# Table of Contents

**Introduction** ...........................................................................................................................................  1

**Overall IT Risk and Control Approach and Considerations When Complying with Sarbanes-Oxley**  ....  2
  1. Is there an overall approach to IT risk and control consideration that should be followed? .................  2
  2. Why is it so important to consider IT when evaluating internal control over financial reporting? ..........  4
  3. How should Section 404 compliance teams define “IT risks and controls”? ..............................................  5
  4. How does management identify and prioritize IT risks? .............................................................................  5
  5. What guidance does COSO provide with respect to IT controls? ..............................................................  6
  6. What guidance is provided by the Information Systems Audit and Control Association's (ISACA) Control Objectives for Information and Related Technologies (COBIT) framework with respect to IT controls? ........................................................................  6
  7. How do COSO and COBIT facilitate a Section 404 compliance effort? ......................................................  6
  8. If a Section 404 project strictly and only follows COBIT, will the project be compliant with the Section 404 compliance efforts? .................................................................................................  7
  9. Should management consider other IT control guidelines and standards, such as ISO/IEC 27000 series, ITIL and CMM? .........................................................................................................................  7
  10. If my company is compliant with Payment Card Industry (PCI) standards, are we compliant with IT SOX controls? ....................................................................................................................................... 7
  11. Is it possible to rely solely on manual controls, negating the need to evaluate IT risks and controls? .............................................................................................................................................  7
  12. Overall, what are the key areas that must be considered when evaluating IT risks? .................................  8
  13. How does management get started using the approach outlined in Question 1? .......................................  9
  14. When should IT controls be considered during the overall Section 404 project? ........................................  9
  15. How does an ERP solution impact the evaluation of IT? ...........................................................................  9
  16. How does a shared-service center impact the assessment of internal control? ........................................... 10
  17. How does outsourcing (e.g., software as a service, data center services) of technology and IT activities impact a company’s control evaluation approach? ........................................................................ 10
  18. How does utilizing a software as a service (SaaS) application impact a company’s application control evaluation approach? ......................................................................................................... 12
  19. What are the different types of SSAE 16 reports, and how do they replace SAS 70 reports? ................. 12
  20. Do we need to address controls for business units that are outside the United States? ......................... 12

**Entity-Level Considerations** ........................................................................................................ 13
  21. What is the IT organization? ....................................................................................................................... 13
  22. How does management consider the entity-level issues around IT risks and controls? ........................... 13
  23. Are there separate “entities” that include just IT operations or processes? ........................................... 14
24. What IT governance issues should be considered for purposes of complying with Sections 404 and 302 of Sarbanes-Oxley? ................................................................. 14
25. What difference does it make if management has strong entity-level IT-related controls? ................................ 14
26. How would management know if the entity-level controls provide a strong control environment? .......... 14
27. What difference does it make if management has weak entity-level controls? ............................................. 15
28. What are examples of a weak entity-level control environment? .............................................................. 15

Activity/Process-Level Considerations – General Control Issues .............................................................. 16
29. What are “general IT controls”? ................................................................................................................ 16
30. What types of controls are “general IT controls”? ...................................................................................... 16
31. What technology stack layers (e.g., application, database management systems, operating systems) are required to be in scope for Section 404? ....................................................... 17
32. What does the Section 404 compliance project team look for when evaluating security administration? ........................................................................................................ 17
33. What does the Section 404 compliance project team look for when evaluating application change controls? ........................................................................................................... 19
34. What does the Section 404 compliance project team look for when evaluating data backup and recovery? .................................................................................................................. 20
35. What systems development life cycle (SDLC) controls should be considered for technology implementation projects or significant system upgrades? ................................................................. 21
36. We outsource our financial applications; do we need to do anything to be SOX compliant? ....................... 21
37. Do we have to hire more IT resources to mitigate risks related to segregation of duties issues? .............. 21

Activity/Process-Level Considerations – The Role of Application and Data-Owner Processes ........ 22
38. Who are the application and data owners? .................................................................................................... 22
39. What are the roles and responsibilities of the application and data owners in relation to the IT organization? .................................................................................................................. 22
40. What processes should the application and data owners have in place to facilitate compliance with Sections 404 and 302? ...................................................................................................... 23
41. What processes should be in place with respect to establishing proper security and segregation of duties? .................................................................................................................. 23
42. What processes should be in place with respect to periodic review and approval of access to critical and/or sensitive transactions and data? ........................................................................ 23
43. What processes should be in place from an internal control standpoint with respect to the application change management around initiating, testing and approving changes before making production application changes? ............................................................... 23
44. If application and data-owner process controls are designed and operating effectively, what is the impact on the evaluation of internal control over financial reporting? ........................................ 24
45. If application and data-owner process controls are not designed and operating effectively, what is the impact on the evaluation of internal control over financial reporting? ................ 24
Activity/Process-Level Considerations – Application-Level Controls .................................................. 25

46. What are the application-level control considerations? ...................................................................... 25

47. How is an appropriate application baseline established? ..................................................................... 25

48. How does the Section 404 compliance team determine the critical applications for each key business process? ................................................................................................................. 27

49. How should the Section 404 compliance team integrate the consideration of application-level controls with business-process controls at the activity/process level? ......................................................... 27

50. What should management do if the Section 404 compliance team finds strong application controls at the business-process level? .................................................................................................. 28

51. What should management do if the Section 404 compliance team finds weak application controls at the business-process level? .................................................................................................. 29

52. How can an organization decrease its reliance on spreadsheets? ......................................................... 29

53. What are some application control considerations for the order-to-cash cycle? ................................ 29

54. What are some application control considerations for the procure-to-pay cycle? .............................. 30

55. What are some application control considerations for the close-the-books/financial-reporting cycle? .................................................................................................................................. 30

Documentation .................................................................................................................................... 31

56. How much documentation should the IT organization and the application and data owners have in place to evidence the controls and functioning of the applications? .......................................................... 31

57. How should the Section 404 compliance team document the IT controls at the entity level? .............. 31

58. How should the Section 404 compliance team document the IT controls for the IT general controls at the activity/process level? .............................................................................................. 32

59. How should the Section 404 compliance team document the IT controls for the processes controlled by application and data owners and for the specific application areas? .......................... 32

Testing ................................................................................................................................................ 33

60. How are IT controls tested? .................................................................................................................. 33

Addressing Deficiencies and Reporting ................................................................................................ 34

61. How should management address deficiencies and gaps in IT controls? ........................................... 34

62. How will the external auditor view IT controls during the attestation process? ................................. 34

About Protiviti Inc. .................................................................................................................................. 36
Introduction

Protiviti has published a series of resource guides that address questions about Section 404 of the Sarbanes-Oxley Act (“SOX” or “Sarbanes-Oxley”). These guides have been updated over time to reflect the U.S. Securities and Exchange Commission’s (SEC) final rules and guidance as well as changes in practice.

Guide to the Sarbanes-Oxley Act: IT Risks and Controls (Second Edition) is a companion to Protiviti’s Section 404 publication, Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements (Fourth Edition). Our IT risks and controls guide presumes that the reader understands the fundamental requirements of Section 404 compliance and internal control evaluation and reporting, as detailed in Protiviti’s Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirement (Fourth Edition).1

Guide to the Sarbanes-Oxley Act: IT Risks and Controls (Second Edition) provides guidance to Section 404 compliance project teams on the consideration of information technology (IT) risks and controls at both the entity and activity levels within an organization. Questions and answers in the book focus on the interaction between the IT organization and the entity’s application and data-process owners, and explain the implications of general IT controls and how they are considered at the process level. This guide also explores how application-control assessments are integrated with the assessment of business-process controls, and addresses documentation, testing and remediation matters.

The questions listed in this publication are ones that have arisen in our discussions with clients and others in the marketplace who are dealing with these requirements. The responses and points of view are based on our experience assisting companies as they document, evaluate and improve their internal control over financial reporting, and as they continue to improve their executive certification process.

This publication is not intended to be a legal analysis in terms of the suitability of approaches in complying with the requirements of Sarbanes-Oxley. Companies should seek legal counsel and appropriate risk advisers for advice on specific questions as they relate to their unique circumstances. Company approaches may be impacted by standards for attestation engagements that will be issued by the Public Company Accounting Oversight Board (PCAOB). Accordingly, a number of the issues addressed in this publication will continue to evolve and warrant dialogue with the external auditor.

Protiviti
November 2012

Overall IT Risk and Control Approach and Considerations When Complying with Sarbanes-Oxley

The impact of IT must be carefully considered in an evaluation of internal control over financial reporting. There are unique risks to be considered. Our responses to the following questions address some of the overall considerations, including the importance of considering IT when evaluating internal control over financial reporting, the definition and identification of “IT risks and controls,” and the use of frameworks to facilitate the evaluation of IT risks and controls. Section 404 compliance teams should take into account these considerations early when planning and organizing the project.

1. Is there an overall approach to IT risk and control consideration that should be followed?

The obvious answer is “yes.” The rationale, a definition of key terms, and each element of our suggested approach will be discussed in detail in the pages that follow. However, we have outlined the overall approach below in order to present the context and “end game” for the IT risk and control evaluations.

The overall approach can be depicted as follows:
The IT approach should be performed in the illustrated sequence because each step impacts the scoping and, in some instances, the nature of the work to be performed in subsequent steps. To illustrate, the initial step of understanding the “IT organization and structure” sets the foundation for the IT entity-level control evaluations. Subsequently, the strengths and weaknesses of the entity-level controls will impact the nature, extent and timing of the IT process-level control evaluations for each of the three levels evaluated.

