deficiency exists when a properly designed control either is not operating as designed or the person performing a control does not possess the necessary authority or qualifications to perform the control effectively.

The project team should consider the following factors in evaluating errors, exceptions, and control weaknesses:

- Has the cause of the error or control exception been identified and corrected?
- How was the error or control exception detected? For example, if detected by management as part of the normal process, overall internal control may be effective due to the existence of compensating controls.
- Is the error or control weakness confined to a single application, or is it pervasive?
- Assuming the control weakness is not pervasive, is the error or control exception attributable to occasional carelessness or inadequately trained staff?
- Provided the error or control weakness is confined to one application, how significant is the application to the overall entity? For example, for a financial institution, a control weakness discovered in the lending area, which is confined to leasing activities where leasing activities represent only an immaterial portion of total loan activity, may not be significant.
- How significant is the deviation from stated policy? For example, if policy states that accounts are reconciled within four weeks of month end, an exception where reconciliations were not performed for six months might be more significant than an exception where reconciliations were actually done within six weeks.
- What is the likelihood that other similar errors have occurred and remain undetected?
- How frequent are deviations or control exceptions in relation to the frequency of performing the control?

This list is not intended to be exhaustive; its purpose is to stimulate thought with respect to other questions that may be relevant in the circumstances. The project team’s consideration of these factors and responses to the team’s other inquiries may indicate that the noted errors or control exceptions are deficiencies that require reporting to management. The project team also may conclude that the deficiency rises to the level of a significant deficiency or material weakness as defined by the SEC and in auditing literature, and described in the following sections.

Significant Deficiencies

A significant deficiency is an internal control deficiency in a significant control or an aggregation of such deficiencies that could result in a misstatement of the financial statements that is more than inconsequential. A significant deficiency may result from either a design deficiency or lack of operating effectiveness.

In determining whether the control exception potentially indicates there is a deficiency in either the design or operating effectiveness of the control, some factors the project team should consider include:

- Whether the control is automated (i.e., in the presence of effective general controls, an automated application control is expected to always perform as designed).
- The degree of intervention by company personnel contributing to the deviation.
- If management was aware of the deviation, the actions taken by management in response to the issue.

If the reasons for the exception do not indicate a weakness in the general design or operation of the control, then the deviation may not indicate a significant deficiency. However, regardless of the reasons for the deviation, numerous or repeated instances may constitute a significant deficiency. A control with an observed non-negligible deviation rate is not an effective control.
The project team may identify multiple control exceptions or deficiencies that are common to a specific account, control component, or location or reporting unit, or otherwise have common features or attributes. A number of internal control deficiencies that have a common feature or attribute may rise to the level of a significant deficiency even though the control exceptions or deficiencies are individually insignificant. For example, the project team may identify numerous instances in which management’s risk assessment process operates deficiently with regard to accounts or locations or both. Similarly, the project team may determine that a reconciliation of detail to the general ledger has not been performed across a range of accounts or business units. Although such deficiencies, if isolated occurrences, may not be individually evaluated as a significant deficiency, the project team may conclude that multiple instances of a deficiency around a common theme rise to the level of a significant deficiency.

A significant degree of judgment is required in evaluating whether an internal control deficiency is a significant deficiency. Additional factors the project team should consider include:

- The frequency of exceptions in the operation of a control.
- The likelihood that the internal control deficiency could result in a misstatement.
- The magnitude of potential misstatements in the financial statements resulting from the internal control deficiency.
- The importance of the control that is deficient, including the degree to which other effective controls achieve the same control objectives.
- The nature of the account balances or classes of transactions affected by the internal control deficiency and the financial statement assertions involved.

Material Weaknesses

A material weakness is a significant deficiency or an aggregation of significant deficiencies that precludes the entity’s internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis by employees in the normal course of performing their assigned functions.

Evaluating whether a significant deficiency is also a material weakness is a subjective process that depends on various factors. These may include the nature of the accounting system and of any financial statement amounts or transactions exposed to the significant deficiency, the overall control environment, other controls, and the judgment of those making the evaluation. The absence of identified misstatements is not a criterion for concluding that significant deficiencies do not constitute material weaknesses.