The IT process-level control evaluations are, by far, where the most time and effort will be incurred for compliance projects. The IT process-level evaluations are made up of three distinct sets of processes that must be considered.

These processes are sequenced in the order by which they should be evaluated. Following is a brief discussion of each of these areas:

**General IT Process Controls**

The review of general IT controls addresses the critical IT processes within each entity or for each key location that supports key financial reporting-related applications. Note that the Section 404 compliance project team may need to review the same general IT controls area more than once in certain circumstances. For example, if there are multiple processes impacting each priority financial-reporting area that are not subject to similar policies, process activities and control procedures, these multiple processes may need to be separately reviewed.

The general IT processes we believe would be evaluated in almost every instance are:

- Security administration
- Application change control
- Data backup and recovery
- Systems development life cycle (SDLC)
Application and Data-Owner Controls

The processes evaluated in this section are those that should be controlled and owned directly by the application and data owners. We believe the processes that should be evaluated for this portion of the project in almost every instance are:

- Establish and maintain segregation of incompatible duties (security roles and administration).
- Assess and implement controls over end-user computing (e.g., spreadsheets, user-developed databases) and critical reports.
- Confirm/review access to critical transactions and data.
- Develop and maintain business owner change control.

Configurable Application Controls

It is essential to evaluate, on an integrated basis, all IT and manual controls at the business-process level. The IT-related portion of this assessment focuses on controls within key applications, which typically support the key processes impacting the significant financial-reporting elements. Accordingly, it is important to integrate this IT risk and control evaluation with the business-process evaluation so that a holistic understanding of the control environment is achieved. Otherwise, the assessment of IT controls becomes a mere appendage, resulting in an inadequate understanding of the process and the underlying risks. Business risks include all risks in a process, whether they are people-based or systems-based.

The following application control areas should be understood for each critical financial application within the critical business processes:

- Automated process controls
- Manual process controls
- End-user computing (EUC) controls
- Reporting controls
- Application security controls
- General IT controls

In summary, a top-down approach is applied to IT risks and controls just as it is applied to other areas of the Section 404 compliance process. Each of the above areas will be discussed in more detail in the following sections.

2. Why is it so important to consider IT when evaluating internal control over financial reporting?

Business processes continue to become more and more dependent on technology embedded within them for timely, comprehensive and accurate execution. The financial-reporting process as well as processes that accept, record, accumulate, summarize and report the transactions underlying financial reporting in most, if not all, companies, are accomplished with computers, programs, and other technology-related equipment and software. Therefore, the effectiveness of the controls around the applications and systems directly impacts the integrity of processing, including the data that is input into processing and the information that is ultimately reported (i.e., the output) upon completion of processing.

Applications and systems have controls programmed into them. Some of these programmed controls may be critical to the evaluation of internal control over financial reporting. If these programmed controls are critical, they must be considered during the evaluation, particularly if management relies on them with limited or no user verification of the results of processing.

IT also introduces risks unique to the IT environment. Individuals develop, maintain and have access to hardware, software and other components of the technology environment. Unauthorized actions of these individuals can directly impact the integrity of the processing and data. Therefore, relevant risks arise from technology that must be considered when evaluating internal control over financial reporting. These risks are inherent in the use...
of technology. For example, unauthorized access to information and data, inaccurate calculations and processing, and unauthorized or flawed changes to programs can introduce errors or cause incomplete processing. These risks must be addressed and considered during an assessment of the internal control structure.

In short, in today’s highly computerized business environment, IT-related risks and controls must be considered in any overall evaluation of internal control over financial reporting (which is required by Section 404 of Sarbanes-Oxley).

3. How should Section 404 compliance teams define “IT risks and controls”?

“IT risks and controls” include risks and controls that either (a) exist through technology (programmed controls within applications, for example), or (b) impact the integrity of processing or data. Compliance project teams should consider these risks and controls in the Section 404 compliance process. In addition, the IT risks and controls considered for Section 404 compliance efforts are limited to those related to the achievement of internal control objectives germane to the reliability of financial reporting.

For purposes of our discussion in this guide, “IT risks and controls” relate primarily to broad areas – general IT controls and application controls.

General IT controls typically impact a number of individual applications and data in the technology environment. As a general rule, these controls impact the achievement of those financial statement assertions germane to critical processes by supporting an environment that provides for the integrity of processing and data affecting those processes. In other words, general IT controls reduce the risk of certain events impacting the integrity of processing or data to an acceptable level. (The impact to which we are referring is discussed later in this guide.)

With respect to application controls, there are two areas of importance:

a) The controls and processes that are designed and implemented in the business areas by the respective application and data owners

b) The programmed or configurable controls within the applications that perform specific control-related activities, such as error checking or validation of key fields

An example of application controls is segregation of incompatible duties. The data owners are responsible for designing and logically determining the responsibilities and duties that should be segregated. The applications programming group is responsible for designing and developing the application in such a way as to provide reasonable assurance that transactions are executed through programmed and other controls in accordance with the application owner’s design, which addresses the financial-reporting assertions.

4. How does management identify and prioritize IT risks?

The framework and approach for identifying and prioritizing IT risks should be the same overall framework and approach as used for identifying and prioritizing any and all risks that affect the critical processes impacting the priority financial-reporting elements. Generally, risks are identified in terms of their relevance to the specific financial statement assertions that form the basis for reaching an overall conclusion on the internal control environment. Risks are prioritized in terms of their significance to financial reporting and likelihood of occurrence.

This approach is consistent with the SEC’s Interpretive Guidance and PCAOB’s Auditing Standard No. 5, both of which highlight the use of a top-down, risk-based approach to evaluating the effectiveness of internal control over financial reporting.

Use of the same overall framework and approach is an important distinction when addressing IT risks. Financial statement assertions are the same, regardless of the nature of the risk impacting internal control over financial reporting. These assertions include generic objectives related to authorization, completeness and accuracy, and access to assets. Stated in terms specific to IT, control objectives relate to the integrity of processing and data (to achieve the objectives relating to completeness, accuracy, consistency and timeliness of financial reporting), and to the proper access to data programs and specific transactions (which supports achievement of the authorization and
access to assets objectives). Developing an understanding of how these technology areas impact (or could possibly impact), either directly or indirectly, achievement of financial-reporting assertions helps to focus the risk and control evaluations that need to be performed in the general and application controls areas.

5. What guidance does COSO provide with respect to IT controls?

The COSO Internal Controls – Integrated Framework discusses IT controls in the same context that it does in referring to controls that are dependent on people. That context is the five components of internal control that must be in place at both the entity and activity levels of an organization to achieve management’s objective, which in the case of Section 404 compliance is reliable financial reporting. The five components are: control environment, risk assessment, control activities, information/communication, and monitoring. When evaluating the effectiveness of IT controls at both the entity level and activity level, these five components provide the criteria that would be considered.

COSO takes the position that technology general controls “must be implemented and operating for automated controls to work properly when first developed and implemented.” In addition, “technology general controls also enable information systems to function properly after they are initially developed and implemented.”

At the application level, COSO asserts that control activities and technology relate to each other in several ways. To illustrate, technology can support business processes. In addition, many control activities in an entity are partially or wholly automated using technology. Automated controls are generally more applicable to financial reporting. For example, a three-way match performed within an enterprise resource planning (ERP) system supporting the procurement and payables subprocesses is an automated control. COSO acknowledges that (a) most business processes have a mix of manual and automated controls, depending on the availability of technology in the entity, and (b) provided the technology general controls are implemented and operating effectively, automated controls tend to be more reliable than manual controls because they are less susceptible to human judgment and error.

6. What guidance is provided by the Information Systems Audit and Control Association’s (ISACA) Control Objectives for Information and Related Technologies (COBIT) framework with respect to IT controls?

There are several frameworks available that are specifically designed for use with IT-related controls. One of the most widely known is the COBIT framework that is published by the IT Governance Institute and ISACA. COBIT is an IT governance framework that provides governance (entity-level) and detailed (activity-level) objectives. It also provides a comprehensive overview and overall understanding of the IT environment. Accordingly, it may be referenced and considered as part of the work on IT risks and controls.

The most recent issuance of COBIT is COBIT 5. The newest version of COBIT builds on previous versions of COBIT as well as Val IT and Risk IT. In general, the COBIT framework is composed of the IT processes that make up a large part of the “general IT controls” areas, and provides control objectives, risks and example controls. The use of this framework (or any other) on a Section 404 compliance project should focus specifically on meeting the objectives of internal control over financial reporting. In other words, the Section 404 approach must focus primarily on the achievement of the assertions that are inherent in reliable financial reporting.

7. How do COSO and COBIT facilitate a Section 404 compliance effort?

COSO provides an overall framework that, for Section 404 purposes, provides for the achievement of effective internal control over financial reporting. The COBIT framework provides overall guidance on the achievement of the broader spectrum of internal control surrounding certain aspects of the IT control environment. COSO should be considered in the execution of a Section 404 compliance project because the SEC specifically references it in the final Section 404 rules as a “suitable framework.” COBIT also provides useful guidance and background material, and may be considered in the execution of a Section 404 compliance project.
8. If a Section 404 project strictly and only follows COBIT, will the project be compliant with the Section 404 compliance efforts?

As discussed in Question 6, COBIT is a comprehensive controls framework that considers the achievement of more than just the objectives related to internal control over financial reporting. To fully document the technology controls using COBIT would create documentation far in excess of what is required of a Section 404 compliance project. If a complete COBIT documentation effort is undertaken, a filtering and linking effort is necessary to determine the controls management must rely upon for financial-reporting purposes. This would also be needed to develop the appropriate testing plan for determining operating effectiveness. A compliance team will also need to address the application-level controls related to specific applications discussed in Questions 46-55 in order to comply fully with the Section 404 compliance efforts.