The project team should focus on both the likelihood and potential impact of misstatements that could arise, either due to error or fraud, and remain undetected. The potential misstatement could range from zero to more than the gross financial statement amounts or gross amounts of transactions that are exposed to the significant deficiency. However, the likelihood of misstatement due to error or fraud generally will vary for the different possible amounts within that range. For example, the risk of misstatement due to error or fraud in amounts equal to the gross exposure might be very low, but the risk of smaller amounts might be greater.

There may be situations where the project team will need to consider whether individual significant deficiencies, when aggregated, amount to a material weakness. In these situations, the project team should consider the following in making its evaluation:

- The range or distribution of the amounts of potential misstatement, whether caused by error or fraud, that may result during the same accounting period from two or more individual significant deficiencies.
- The likelihood that such a combination of misstatements would be material.

Similar to evaluating whether deficiencies are significant in the aggregate, the project team generally will consider significant deficiencies in the aggregate to also be a material weakness when it determines the impact of a potential misstatement that could result from the deficiencies is a material amount and the likelihood of a combination of misstatements occurring is more than low.
Updating the Evaluation of Controls to the Date of the Assertion

The project team will need to update its evaluation of controls from the time of the original evaluation through the end of the company’s fiscal year. The project team should identify changes in the components of internal control through inquiry of the process and/or control owners, observation of procedures, and in many cases, walk-through, inspection, or reperformance of the controls. When the project team determines there have not been significant changes in the controls from the original evaluation date to the end of the company’s fiscal year, the team might limit its procedures to inquiry and observation that the controls continued to function without the need for additional tests of controls. For example, the project team may interview appropriate officers and employees and look for evidence of reassigned duties; changes in key personnel; the introduction of new equipment, procedures, or programs; and other changes that may affect their conclusion about the continued effectiveness of specific controls. If changes are identified, the project team should consider the effect of such changes on its evaluation and whether there is a need for additional tests of controls. For example, if the project team becomes aware of a reduction in staffing causing understaffing, additional tests of controls may be required to determine that the controls continued to function as expected.

Documentation Considerations

The project team’s documentation of controls should provide a basis for the evaluation of controls, including both the design of the internal controls and their operating effectiveness. As to design, the documentation should substantiate that management has established appropriate controls over initiating, recording, processing, and reporting transactions that are effectively designed to prevent or detect material misstatements or omissions. We also recommend the documentation include a description of each significant control, including how the control is performed, who performs the control, what data reports, files, or other materials are used in performing the control, and what physical evidence, if any, is produced as a result of performing the control.

As to operating effectiveness, the SEC final rule requires that management’s documentation should provide reasonable support for the conclusion that the tests were appropriately planned and performed and that the results of the tests were appropriately considered. The documentation should include descriptions of the nature, timing, and extent of the procedures relied upon in evaluating the effectiveness of the controls and should include a list of exceptions (if any), their causes and implications on management’s assertion.

Summarize and Evaluate Control Deficiencies

Having considered the various types of information described above, the project team should accumulate and present its findings so that executive management may perform an overall evaluation of the effectiveness of internal control.

The project team might prepare a summary of control deficiencies to communicate its findings to executive management, the audit committee and the external auditors. The summary should include a description and analysis of each control deficiency or weakness in internal control and summarize all relevant information that was considered. Appendix C provides an illustration of a summary of control deficiencies that the project might use to accumulate and communicate control deficiencies.
Identify Matters for Improvement

Over the course of the evaluation process it is likely the project team will identify areas where controls may require modification or where the project team determines certain systems require control enhancements to respond to new products or emerging risks. The project team also might identify areas where automating manual controls may improve both efficiency and compliance with management’s policies or areas where the team’s evaluation of processes and controls point out redundant controls or other procedures that are no longer necessary. Management should encourage the project team to communicate all suggested enhancements for consideration. The project team and management should consider the concept of reasonable assurance when evaluating whether suggested improvements should be implemented.