9. Should management consider other IT control guidelines and standards, such as ISO/IEC 27000 series, ITIL and CMM?

In addition to COBIT, there are a number of frameworks and materials that provide guidance on IT risk and controls. Each of these frameworks offers specific guidance aimed at assisting organizations in “improving” their IT operations and processes. In addition, each framework provides excellent examples of how processes could be organized, as well as best practices for designing and operating processes in the IT organization. If an entity’s IT organization already uses one or more of these frameworks in documenting its operations, then it would be logical to use that framework as a basis to begin Section 404 compliance-related work. However, risks and controls should be evaluated in the context of the financial reporting internal control objectives or assertions that are discussed in Question 4.

Compliance with any of the frameworks must be evaluated as it relates to achievement of the internal control objectives for financial reporting. A compliance effort using other frameworks does not guarantee the sufficiency of nor supplant the need for an evaluation that considers assertions germane to effective internal control over financial reporting.

10. If my company is compliant with Payment Card Industry (PCI) standards, are we compliant with IT SOX controls?

The PCI framework is typically only associated with an organization’s payment systems. As a result, most companies would not be compliant with SOX because their financial-reporting systems are not included in the PCI scope.

11. Is it possible to rely solely on manual controls, negating the need to evaluate IT risks and controls?

Not if your company has any accounting systems. The PCAOB's Auditing Standard No. 5 references the system and automated controls. For example, with respect to obtaining an understanding of internal control over financial reporting, the PCAOB provides a number of procedures for auditors to follow. One such procedure is gaining an understanding of the design of specific controls by following a transaction from origination through the company’s processes, including the applicable information systems, until it is reflected in the company’s financial records. The PCAOB also states elsewhere that the auditor must “understand the flow of transactions, related to relevant assertions, including how transactions are initiated, recorded, processed and reported.” The fundamental premise here is that information systems are important to financial-reporting processes; accordingly, management must fully understand the applications that impact financial reporting, the related risks and the controls mitigating those risks before the company’s auditors commence the audit process.
12. Overall, what are the key areas that must be considered when evaluating IT controls?

In the IT area, just as in the overall control areas, the places to begin are corporate and IT governance. First, there is overall corporate governance. This is the “tone at the top” as defined by the words and actions of the CEO, the board of directors and the executive team.

With respect to IT governance, there are two areas that must be addressed, both of which affect how an evaluation of IT controls impacts internal control related to financial reporting. These are depicted as follows:

The IT organization consists of IT operations and the overall governance of the processes impacting IT. IT typically consists of the CIO’s organization and impacts the effectiveness of the general or pervasive controls. (The impact of the IT organization and general IT controls is discussed in Questions 21 through 37.)

The application and data owners are the business groups interfacing with business-process owners. The effectiveness of the application and data-process controls significantly impacts the effectiveness of controls at the activity or process level. (The impact of the application and data-process controls is discussed in Questions 38 through 45.)

**IT Control Considerations in Relation to Business-Process Controls**

Since technology today is integrated more than ever into business processes, technology-specific controls, i.e., those embedded and designed into the applications that support the processes, must be considered when evaluating controls at the process or activity level. In most cases, there is significant reliance on those controls at the activity/process level to mitigate risks and to achieve relevant objectives related to internal control over financial reporting.

Our responses to the questions in this section are intended to assist Section 404 compliance teams in integrating the consideration of IT with the assessment of internal control over financial reporting. Ultimately, this integration must take place at the process level. Questions 13 through 17 address getting started with the evaluation.
of IT risks and controls, the matter of timing the consideration of IT risks and controls, the evaluation of ERP systems, and the impact of a shared-service center and outsourcing of IT activities on the evaluation.

13. How does management get started using the approach outlined in Question 1?

The approach outlined in our response to Question 1 provides management with the overall framework to begin its IT risk and controls evaluation within the context of the Section 404 compliance process. This approach is based on management’s overall identification and prioritization of both the financial-reporting elements and the critical business processes that directly relate to those elements. This identification and prioritization process is an integral part of each Section 404 compliance project, and it is also the logical starting point for the consideration of IT risks and controls. It is within this context that the suggested approach, as outlined in our response to Question 1, presents a practical way to begin considering IT risks and controls, regardless of the controls framework used by the company. The project team should start with the premise that IT risks and controls at both the general control and application control levels are critical to the evaluation of internal control over financial reporting. The risk-based approach is similar to the approach outlined by the Guide to the Assessment of IT Risk (GAIT) published by The Institute of Internal Auditors (IIA). GAIT provides a set of principles that can assist management in determining the technology assets and controls in-scope to meet Section 404 objectives.

To illustrate the logical progression of IT controls-related evaluations, the project team should first document the key applications related to the critical business processes that have been linked to the priority financial-reporting elements. From that point, the project team can undertake the process of identifying the related technology components and general IT controls (see Question 29) that provide assurance of processing and data integrity for the key applications. Once those components and general IT controls are identified, the associated documentation and evaluation work is linked to the associated business processes (as well as to the related applications).

14. When should IT controls be considered during the overall Section 404 project?

As discussed in Question 13, the identification of in-scope technology systems is based on management’s overall identification and prioritization of both the financial-reporting elements and the critical business processes that directly relate to those elements. The IT controls should be considered for the systems that support critical business processes after the prioritization process is completed. It is critical that the IT control evaluation be done as early as possible after the prioritization process because the Section 404 compliance project team must understand the strengths and weaknesses of the IT entity-level controls and the general IT controls at the activity/process level as it scopes and plans the evaluation of controls over business processes.

The nature of the strengths and weaknesses in the entity and general IT controls will determine the extent to which application and business-process controls must be documented and evaluated in order to reach an appropriate conclusion on the effectiveness of internal control over financial reporting at the business-process level. For example, weaknesses in IT general controls and application controls would require increased emphasis on documenting and evaluating additional detective (or supervisory or monitoring) controls at the business-process level. In some cases, weaknesses in IT general controls can result in a material weakness in internal control that is so pervasive, it is difficult to compensate at the application level for the deficiency. However, if strong preventive IT controls over access to assets exist at the general control level, then the need for the additional detective and monitoring controls at the business-process level would not be necessary.

15. How does an ERP solution impact the evaluation of IT?

An ERP system that is utilized across an entity potentially provides many advantages to the IT risk and control considerations for Section 404 compliance efforts. If there is a single worldwide implementation, there is uniformity to many of the general and application controls that impact the financial applications. However, caution should be exercised to understand how the organization has installed its ERP solution. For many organizations, there is more than a single “instance” (an installation) of the ERP system. Often, ERP applications are configured
and operated differently for various business units or geographic areas. If there are several individual installations, each would have to be evaluated and documented as part of the Section 404 compliance effort.

Another advantage related to ERP applications is that they are widely used, leading to potentially significant efficiencies. The control features and functions of the major ERP applications are understood by a number of application specialists. Depending on the nature of the entity's application, these specialists likely will understand the particular configurations deployed across the organization and quickly determine if the optimum control options are being utilized. If not, they can make the appropriate recommendations to management. By contrast, if there are custom applications or highly customized ERP systems, the understanding, documentation and evaluation of the design of programmed (computerized) controls must be accomplished for each application or system.

16. How does a shared-service center impact the assessment of internal control?

A shared-service environment has some of the characteristics discussed in Question 15 related to ERP applications. For shared services, certain processes and procedures are similar across the enterprise, with the related impacts on its risks and controls. For the general IT processes discussed in Questions 29 through 37, the more these processes are managed within a shared-service environment, the less overall time and effort will be incurred with respect to evaluating IT processes. For example, if an enterprise has a shared-service center that handles, through a common process, all changes to application programs, then the evaluation of the application-change process can be done just once. Thus the findings and the evaluation can be considered for all applications under the shared process. By contrast, in a situation where the change-control process is unique to each application or group of applications, this process would need to be evaluated for each significant application or group of applications.

17. How does outsourcing (e.g., software as a service, data center services) of technology and IT activities impact a company’s control evaluation approach?

When transaction processing is outsourced, management still must assess controls over processing that are significant to the company’s accounting systems and controls. The SEC’s Interpretive Guidance states that when management outsources a significant process to a service organization, it must determine that evidence of the operating effectiveness of the controls over that process is necessary. The Commission notes that its disclosure requirements do not permit management to issue a report on internal control over financial reporting with a scope limitation. In essence, IT and other control issues exist regardless of whether transaction processing takes place internally or externally. Under the provisions of Section 404 of Sarbanes-Oxley, management must evaluate the controls over the process activities and applications that are critical to the company’s internal control over financial reporting. This evaluation must be directed to processes and applications that the company operates, and to processes and applications that the company outsources to external service providers. The PCAOB has also reinforced this point of view.

When an organization considers internal controls relative to outsourced processes and systems, reviewing the outsourcing agreement is a critical first step. The agreement ideally will describe the responsibilities of each party related to key aspects of the process and the application’s operations and maintenance (e.g., security administration, change management, data management and ownership rights). It also should define service-level agreements, which also may address some of the control aspects that need to be understood. The contract is the only real control document in an outsourcing relationship as it outlines “who is responsible for what.”

The evaluation of internal controls resident in business processes should consider the controls needed to achieve the financial statement assertion objectives, which are likely to require appropriate controls residing at the service organization (outsourcer). During a Section 404 compliance project, these controls must be evaluated and tested like any other controls for a process or an application managed and controlled directly by the company. Both the SEC and PCAOB have made it clear that the use of a service organization does not reduce management’s responsibility to maintain effective internal control over financial reporting. Organizations may accomplish this evaluation and testing either (1) through a third-party assurance report, in accordance with a Statement on Standards for Attestation Engagements (SSAE) 16 report (formerly known as a SAS 70 report), provided by the outsourcer (assuming the issues noted below are addressed), or (2) by having independent testing performed by the company's
designee (e.g., internal audit, outside consultant). There are various types of SSAE 16 reports that can be issued by a service organization. Refer to Question 19 for descriptions of the SSAE 16 reports.

When deciding on the approach for pursuing this evaluation effort, here are a few thoughts to consider:

- The contents of an SSAE 16 Service Organization Controls (SOC) 1 report are reviewed in relation to controls at the user organization. Therefore, the user organization should develop a process map that documents input controls, the processing that is done at the service organization, and the expected outputs and output controls. In addition, the user would also map key master file maintenance processes and user organization security administration procedures for the application because, typically, the key controls over authorization and segregation of duties are internal to and under the control of the user organization.

- In the past, third-party assurance reports have been written and scoped for the purpose of communication between the independent auditor for the service organization and the user company's external auditor for his or her use in conjunction with the audit of the user organization's financial statements. Section 404 has changed the dynamics of these requirements by assigning management the responsibility to make an assertion with respect to the entity's internal control over financial reporting. Thus management likely will need an SSAE 16 SOC 1 type report from the service organization's auditors. The alternative is for management to test the service organization's controls independently, which may not be a practical option.

If an SSAE 16 report is to be used by management, there are several considerations to keep in mind:

- First, if the outsourcing service agreement doesn’t spell out the SSAE 16 SOC 1 report requirements, management should consult with legal counsel to review the legal aspects of their reliance on the letter. It is desirable that the outsourcing agreement be appropriately modified to articulate the SSAE 16 SOC 1 report requirements, so the letter and the reporting relationship can be conformed to satisfy those requirements.

- Second, the scope of the SSAE 16 SOC 1 review needs to be evaluated carefully. Prior periods' scope to satisfy the auditors for purposes of expressing an opinion on the financial statements may need to be expanded, perhaps significantly, to satisfy the additional requirements of management to obtain sufficient evidence supporting a conclusion on the effectiveness of internal control over financial reporting. For example, the SSAE 16 SOC 1 report must address relevant financial-reporting assertions and focus on both design and operating effectiveness. Again, this is an area for which management is clearly responsible under Sarbanes-Oxley. In conjunction with the controls over processes and applications managed by the entity, management must make the decisions regarding the sufficiency of scope, and is responsible for determining the adequacy of the testing coverage and evaluation of test results. The extent to which management is also responsible for making these decisions with respect to service-provider controls is driven by many factors, including the strength of the input controls, output controls, segregation of duties and other controls of the user organization, and the criticality of the service provider’s process and application to the reliability of the user's financial statements.

- There is also the issue of the point-in-time internal control report that management must issue to comply with Section 404 as of its annual year-end. An SSAE 16 SOC 1 report may cover either a point in time or a period of time, with a warning about projecting the results into the future beyond the date of the report. How would this requirement impact management's ability to sign off on its assertion about the controls as of year-end if the date of the SSAE 16 report differs significantly from that date? At minimum, management should understand whether there have been changes in the service organization's controls subsequent to the period covered by the service auditor's report. Such changes might include (1) changes
communicated from the service organization to management, (2) changes in service organization personnel with whom management interacts, (3) changes in reports or other data received from the service organization, or (4) errors identified in the service organization’s processing.

In addition, service organizations may choose to have their auditors issue periodic (e.g., semi-annual) SSAE 16 reports that they can provide to interested user organizations. In such instances, management must assess whether the specificity of such reports in relation to the relevant assertions is sufficient for its purposes.

– Lastly, management should review and ensure that user control considerations listed in the SSAE 16 SOC 1 report are operating effectively at their organization. User control considerations are controls within the SSAE 16 SOC 1 report that are required at the user organization to ensure effective operation of the SSAE 16 SOC 1 controls. Clearly, these considerations place a burden on management to perform the necessary work to assess effectiveness.

While there are many issues that should be considered, it is clear that for significant applications some work at the service provider is required. An SSAE 16 report is a good starting point, but it is possible that the SSAE 16 reporting process may require modification, as noted above, to align with the requirements of Section 404. The financial-reporting implications of the outsourcing arrangement are key and management is ultimately responsible for deciding what must be done. Due to management’s responsibilities to report on internal control and the independent auditor’s responsibility to attest to and report on management’s assertion, it is now necessary to focus closer attention on the adequacy of SSAE 16 reports for management’s purposes.

18. How does utilizing a software as a service (SaaS) application impact a company’s application control evaluation approach?

Depending on the nature of the SaaS application (i.e., cloud-based), management may or may not have the option to configure application controls. In the case that management does not have the ability to configure application controls, management should understand the existing application controls and how they impact the flow of transactions and any risks presented. Manual controls, user access levels and security administration should be considered for any risk exposures.

19. What are the different types of SSAE 16 reports, and how do they replace SAS 70 reports?

The SSAE 16 SOC 1 is intended to replace the SAS 70 reports that service organizations have previously issued. While the SSAE 16 report still has a Type I (control design assessment) and Type II (control design and operating effectiveness assessment), it also has three distinct reports, which consist of SOC 1, SOC 2 and SOC 3 reports. The SSAE 16 report that most resembles the SAS 70 is the SOC 1 report as it is based on control objectives. The SOC 2 and SOC 3 reports are based on a control requirement framework (i.e., Web Trust Principles).

20. Do we need to address controls for business units that are outside the United States?

As with all business units, the scope of the SOX controls should be based on financial-reporting risk and materiality. If business units outside the United States meet materiality thresholds established by the company when assessing risk, then SOX control requirements would apply, including IT controls.
Entity-Level Considerations

During the project, Section 404 compliance teams need to consider the overall strengths and weaknesses in the control environment surrounding IT. Overall entity-level controls include:

- The control environment, including the assignment of authority and responsibility encompassing IT operations and application management, consistent policies and procedures, and entity-wide programs such as codes of conduct and fraud prevention that apply to all locations and business units
- The risk-assessment processes used by management and process owners
- Overall structuring and organizational considerations around centralized processing and controls, including shared-services environments
- Procedures and analytics for monitoring results of operations
- Controls related to the prevention, deterrence and detection of fraud
- Processes for monitoring performance of controls, including activities of IT compliance and risk management functions, internal audit function and self-assessment programs
- Controls over the period-end financial-reporting process

These types of controls, often entity-wide in scope, are equally important in the IT areas as well as the business-process areas. Below is a more detailed discussion of certain entity-level control issues relevant to IT. Responses to these questions differentiate the IT organization from the entity's application and data owners, discuss how entity-level issues around IT risks and controls are considered, and provide guidance on the impact of strong and weak entity-level controls.

21. What is the IT organization?

As noted in Question 12, the “IT organization” consists of the IT operations and the overall governance of the processes impacting IT. Often consisting of the CIO’s organization, the IT organization sets the tone for effective control of IT risk across the enterprise. It manages areas defining the control environment affecting financial-reporting applications. These areas include the overall security administration policies, the application change control environment, the data backup and recovery, and SDLC. These processes should be considered when evaluating the “tone at the top” for entity-level considerations. The IT organization plays a significant role in overseeing these processes.

22. How does management consider the entity-level issues around IT risks and controls?

Management should initially consider how it manages the IT organization(s) in determining the entity-level issues around IT (see Question 21). Where and how is IT managed at a high level within the organization? Is it viewed as an integral part of each business unit, is it a separate unit, or some combination of the two?
Often in today’s environment there is some form of shared technical infrastructure between business units. If there is a central technical infrastructure, it is not unusual for the application management to be performed at the business-unit level. This structure definitely impacts how the entity-level controls need to be understood, documented and evaluated. To illustrate, there most likely will be an entity for the technical infrastructure part of the organization (the CIO’s organization, for example), and the various applications may be considered part of the business unit’s entity structure, may be unique entities within the business units, or may be some combination of the two. Because of the variability in ownership and responsibility for the respective areas, each of these organizational structures would be addressed in a slightly different manner in the entity-level evaluations, including in the way those evaluations are approached and documented.

23. Are there separate “entities” that include just IT operations or processes?

In Question 22, there could be separate entities in many organizations (from a COSO standpoint) related solely to IT. Also, there could be multiple entities related to IT within an organization. The number of IT-relevant entities will be unique to each organization because the approach to and management of IT differ significantly within an industry and based on the size of the organization. One of the first steps in the Section 404 compliance process is understanding the IT organization and structure, and determining how it is managed and organized. This step is critical to planning an effective IT evaluation approach for Section 404 compliance efforts.

24. What IT governance issues should be considered for purposes of complying with Sections 404 and 302 of Sarbanes-Oxley?

As discussed in our response to Question 12, there are two areas of overall governance within the IT structure. One relates to the management of the technology area, usually the CIO organization. The other relates to the application and data owners. The importance of IT governance in each of these areas relates to the way the organization instructs the process owners to understand, evaluate, and manage risks and controls, and to address control issues. At the entity level, the focus should be on the governance around the key process areas discussed in Questions 32-35 and 41-43. Governance is a critical issue related to the COSO “control environment” component that sets the “tone at the top.” If this is lacking, there is less likelihood that the overall entity-level controls will be strong.

25. What difference does it make if management has strong entity-level IT-related controls?

Strong entity-level controls provide the foundation upon which process/activity level controls are based. Strong entity-level control means that management is mitigating risks effectively and implementation of controls is a priority within the organization. Management will generally have a process for evaluating and understanding where the risks are, will often communicate and understand that they must have information supporting the entire control process, and will monitor key parts of the process so that they know on a timely basis when issues or problems arise. These capabilities greatly increase the likelihood of strong controls at the general IT controls activity/process level and at the application level.