Where the project team’s summary of control deficiencies, internal control weaknesses, and suggestions for improving controls indicate that existing controls do not provide reasonable assurance that errors of importance are prevented or detected and corrected in a timely manner, management will need to remediate the current controls or identify and implement alternate controls that provide reasonable assurance. There frequently is more than one course of action that will reduce a particular risk, and management will need to weigh the various alternatives.
Public companies and the business environments in which they operate are dynamic. As such, the system of internal control changes over time, the way controls are applied evolves, and once-effective procedures can become less effective or perhaps are no longer performed. New personnel, inconsistent training and supervision, and time and resource constraints often contribute to changes in controls. Also, circumstances for which aspects of the system of internal control originally were designed may change, causing them to be less able to warn of the risks brought by new conditions. Therefore, to maintain effective internal control, management should monitor the quality and performance of the system of internal control over time to determine whether it continues to be relevant and able to address new risks.

Internal control should be structured to some degree to be self-monitoring and self-correcting. Monitoring can be performed in two ways: through ongoing monitoring activities or separate evaluations.

**Ongoing Monitoring Activities**

Ongoing monitoring entails building monitoring procedures into the normal recurring operating activities of the entity. Ongoing monitoring activities generally are more effective than separate evaluations since they: (1) are ingrained in the entity, (2) are performed on a real-time basis, and (3) react dynamically to changing conditions. While highly ingrained and effective ongoing monitoring activities reduce the need for separate evaluations, most companies nonetheless conduct some separate evaluations of their system of internal control on a recurring basis.

Ongoing monitoring activities include regular management and supervisory activities and other routine actions such as comparisons and reconciliations. Many of these activities are informal and not documented, which normally does not detract from their effectiveness. However, the documentation likely will need to be more substantive when these activities are used to support management’s assertion as to the overall effectiveness of controls. Examples of ongoing monitoring activities might include:

- Management regularly reviews operating reports that are integrated with, or reconciled to, information derived from the financial reporting system, and significant inaccuracies or exceptions to anticipated results of operations are identified and pursued.
- Appropriate attention to organizational structure, supervisory activities, and segregation of incompatible duties provide oversight to control functions and identification of deficiencies.
- Data recorded by information systems are compared to physical assets.
- Appropriate attention is paid to communications from external parties (e.g., customers, vendors, service providers) that either corroborate internally generated information or indicate problems.
Internal auditors or others performing similar review functions regularly monitor the entity’s activities.

Management provides venues (e.g., employee meetings, planning sessions, surveys, fraud “hotlines”) for employees to provide feedback regarding problems and concerns that may indicate control issues.

Personnel are asked periodically to state whether they understand and comply with the entity’s code of conduct.

Appropriate mechanisms to continually monitor the system of internal control and, when necessary, take corrective action in a timely manner help to ensure that the system of internal control is self-correcting.

Generally, one group should not be assigned exclusive responsibility for making the system of internal control self-monitoring and self-correcting. The system of internal control is, in its broadest sense, comprehensive. It involves people throughout the organization, including many who may not think of themselves as having any accounting or control responsibilities. The people involved should include those who establish, issue, and monitor accounting policies and procedures: divisional controllers, internal auditors, the corporate controller, the chief financial officer, other members of senior management, audit committee members, and members of the board of directors. They all need to be concerned, with varying degrees of detail, that the system of internal control is kept “under control.” An important requirement of ensuring this is appropriate lines of communication and adequate feedback, both when the system of internal control is under control and when problems arise.

**Separate Evaluations**

Not to be confused with the annual overall evaluation of internal control over financial reporting required by the Act, separate evaluations of internal control on a periodic basis that focus on the operating effectiveness of controls provide a fresh look and allow management to consider the continued effectiveness of the ongoing monitoring activities. Separate evaluations may take the form of: (1) control self-assessments, where persons responsible for a reporting unit or function determine the effectiveness of controls, (2) special reviews by internal audit or other appropriate groups, and (3) procedures performed by members of management.

Self-assessment programs will likely become more common in light of the need for recurring annual assessments of controls. Also, the real-time nature and efficiency of ongoing monitoring achieved through control self-assessments will support management’s required quarterly certifications under Section 302 of the Sarbanes-Oxley Act. Management will need to determine that these assessment programs focus on the controls that assure achievement of key financial reporting objectives. Similarly, in many cases management will need to supplement these programs with other procedures to provide appropriate evidence to support its assessment of the operating effectiveness of controls.

Separate evaluations of all or portions of the entity’s system of internal control also might take the form of special reviews by internal audit, other appropriate groups, or members of management. The procedures these groups employ to evaluate operating effectiveness should include procedures to understand each of the entity’s activities and the design of the controls. These groups may employ a wide variety of methodologies, techniques, and tools to conduct their separate evaluations including checklists, questionnaires, or benchmarking. Each of the methodologies, techniques, or tools can be effective, providing they are sufficiently sensitive to evaluate the operating effectiveness of the controls subject to evaluation.

The project team should not consider its task completed until either:

- It is satisfied that appropriate ongoing monitoring activities are in place, or
- It has made reasonably specific recommendations for establishing them.

Once all the key recommendations have been implemented, a baseline will have been established to enable management to report on the effectiveness of controls. This does not mean that evaluations will cease. On the contrary, it means that evaluations will have become a part of the company’s ongoing, repetitive processes and thus an important part of the company’s internal control. After implementation of an ongoing monitoring process, the company can expect that any weaknesses—and some will inevitably arise—will be corrected within a reasonable period of time.
Our previous publication, Evaluating Internal Controls—Considerations for Documenting Controls at the Process, Transaction, or Application Level (Ernst & Young SCORE Retrieval File No. EE0692) describes the methodology and steps the project team should follow to document the design of controls identified over specific processes by:

- Determining whether significant risks identified as “what can go wrong” questions are addressed by one or more of the identified controls.
- Determining whether the controls that address the identified risks are adequately designed to prevent or detect material misstatements, whether caused by errors or fraud.
- Walking through the significant controls to determine they have, in fact, been placed in operation.

Walk-throughs are an important preliminary step to designing procedures to evaluate the operating effectiveness of controls. It would be inefficient to perform procedures to test controls that are not adequately designed or have not been placed in operation. Therefore, we recommend the project team perform this important step before investing significant time to design procedures to evaluate the operating effectiveness of controls.

A reviewer in a supervisory capacity (e.g., the division controller or the subsidiary’s treasurer) or a member of the project team should make the determination of whether controls as designed are effective. In making this assessment, the reviewer should consider:

- Account characteristics of related accounts (such as size, susceptibility to error or manipulation).
- The effectiveness of internal control at the entity level.
- Conclusions related to the information technology (IT) processes.
- The design of the control itself.
- The sensitivity of the control.
- Policies and procedures regarding authorization, the safeguarding of assets, asset accountability, and segregation of duties.

Determining whether the controls are designed to achieve a given objective (e.g., that errors of importance are prevented or detected and corrected) often requires considerable judgment. A design deficiency exists when either a necessary control is missing or an existing control is not properly designed so that even when the control is operating as designed the control objective is not always met. The key question is whether the essential controls would be likely to prevent and/or detect a material misstatement relating to each of the relevant financial statement assertions.

To evaluate the design effectiveness of an entity’s internal control, the project team should obtain an understanding of the controls within each component of internal control. The project team generally obtains an understanding of the design of specific controls by making inquiries of appropriate management, supervisory, and staff personnel; by inspecting entity documents; by observing the application of specific controls; by tracing transactions through the information systems relevant to financial reporting, or otherwise walking through the processes and related controls.

Procedures to evaluate the effectiveness of the design of a specific control are concerned with whether the control is suitably designed to prevent or detect and correct errors or material misstatements with respect to specific financial statement assertions. These procedures will vary depending
upon the nature of the specific control and related documentation, and the complexity and sophistication of the company’s operations and systems. Controls may relate to any of the components of internal control.