26. How would management know if the entity-level controls provide a strong control environment?

A strong entity-level IT control environment is one in which upper management (the CIO, for example) of the IT organization, and the application and data owners, fully understand, communicate and monitor the overall control environment. In other words, they have the transparency required to know what is going on and whether there are any problems or issues. There will usually be management meetings with an agenda item to discuss internal controls and related issues. There will be documented policies and guidance around what is expected in the area of internal controls. The guidance at this level could amount to communication of the overall objectives or could
be provided at a more granular level. There also should be some sort of process to monitor the environment as well as effective upward and cross-functional communications to foster transparency. Further, there should be some documentation that evidences the key steps for the process.

27. What difference does it make if management has weak entity-level controls?

If there are weak entity-level controls, the likelihood of consistently strong general IT controls at the business process/activity level is greatly reduced. This does not mean that strong controls cannot exist at the general control process/activity level, but it does mean that upper management has not communicated clearly the need for such controls nor is there consistent monitoring of the environment. Lack of leadership at the entity level can foster an ad hoc and inconsistent control environment. This environment is one in which management and the process owners may not adequately focus on the need for the necessary IT-related controls that contribute to the effective achievement of financial reporting internal control objectives.

28. What are examples of a weak entity-level control environment?

In a weak entity-level control environment, there is a lack of communication and commitment to have an effective internal control structure. Overall policies and guidance related to the expectations for the development and maintenance of strong process-level controls are nonexistent or lacking. Communications emphasizing the need for strong controls are not evident. The goals and objectives (and tone set by management) of the IT organization are often focused on “lower costs” and staying within budgets instead of emphasizing quality of service or management of risk.
Activity/Process-Level Considerations –
General Control Issues

These questions explain the nature and importance of “general IT controls” to an evaluation of internal control over financial reporting. They also provide guidance as to what the Section 404 compliance project team looks for when evaluating these controls. While these controls have always been important, their impact often has been misunderstood. Our point of view is that Section 404 compliance teams should take a process view to understanding these controls. In this section, we break down the general IT controls into several basic processes, articulate the relevance of those processes to financial reporting, and discuss the impact of strengths and weaknesses on the evaluation of controls over applications and data processing. These controls include processes relating to security administration, application change control management, data backup and recovery, and SDLC.

29. What are “general IT controls”?

General IT controls typically impact a number of individual applications and data in the technology environment. As a general rule, these controls impact the achievement of the financial statement assertions germane to critical processes by supporting an environment that provides for the integrity of processing and data. The “general IT controls level” refers to processes impacting multiple applications; therefore, the controls over those processes are general IT controls.

General IT controls prevent certain events from impacting the integrity of processing or data. For example, if a critical manual control is dependent on IT-generated data, the effectiveness of general IT controls is a significant consideration when evaluating the process-level controls dependent on the IT system or on IT-generated data.

30. What types of controls are “general IT controls”?

General IT controls are pervasive or overall process-level controls. COSO uses the term “technology general controls” when referring to general IT controls and defines them as “general control activities over technology” that “must be implemented and operating for automated controls to work properly when first developed and implemented.” In addition, these general control activities “enable information systems to function properly after they are initially developed and implemented.” These controls include “controls over the technology infrastructure, security management, and technology acquisition, development, and maintenance.” COSO acknowledges that other terms sometimes used to describe technology general controls are “general computer controls,” “general controls” and “information technology controls.”

For the purposes of this publication, we will use the basic COSO definition above with the understanding that COSO is describing a set of processes and activities within the IT organization. Typically in today’s IT organizations, these processes include security administration, application change control management, data backup and recovery and SDLC. These IT processes will have the types of controls one would typically find in all business processes. Thus there will be a combination of manual and systems-based control activities, and preventive and
detective controls will be in place. There will be supervisory and management controls. Most importantly, as with all processes, management must determine for each of these IT processes the relevant specific control objectives related to the achievement of the overall internal control objectives for financial reporting. Stated in terms specific to the IT processes, the control objectives should relate to the integrity of processing and data (that achieves the completeness, accuracy, consistency and timeliness of financial reporting), and the proper access to data programs and specific transactions (which directly relates to the authorization and access to assets objectives).

Our responses to Questions 32 through 35 address some of the more common control objectives and control activities that would be considered during the Section 404 compliance effort. Our responses should not be viewed as all-inclusive or as checklists of matters that should be considered in every instance. However, the responses provide a good baseline of objectives and controls to be considered.

For each area addressed in Questions 32 through 35, we provide guidance on the following issues:

a) The relevance of this general control area to financial reporting internal control objectives
b) The impact of strong controls
c) The impact of weak controls

31. What technology stack layers (e.g., application, database management systems, operating systems) are required to be in scope for Section 404?

As discussed in our response to Question 13, GAIT can be a framework utilized to assist in determining the technology scope of a Section 404 program. As critical applications are identified, the risks at each layer of the stack for a potential failure that would cause a critical application function to fail should be assessed. Although dependent on an organization’s environment, typically operating systems and network infrastructure have fewer risks than the application and database layers. The organization should consider risks outlined in the GAIT methodology as it considers risk and controls for each technology layer.

32. What does the Section 404 compliance project team look for when evaluating security administration?

Background

In the security administration area, the primary process goals are in the area of establishing and maintaining the overall computer security for the IT environment. Security administration is comprehensive in focus, as it includes processes germane to applications, databases, platforms and networks. There also are processes that address identifying risks, formulating strategies to reduce risks to an acceptable level, and determining management’s explicit acceptance of residual risk or risk tolerances. Security administration requires an effective process for executing and monitoring the policies and processes dictated at all levels of the IT environment. There also are subprocesses to deal with access to each information asset and to control the risk of unauthorized access.

Within many companies, security administration is a complex and distributed process with multiple “technology layers” (e.g., applications, databases, platforms and networks) handled by different IT organization areas. For the applications, security administration may be distributed to different IT and user groups. A significant challenge during the evaluation of internal control is to understand how security administration is handled and distributed. This task requires the Section 404 compliance project team to obtain enough detail concerning the IT organization to understand where access to critical data and applications through each of the various “technology layers” is managed. The security administration process also includes processes and procedures around how to manage the administrative users who typically have full access to all transactions and data. It should be understood that administrative access is needed (and in most instances cannot be fully removed); however, stringent controls are necessary to restrict access and to monitor the administrator’s activities as he or she accesses and uses these privileges.
Other areas to be considered in this area include the access to automated job schedulers and the controls in place to ensure data processing occurs timely and without exceptions.

Following is a brief, high-level listing of the impact on an entity's financial-reporting assertions, and the impacts strong and weak controls over security administration have on the Sarbanes-Oxley 404 project scope:

**Impact on Financial-Reporting Assertions**

a) Limit access on a business need basis to critical systems (transactions, applications, databases, platforms and networks) to ensure access to data (assets) is appropriate.

b) Limit the ability to execute, approve and view transactions to those with a valid business purpose so that authorization is appropriately limited in accordance with management's criteria.

**Impact of Strong Controls**

a) Access is appropriately limited to critical information assets; therefore, other control activities related to the access to assets control objective (such as detective controls and monitoring activities at a relatively low level) are not necessary.

b) There is assurance at the general IT controls level (as explained in Question 29) that the authorization control objective has been fulfilled. These controls may be considered when evaluating authorization controls at the application and data-owner process level (as explained in Questions 41 and 42) and at the application-specific level (as explained in Question 46) to fully evaluate the control structure related to the objective.

c) There is assurance that these processes do not impact the completeness, accuracy and consistency of processing.

d) Access to critical transaction processing and data is appropriately restricted or monitored such that significant errors or omissions would not go undetected.

**Impact of Weak Controls**

a) Weak general IT controls over access to information assets (transactions, data and systems resources) causes the need to evaluate and understand potential compensating controls. In order to evaluate the appropriate controls, each individual asset (the transactions, data and systems resources) at issue should be evaluated as to “what could go wrong.” As each of these is evaluated, appropriate additional preventive, detective or other controls should be documented and evaluated. The primary question is as follows: “Since I cannot determine that access to the asset is properly controlled through the general IT controls, how would I know if an unauthorized modification, addition or deletion has been made and, if any has been made, that they have been detected and corrected timely?” Admittedly, this is a tall order, which is why no company would ever want to be in this awkward position.

b) If there are overall weaknesses in the general IT controls in security administration, assurance cannot be obtained that all transactions have been authorized in accordance with management's general and specific criteria. This raises the issue of whether there are unauthorized transactions, and if so, how such transactions would be detected so that appropriate adjustments are made. Again, this issue would need to be addressed in the context of the specific transactions under review.

c) Additional manual detective controls are needed at the application and data-owner level as well as at the IT organizational level when there are weaknesses in the security over the data processing areas. In the application and data-owner area, these controls would include more detailed procedures designed to detect changes to application processing and data. The additional procedures within the IT organization would include monitoring and supervision of individuals in these areas as well as potential systems monitoring and reporting of activities performed with extensive access privileges.
33. What does the Section 404 compliance project team look for when evaluating application change controls?

**Background**

The application-change process is one of particular significance to internal control over financial reporting. The integrity of application changes directly impacts the accuracy, consistency and completeness of transaction processing, as well as the accurate and timely accumulation, summarization and reporting of transactions.

As companies change their application systems, the risk emerges that these changes may cause applications that at one time processed and reported transactions with integrity to lose that integrity. This creates a potentially substantial risk of inaccurate, incomplete or otherwise incorrect financial reporting. Because of this financial reporting-related risk (as well as other obvious strategic and operational business risk issues), companies must have a well-designed and effectively operating application change management process.