Some controls may have a pervasive effect on the effectiveness of other controls in assuring that assertions relevant to numerous significant accounts, classes of transactions, or disclosures are achieved. For example, IT general controls over program development, program changes, computer operations, and access to programs and data help assure that specific controls over the processing of transactions are operating effectively. In contrast, other controls are designed to assure that assertions relevant to specific significant accounts, classes of transactions, or disclosures are achieved. For example, management generally establishes specific controls, such as accounting for all shipping documents, to ensure that all valid sales are recorded.

The project team should focus on the significance of a combination of controls in achieving relevant assertions rather than on specific controls in isolation. The absence or inadequacy of a specific control designed to achieve a specific assertion may not be a deficiency, if other controls also address the assertion.

Performing tests to determine whether controls are designed to assure that one or more assertions are achieved may be accomplished by the reviewer making inquiries of the individuals responsible for each control and examining evidence that the control was performed and was effective (e.g., reviewing bank reconciliations), or by the reviewer retracing a transaction and/or reperforming controls (e.g., recalculating extensions on a sample of invoices). In other instances, assurance that controls are functioning as intended may be gained by observing employees as they perform their work, and through interviews to determine how employees understand what is required in the event an error is identified in the performance of their duties.

In instances where transactions are processed by the IT system, in addition to following the physical flow of documents and forms, the reviewer also follows the flow of data and file information through the automated process in the application (at a system level, not a detailed logic level). This may involve procedures such as inquiry of independent and knowledgeable personnel (e.g., IT, process owner), review of user manuals, observation of a user processing transactions at a terminal in the case of an online application, and review of documentation such as output reports.

At the conclusion of this task, the reviewer should document whether the manual and programmed controls are effectively designed, and include any other pertinent comments that might assist the project team.
Tests of Programmed Controls
Companies often rely on programmed controls to prevent or detect errors in automated applications. Programmed controls are usually either programmed control procedures (e.g., edits, matching, reconciliation routines) or computer processes (e.g., calculations, on-line entries, automated interfaces between systems).

For example, in a simple application, controls over the pricing of shipments may include the user’s review of sales invoices to determine whether the correct prices and discounts are used and whether extensions were performed correctly. In a more complex application, however, a company may rely on a computerized edit routine to identify prices and discounts that do not meet established criteria.

When a company relies on programmed controls, the project team will need to test the functioning of the programmed controls just as it would manual controls. For example, testing a programmed edit control might include determining whether the transactions exceeding the established edit limits are appropriately identified and reported, inquiring of the employee responsible for the manual follow-up procedures that support the programmed control, and reviewing the actual follow-up procedures performed. Many times, particularly in more complex environments, an individual with experience in auditing IT will need to perform, or assist the project team in performing, tests of programmed controls.

By recognizing that programmed controls operate in a systematic manner, a project team may be able to limit the extent of its testing of such controls. For example, a computerized interest calculation may always use the same formula (principal multiplied by an interest rate from a rate master file or table) or a computerized edit check may disallow further processing of checks over $100,000.

The project team performs tests to obtain evidence that the programmed controls operated effectively as documented by one or more of the following:

- Testing IT general controls that ensure that any changes to the program performing the calculations are authorized, tested, and approved before such changes are placed in operation (i.e., program change controls) and that access to data files is appropriately controlled (i.e., access controls). Testing these controls is most effective and efficient when they support management’s reliance on several programmed controls.

- Program change controls:
  - Observing and/or reviewing a sample of significant projects (e.g., those affecting the information that support the processes that are important to management’s assertion on internal control) to determine:
    - Acceptance testing is routinely performed.
    - Environments for development (or modification) and testing of IT solutions are separated from production systems.
    - Development personnel are prohibited from migrating applications and data from the test environment to production.
  - Reviewing or conducting a user satisfaction survey to determine how well users’ information technology needs are being met. Alternatively, the project team can discuss with end users how well their information needs are being fulfilled by the information technology organization.
  - Attending or reviewing minutes of the Information Technology Steering Committee’s meetings (or the equivalent) where the priorities for information technology projects are discussed.
— Attending project design meetings (or holding discussions with users) to understand how users’ needs are translated into information technology project specifications.

Access controls

— Reviewing the process for administering access to information systems and obtaining evidence to determine that appropriate authorizations are obtained for users who are granted access to these systems.