This change process should cover all aspects of the change cycle, including initiation, monitoring, testing, and approval as well as migration of the appropriately approved change into the production environment. This process must also be appropriately secured so that personnel in this function cannot, without detection, make inappropriate changes to the program or the related data. The change process must be comprehensive in nature considering all possible implications of the changes, such as systems interfaces, data and error-checking routines, application security changes, management reporting, etc.

**Impact on Financial-Reporting Assertions**

a) Application changes directly impact the completeness, accuracy and consistency of the applications that process transactions and summarize and classify accounting information and disclosures.

b) Application changes can affect the appropriate segregation of incompatible duties when changes are made to add or modify duties and/or impact access to sensitive transactions and data.

c) Access to information assets may be made available to unauthorized individuals through the change-control process.

**Impact of Strong Controls**

a) Applications can be relied upon to work as intended by the users. The programs’ functionality and controls operate consistently and as intended. Change controls directly affect the control assertions around the completeness, accuracy and consistency of processing.

*A word of warning here – these controls assure the application functions as designed and intended. The control considerations within each application must be evaluated to determine whether the application’s design provides for all the necessary controls to achieve reliable financial reporting.*

b) There is assurance that the change-control process has not compromised the integrity of the data.

**Impact of Weak Controls**

a) There is no assurance that modifications to the programs have not adversely impacted the intended programmed controls. As a result, compensating controls would need to be evaluated and documented. These compensating controls should generally be manual and detective in nature, and may need to be performed at a fairly detailed level. In addition, there may be a need to further investigate the changes made to critical programs (the nature and frequency) in order to understand the particular types of controls required to detect specific errors that may arise if changes to the applications were not appropriate. As with weak controls over security administration, this position is one in which no company would ever want to be.

b) If access to applications and production data has not been appropriately restricted during the application-change process, there would be a need to consider and document compensating controls necessary to detect such inadvertent or intentional changes to the data or programs.

c) Reports produced by the system must be validated to source data to be relied upon.
34. What does the Section 404 compliance project team look for when evaluating data backup and recovery?

**Background**

Data may need to be recovered for any number of reasons, most of which arise from a hardware or software failure in which data has been corrupted or lost. The company must have the ability to restore or restart the processing in a manner such that it sustains operations and does not lose the integrity and completeness of transactions or data. The loss of the transactions and data obviously could affect the accuracy and completeness of processing.

Data backup and recovery also includes the considerations around the criticality of the application, and the appropriate timing and frequency of the backup process. The frequency and reliability of this process often reflect a cost/risk/benefit judgment around how much data (or transactions) a company can afford to lose without negatively impacting the business (in many different ways).

There are some who argue that Section 404 of Sarbanes-Oxley requires companies to have a full business continuity and disaster recovery plan in order to meet the “going concern” assumption inherent in the financial-reporting model. The “going concern” presumption has been around a long time and, in our view, was not modified under Sarbanes-Oxley. If a company had a “going concern” issue before the passage of Sarbanes-Oxley, it would likely have one now unless there has been a change in the facts and circumstances surrounding the company’s performance and prospects, and vice versa. However, that said, we strongly believe prudent companies should have appropriate business continuity and disaster-recovery plans in place based on a comprehensive business-impact analysis.

**Impact on the Financial-Reporting Assertions**

a) The ability to completely and accurately report transactions and financial-reporting data is impacted by the data management.

b) Access to assets could be impacted if inappropriate access is granted through the data management process to production or backed-up data.

c) The company’s ability to meet its obligations to file timely, complete and accurate reports with the SEC could be impacted if data recovery and restoration procedures are not effective.

**Impact of Strong Controls**

a) The data management process preserves the completeness and accuracy of data; thus subsequent processing following restoration and recovery can be relied upon.

b) Access is properly restricted, assuring data is not altered or deleted through the data-management process.

c) The risk of not being able to meet the filing requirements of the SEC due to loss of processing capabilities or loss of data essential for processing is adequately mitigated.

**Impact of Weak Controls**

a) There is no assurance that the data management process has not adversely impacted data. There is a need to document and evaluate mitigating controls designed to detect potential errors or omissions. These procedures and controls would most likely include procedures that inform users when data has been restored or when an attempt to restore data has occurred. The mitigating controls should include specific detective controls designed to determine inappropriate changes to data upon a restoration or recovery incident. In processing environments involving high transaction volumes, it is a formidable challenge to overcome inadequate data backup and recovery.

b) With respect to the company’s ability to comply with SEC filing requirements, there may be an inadequate business-impact and/or disaster-recovery plan. In such instances, the company should consider what procedures are needed to implement both a short- and long-term solution. This situation could possibly become a potential disclosure issue under Sarbanes-Oxley Sections 302 and 404. Therefore, the choice as to the steps to take must be carefully considered, including obtaining the advice of counsel, and appropriate action taken.
35. What systems development life cycle (SDLC) controls should be considered for technology implementation projects or significant system upgrades?

Technology implementation projects or significant system upgrades that impact critical business processes supporting financial elements should have control considerations above and beyond the change management controls discussed in Question 33. The following are controls that management should consider as Section 404 controls for these types of projects.

- Requirement of appropriate approval of executive management for project initiation.
- Validation of intended objectives of new system with appropriate management to ensure it adequately meets business requirements.
- Project roles and responsibilities are defined to ensure accountability for key project tasks.
- Project plan is documented and continuously updated throughout the project.
- Validation that the projected system implementation costs and timelines are met.
- New system has the appropriate application controls providing for reasonable protection from and/or detection of errors and malicious activities.
- New system is compliant with any statutory and/or organizational requirements.
- Final sign-offs are obtained by the business and IT management prior to installation and implementation of production.
- Any identified issues have been appropriately addressed.

Other control considerations include interface controls, testing processes, data conversion processes, ongoing support and maintenance, as well as user access and security controls.

36. We outsource our financial applications; do we need to do anything to be SOX compliant?

As with all organizations, a risk-based approach should be used to identify and prioritize IT risks and to identify applications that are related to critical business processes that support financial-reporting elements. Refer to Question 13 for information on the IT scoping process.

If all applications identified in the scoping process are outsourced, management should ensure SSAE 16 reports are obtained and evaluated. For each SSAE 16 report, management should ensure that user control considerations listed in the report are being followed by management. Refer to Question 17 for additional information on the SSAE 16 reports.

In addition to the general controls over managing applications, management should consider the risks (e.g., security, data backup, and availability) related to the organization’s network and potential impact on financial reporting.

37. Do we have to hire more IT resources to mitigate risks related to segregation of duties issues?

During the assessment of internal controls, management should evaluate the risks of weak controls resulting from segregation of duties issues. There is no one right answer for organizations; however, alternative controls can be explored depending on the type of risks presented to the organization. In some cases, manual detective controls can be implemented with minimal cost.
Activity/Process-Level Considerations –
The Role of Application and Data-Owner Processes

Responses to these questions explain who the application and data owners are, including their roles and responsibilities in relation to the IT organization and in facilitating compliance with Sections 404 and 302. This section provides guidance as to the processes that application and data owners must have in place with respect to areas that are especially critical to effectively functioning internal controls. Our responses also address the impact of application and data-owner process controls on the evaluation of internal control over financial reporting. For key financial-reporting applications, the Section 404 compliance team needs to identify the application and data owners. In some instances, these individuals may be process owners. The key activities and processes for which these individuals are responsible include security roles and administration, managing access to critical transactions and data, developing and maintaining business-impact analyses and continuity plans, and developing and maintaining business owner change control.

38. Who are the application and data owners?

Typically, application and data owners are part of the business process. Often they own the overall business process from a controls design and operations perspective, meaning they make decisions regarding the adequacy of the controls design and monitor the effectiveness of controls operation. While the overall process owner can delegate this ownership to someone or may assign responsibility to build out and execute the controls in accordance with the design, the process owner must clearly communicate what is expected out of delegates. In taking responsibility to understand, design and maintain the application’s controls, application and data owners must understand computerized controls so that they can knowledgeably design such controls and communicate their needs and requirements to IT personnel. Application and data owners also must understand the limitations of computerized controls, and be able to assist in the design of detective and monitoring controls that may be needed to compensate for weak IT general controls for certain IT processes.

39. What are the roles and responsibilities of the application and data owners in relation to the IT organization?

The application and data owners must be able to effectively communicate the intended application functionality, including the internal controls, to the IT organization. These communications are much like developing the blueprints for a building and then, as the structure is built, understanding whether it is meeting the desired specifications. If the structure is not being built to specifications, the application and data owners must articulate the overall adjustments needed to compensate for the gaps, particularly from an internal control perspective. The ongoing role of the application and data owners is to work with the IT organization as the application is changed and modified. Because applications are changed and modified constantly, it is the role of these owners to develop and maintain the requisite controls within the application. Overall, the application and data owners ensure the proper balance in the overall process to assure the adequacy of internal control over financial reporting.
40. What processes should the application and data owners have in place to facilitate compliance with Sections 404 and 302?

Like all process owners, application and data owners should periodically self-assess the controls for which they are responsible. Application and data owners should understand their applications in the context of the entire set of business-process controls, both manual and automated. As the application evolves and changes, the application and process owners should have an active part in both the quarterly Section 302 executive certification process and the annual Section 404 assessment process, particularly if significant issues arise. In both of these processes, the certifying officers depend on the integrity and reliability of significant financial applications. Therefore, feedback from the application and data owners, either directly or through unit management and/or the disclosure committee, can be invaluable to the certifying officers as they evaluate the impact of change.

41. What processes should be in place with respect to establishing proper security and segregation of duties?

Application and data owners must understand the transactions and data for which they are responsible well enough to ensure the activities around those transactions and data are appropriately segregated from an internal control standpoint. For example, the proper segregation of the authorization, execution and record keeping of transactions is a fundamental internal control principle. Application and data owners should not permit the technology environment to compromise this principle. Therefore, they should document the required separation of incompatible duties in a way that the IT organization can understand and enact these requirements from an application security standpoint. In other words, it is the application and data owner’s responsibility to document the system requirements for application security purposes.

On an ongoing basis, it is also the application and data owner’s responsibility to update and maintain this “transaction and segregation list” as the various applications evolve and change.

42. What processes should be in place with respect to periodic review and approval of access to critical and/or sensitive transactions and data?

As part of their responsibilities, application and data owners should oversee periodic reviews of how, how often and by whom critical transactions were accessed. Their reviews are intended to ensure that only those individuals with a legitimate business need are authorized and able to execute and/or view critical transactions and data. This review should be accomplished periodically based on the criticality and sensitivity of the transactions and data. The process should be documented to evidence the application and data owner’s sign-off on the propriety of the access “touch points” occurring during the review period. If actions and changes are needed, there should be a process in place to ensure these exceptions are handled in an expedient manner. If there are findings in this area that evidence a breakdown in the security administration process (see Question 32), a root-cause analysis should be undertaken and the matters resolved on a timely basis.

43. What processes should be in place from an internal control standpoint with respect to the application change management around initiating, testing and approving changes before making production application changes?

The application and data owners need to interact effectively with the IT organization’s change control process. They should:

a) Have the ability to initiate an application change.

b) Communicate the change through agreed-upon documentation to the IT organization.

c) Evaluate and document the impact of all proposed changes on the internal control environment.

d) Test the changes before they are moved into production. These should include procedures to validate the working of critical programmed controls (to ensure there are no unintended impacts on the control
environment from the change). Testing applies to any emergency changes to applications, i.e., application and data owners should be notified in advance of emergency changes so they can evaluate them appropriately.

e) For each of the above, there should be adequate documentation to demonstrate the process is operating as intended, and that the interaction between the application and data owners and the IT organization is effective.

44. If application and data-owner process controls are designed and operating effectively, what is the impact on the evaluation of internal control over financial reporting?

If all the critical application and data-owner process controls are working effectively, there is assurance that segregation of duties is being properly maintained from the standpoint of automated transactions and data. Thus, the application and data owners have assurance that segregation of incompatible duties and security over critical application systems and data are in place so that only authorized persons and applications have access to data, and then only to perform specific functions that directly relate to the authorization and access to assets assertions. Therefore, there should be no need to separately evaluate other compensating processes and procedures to ensure proper segregation of incompatible functions at the process level except for manual functions that are not systems-based.

If the change controls are working effectively, the accuracy and consistency of processing can be assured and, again, alternative or compensating detective control procedures can be minimized. Changes to application systems (through systems development, upgrades and maintenance) are authorized, tested and approved before they are implemented, which directly relates to the authorization, completeness and accuracy, classification, and access to assets assertions.

With effective business-impact analysis and continuity-planning procedures in place, the exposure to a business interruption compromising timely reporting under the SEC regulations is reduced.

These are some primary examples of the impact of effective application and data-owner process controls on the internal control objectives for financial reporting. However, we must inject a word of caution here. There is a direct relationship between the general IT controls within the IT organization and the effectiveness of the processes and controls falling within the domain of the application and data owners, as discussed above. In order to have a strong overall control environment, both the general IT controls and the application and data-owner controls must be designed and operating effectively.

45. If application and data-owner process controls are not designed and operating effectively, what is the impact on the evaluation of internal control over financial reporting?

Our response to Question 44 points out that the Section 404 compliance team need not look for alternative or compensating controls relating to the segregation of duties and the accuracy and completeness of processing if application and data-owner controls are strong. However, if application and data-owner controls are not adequate, then alternate or compensating controls must be documented, evaluated and tested.

In the absence of adequate business-impact analysis and continuity planning, there is an increased risk of a business interruption impacting timely reporting in accordance with SEC rules. If this risk is significant, the disclosure implications must be evaluated.
Activity/Process-Level Considerations – Application-Level Controls

Application-level controls include such controls within business processes as application-programmed controls, access controls (for key transactions and data), data-validation and error-checking routines, error reporting, and other controls. Our responses to these questions explain the application-specific control considerations at the activity/process level, including the selection of critical applications for each key business process and the integration of application-level controls with the evaluation of business-process controls. They also provide guidance as to the implications of strong and weak application-specific controls at the activity/process level.

46. What are the application-level control considerations?

Application-specific control considerations relate primarily to the controls programmed within an application that could be relied upon to mitigate business-process level risks. COSO defines application controls as, “Programmed procedures in application software, and related manual procedures, designed to help ensure the completeness and accuracy of information processing.” There are six primary areas of application controls that should be considered with respect to Section 404 compliance:

1. **Automated process controls**: Automated process controls are those controls addressed by application functionality. These controls can be codified controls that an application enforces based on programmed code and typically require application developers or programmers to modify or maintain. For example, most applications will not allow an unbalanced journal entry to post. For organizations with in-house-developed applications, many of the controls require IT developers to maintain them. However, for organizations with applications, many automated process controls can be configured to operate according to the organization’s specific policies, rules and strategies. Configurable controls are “switches” that can be set in an application by turning them on or off to secure data against validations and edits, screen layout, authorization groups, transaction variants, exception reports, and security settings. Configurable controls can be either preventive or detective in nature. Examples of configurable controls include tolerance limits with respect to purchase orders and invoice variances, acceptable ranges for determination of useful lives for asset classes or required fields for posting manual journal entries. Within each critical business process or transaction cycle, configurable controls addressing critical process risks should be identified and relied upon as appropriate. Where feasible, organizations should seek to continually optimize the use of and reliance upon configurable controls to both improve the sustainability and cost-effectiveness of the control environment and increase the efficiency of the testing of critical controls. During the initial testing process of Section 404, automated process controls in an application should have a baseline conducted. Refer to Question 47 for information on what is included in an application baseline.

2. **Manual process controls that may be candidates for automation**: No matter how integrated an application may be, generally an organization employs critical manual controls that operate outside of the application to ensure the integrity of the data and reliability of financial reporting. Examples of manual
controls include account reconciliations and approvals. An organization should consider all possible opportunities to “convert” manual controls to system-based controls, where feasible, in order to increase the effectiveness of the control as well as the efficiency by which the control can be validated.

A common category of manual process controls that may be candidates for automation is interface/integration controls. A SOX compliance approach should ensure interfaces between applications are considered as risk factors in the financial-reporting process, particularly if the interface is manual (e.g., download of data from one application for upload/entry to another). Controls that ensure the data integrity of the interface should be identified and validated. Organizations should document and assess how files are transferred, how users assure business transactions are authorized before being transferred, and whether any reconciliation procedures or other tools help ensure completeness and accuracy of the interface. For example, if an organization utilizes a payroll application that interfaces with the core financial-reporting application, the controls addressing the inherent risks relating to the “hand-off” of critical data between the two applications should be identified and validated. It is just as important to evaluate these controls as it is to assess the critical controls within each individual application.

3. **End-User Computing (EUC) controls:** Critical worksheets, spreadsheets and other user-developed and implemented technology tools need to be documented and evaluated as any other control or IT component. The difference is that these tools are often designed and deployed by users outside of the IT control environment. For example, when the IT department implements an application, there is rigorous and extensive testing of the application prior to implementation. The IT department then has a number of processes such as change control, security, backup and recovery that provide assurances about the maintenance and operation of the application. For user-developed and maintained applications, there is a need for separate evaluations of these IT-related processes for these applications, particularly if the applications have a significant impact on the overall financial-reporting process. This separate evaluation should address the change control, security, backup and recovery issues related to these applications. With respect to application functionality, the evaluation must consider areas such as the accuracy of critical calculations, data validation and error checking, completeness and accuracy issues, key interfaces, and the integrity of the reporting process. There is also a need to evaluate and conclude on the consistency, accuracy and substantiation of processing based on audit trails and other evidence regarding the processing performed by these and user-developed applications, spreadsheets and tools.

4. **Reporting controls:** Reporting controls are necessary to ensure reports generated from the application accurately reflect the financial position of the organization. The compliance team should assess risk from the financial reports through the intermediary systems (e.g., Hyperion and other consolidation systems) and ultimately back to the source system to ensure all risks and controls are considered within and outside the application. This includes consideration of report design and maintenance processes as well as processes governing the manipulation of extracted data outside the application. A common example is an organization’s download of financial data from the core financial-reporting application (e.g., an ERP application) into a spreadsheet for use in preparing financial reports and disclosures, including EDGAR formats for filing with the SEC. The compliance team should identify and validate controls that address the risk of the data being modified inappropriately subsequent to the download of the data and prior to the final preparation of the financial statements. All of the aforementioned configurable, application, interface and EUC controls are rendered useless if a risk at this point in the financial-reporting process remains unmitigated.

5. **Application security, as it relates to segregation of duties and access to sensitive transactions:** Different from security administration, this area relates to the risk that individuals or groups have been granted inappropriate or excessive access to an application, resulting in the ability to perform conflicting duties (e.g., set up a vendor/pay a vendor) and/or inappropriate/unnecessary access to sensitive transactions (e.g., vendor pay data or ability to modify critical application configurations). Application security should be considered for each critical business cycle to ensure appropriate access based upon a succinct role definition. The access defined for each role should be free of any conflicting duties. From there, roles should be allocated to individuals who perform the specific roles defined. Care should be taken to ensure that no individual is assigned a combination of incompatible roles that create a conflict.
47. **How is an appropriate application baseline established?**

Management should consider performing an application baseline to confirm programmed functions and application controls are operating as intended. After the initial baseline is conducted, reliance can be placed on the general IT controls to ensure effectiveness in subsequent years.