— Determining whether the access control software options are in effect by reviewing appropriate systems reports, and considering whether the options are appropriate.

— Reviewing the system log reports and access violation reports with the process owner, inquiring about the scope of his/her review, and determining whether there is appropriate follow-up.

— Testing the operation of the programmed controls. For example, the project team may choose to select a sample of invoices and compare the prices to the approved price sheet. Alternatively, the project team may be able to use audit software to test the operations of those programmed controls. Another example might be transaction transmission controls over sales orders from individual customers via the Internet or another network. The project team might determine the relevant control features through discussions with the network manager and web developers, observe the transmission controls through a demonstration and review the related reports or logs, and evaluate the authentication (security) features and procedures.

Testing manual controls that support the programmed control. For example, the computer program prices invoices using data on the price master file and produces a listing of sales orders, invoices, part numbers, and unit prices. The company has a manual control to review and approve the list. Note, however, the project team should obtain evidence that the control operated effectively.

Performing benchmarking procedures (addressed in more detail in the following section).

Benchmarking Programmed Controls

Benchmarking programmed controls is a testing strategy that may be used to extend the benefits of certain tests of programmed controls into subsequent periods. It may also enable a project team to reduce or eliminate certain testing in subsequent years. Benchmarking programmed controls is based on the premise that a computer will continue to perform a given procedure (e.g., aging of accounts receivable, edit test) in exactly the same way until the program is changed. If a project team verifies that a particular program executing a process or programmed control has not changed, since the project team last tested it, they may choose to not repeat the specified test(s) in subsequent years.

A project team can establish its programmed controls benchmark, as of a point in time by performing a test of programmed controls using traditional testing procedures (e.g., total and extend inventory listings either manually or using another computer program). Then at an appropriate subsequent time, rather than repeating the traditional testing procedures, the project team’s IT specialist along with other appropriate project team members can determine that the program has not been modified since the project team last tested the programmed control.

Obtaining reasonable assurance that the program did not change could involve discussions with individuals from the IT and end user departments and review of appropriate reliable reports (such as a listing detailing the compilation dates of all programs placed in production), and then briefly documenting any conclusions. An IT specialist may be used to help obtain these assurances. In the case of a more complex system, obtaining reasonable assurance also could involve testing IT general controls (as discussed in prior section). The length of time a project team can rely on a benchmark will vary, and will depend on the level of assurance they can obtain that significant program changes would be identified. Programmed control benchmarking procedures do not extend to the accuracy of the underlying data input into the application. The project team will need to test the underlying data or the applicable controls to be satisfied that the data is accurate.
Benchmarking programmed controls is usually appropriate when:

- A programmed control can be matched to a defined program within an application. For example, the project team may be able to benchmark programmed controls for the specific program that performs the invoice extension calculation or aging computation. However, except in the case of simple, pre-packaged software, it is unlikely that a project team could benchmark programmed controls for all processing procedures or programmed controls performed by the sales or accounts receivable application.

- The application is stable (i.e., few changes from year to year).

- A report of the compilation dates of all programs placed in production is available and is reliable.

Benchmarking programmed controls can be especially effective when a company uses purchased software where the possibility of program changes is remote (e.g., when the software does not allow access to the source code or the client does not have the capability to make changes). When purchased software is integrated with other applications, the project team should also consider user access to the applications and the adequacy of segregation of duties when determining the opportunity to benchmark.

The project team may need to reestablish (i.e., reperform the testing) the benchmarks for programmed controls at future intervals. Factors the team will need to consider in determining when to reestablish a benchmark include: the effectiveness of the information technology environment, including the controls over application and system software acquisition and maintenance; the project team’s understanding of changes, if any, to the specific programs, and the nature and timing of the related tests; and the consequences of errors associated with the programmed control that was benchmarked.
## Appendix C—Summary of Control Deficiencies

<table>
<thead>
<tr>
<th>Application/Process</th>
<th>Description of Deficiency</th>
<th>Working Paper Reference</th>
<th>Management’s Response</th>
<th>Is Deficiency a Significant Deficiency?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>