Key elements of establishing a baseline for a given application include:

- **Establish baseline scope:** Identify key application controls, programmed functions and reports that are relied upon to help assure complete, accurate, timely and proper processing and reporting of transactions. The identified population of controls, functions and reports creates the baselining scope.

- **Document configurable controls and supporting general application processes:** Document configuration settings and business rules for the controls, functions and reports, and obtain approval by appropriate management that such settings and rules are expected within the applications.

- **Validate operation of configurable controls and general application processes:** Validate that the established baselines are operating and utilized as designed and documented. This can be achieved via multiple methods, including:
  
  - If the system has been recently implemented, review existing application implementation documentation, including unit/integration testing, system testing and user testing.
  
  - Reperform the control or function through automated or manual testing.

48. **How does the Section 404 compliance team determine the critical applications for each key business process?**

After high-priority financial-reporting elements and related high-priority processes are identified, a critical part of the compliance effort is identifying the applications that are utilized in the high-priority processes. These applications are likely to impact the priority financial-reporting elements. In analyzing any critical business process, the compliance team should document the key inputs, processing activities and process outputs. This documentation should include a description or map of the applications systems that are an integral part of the process.

The related critical applications for each significant business process that are involved in the data flow from the originating transaction to financial statement generation (including all access points into applications and hand-offs and interfaces between applications) should be identified and prioritized. In other words, the compliance team should select the applications that (a) are integral to the success of the process in making the process perform to achieve its objectives, and/or (b) expose the process to increased risk of not achieving the relevant financial-reporting assertions. These applications should be integrated into the documentation and evaluation process supporting management’s assertion regarding the effectiveness of internal control over financial reporting in the Section 404 internal control report.

Some factors to consider when prioritizing applications include:

- **a)** The volume of transactions processed (typically, the higher the volume, the more critical the application)

- **b)** The dollar amount of the transactions (typically, the larger the amount, the more critical the application)

- **c)** The complexity of the calculations – complex in this situation means the ability of the users to determine the propriety and reasonableness of the calculation (typically, the more complex, the more critical the application)

- **d)** The sensitivity of the data and transactions (typically, the more sensitive, the more critical the application)
Many companies employ an ERP solution (e.g., SAP, Oracle) for their general ledger, but complement that solution with a financial consolidation solution (e.g., Hyperion) for financial-reporting purposes. As many companies began Section 404 compliance activities, they realized that their ERP access structures gave users excessive authorization and data access. In response, these companies re-implemented authorization and data access structures within the application to ensure proper restrictions. However, users could still freely access equivalent data via the consolidation application, thereby circumventing the intended security restrictions. Thus, without also identifying the consolidation application as a critical element within the security assessment scope in addition to ERP security, the organization’s assessment would be inadequate.

When the applications are being prioritized, it is important to identify all applications used, including worksheets, spreadsheet macros, user-database programs (e.g., Microsoft Access) and web-based programs and calculators. These types of programs need to be documented and the change control, security, backup and recovery procedures need to be separately evaluated, particularly if the applications have an impact on the overall financial-reporting process.

In summary, it is important to identify the complete universe of applications utilized within the organization that enable critical processes to perform and produce key financial statement elements. This effort will enable the compliance team to determine which key applications fall within the compliance scope and ensure that the Section 404 documentation and control assessment is complete.

49. How should the Section 404 compliance team integrate the consideration of application-level controls with business-process controls at the activity/process level?

The application-specific controls are a critical part of business processes and should be documented and evaluated at the same time as the other business-process controls. The compliance team needs to consider the process risks and key control points, and determine which controls are programmed application controls (such as an automated three-way match) and which controls rely upon computer-generated information to operate effectively (such as an exception report). Manual and application-related controls do not operate in a vacuum. They are often times not mutually exclusive. Therefore, it is important to identify and assess them together in order to identify control dependencies and achieve a holistic assessment of the business process as a whole. The PCAOB included case examples in an appendix to Auditing Standard No. 5 that illustrate this point.

By considering manual and related application controls simultaneously within a business process, the compliance team will be far more likely to identify a more sustainable and efficient mix of manual and application controls in terms of testing controls operating effectiveness. In addition, the compliance team also will be able to identify opportunities to further automate manual controls.

Once the key applications and manual controls are identified for purposes of Section 404 compliance, the team then needs to consider what steps are necessary to fully understand and document the key controls within the application. Skills and resources are important factors to consider when planning these steps (i.e., use a specialist to understand the design and operations of critical application systems and the control capabilities embedded within those systems).

50. What should management do if the Section 404 compliance team finds strong application controls at the business-process level?

If there are strong application controls at the business-process level, then generally there should be strong preventive and programmed detective controls in place. Under these instances, there is no need to have redundant manual detective controls. When strong application controls exist, the nature of the monitoring controls can be focused at a higher level and with larger scope tolerances than with weak application-level controls.
51. What should management do if the Section 404 compliance team finds weak application controls at the business-process level?

If there are weak application controls at the business-process level, then compensating detective and monitoring controls need to be documented and reviewed. These detective and monitoring controls need to be detailed and extensive in nature and scope and perform at a high level of precision. The detective and monitoring controls should also not depend on computer processing to operate effectively. For high-volume processes, these requirements are difficult to accomplish. Depending on the nature and severity of the weaknesses, consideration of changes to improve the application-level controls may need to be undertaken. Furthermore, without the requisite application-level controls, it may not be possible to conclude on the effectiveness of internal control in reducing certain risks to an acceptable level.

52. How can an organization decrease its reliance on spreadsheets?

Many organizations have opportunities to better utilize the existing reporting capabilities of their applications. Often, when company representatives rely on reports or data generated from software other than their existing applications, it is a good indication that the individuals who utilize that software to support financial reporting aren’t maximizing the reporting capabilities of their applications. Reliance on spreadsheets is a good example of this problem.

For example, many organizations often extract data from an application and download it to a spreadsheet application for custom sorting and filtering. This process may be undertaken without understanding that the application has similar capabilities built into its reporting functionality. Ultimately, this activity may be a result of inadequate user requirements analysis during implementation. Alternatively, it may be a training issue where the end users are not made aware of the functionality offered by the application. If this situation is prevalent throughout the company, management should consider it a possible risk. As individuals involved in the compliance efforts begin to fully understand the capabilities of their company’s applications, they more fully realize the importance of using the reports generated from that application, as well as the control implications and related compliance costs and risks of not doing so.

53. What are some application control considerations for the order-to-cash cycle?

The order-to-cash (OTC) cycle in an ERP system encompasses all activities related to the sale, delivery and billing of materials and/or services to the organization’s customers. Activities within the ERP system that support this major cycle include:

- Customer master data maintenance
- Inquiries, quotations, pricing and contract administration
- Goods/services issues and shipping/delivery processing
- Returned material processing
- Billing, invoicing and payment processing
- Sub- and general ledger updates

Throughout these processes there are several configurable controls and functions that should be considered. Examples include customer master record maintenance, duplication checks, pricing tolerances, invoice posting tolerances, duplicate invoices checks, dunning process, credit limits, credit memo limits, shipping-to-sales order tolerance, journal entry processing, transaction account impact and reconciliation, and revenue recognition and account determination.
54. What are some application control considerations for the procure-to-pay cycle?

The procure-to-pay (PTP) cycle in an ERP system encompasses all activities related to the requisition, order, receipt and payment for materials and/or services from the organization’s vendors and suppliers. Activities within most ERP systems that support PTP include:

- Vendor and item master data maintenance
- Purchase requisitions and orders processing
- Goods/services receipt and verification processing
- Invoice entry, verification and matching
- Payment and credit note processing
- Sub- and general ledger updates

As with OTC, there are several configurable controls and functions that should be considered. Examples include:

- **Purchase order, goods/services receipt and invoice matching:** ERP systems can be configured to validate purchasing transactions in a variety of ways. Many systems can incorporate a two-way, three-way or four-way match for the company’s purchases and, in many cases, the type of matching used relates to the type of purchase. Within most ERP systems, the matching procedure is only part of the validations occurring prior to the payment of an invoice. The software also can be configured to identify receiving tolerance amounts, which are utilized to determine acceptable variance limits associated with differences between a purchase requisition and purchase order, and/or a purchase order and a goods receipt.

- **Goods/services receipt and verification processing:** It is important to ensure that the inherent risks in this process relative to unrecorded liabilities are carefully managed. Most ERP systems mitigate this risk by recording inventory receipts in an un-vouchered account and subsequently recording vendor invoices in the accounts payable subsidiary ledger when the invoice is received.

- **Invoice entry:** Mitigating inaccurate recording of liabilities is important.

55. What are some application control considerations for the close-the-books/financial-reporting cycle?

The financial-close process should be configured within an ERP system to assist in addressing risks inherent in subprocesses, such as the processing of journal entries, account reconciliation, closing reports, consolidation and the drafting of financial statements. Some other items to consider within the ERP system include:

- Configuration of the organizational hierarchy, chart of accounts, reporting structure and closing of the books
- Frequency of posting of journal entries to subsidiary ledgers and reconciling subsidiary ledgers to the general ledger (Note that some ERP systems post to the general ledger on a monthly basis in batch mode, while other ERP systems post to ledgers immediately.)
- Journal entry configuration options such as “park and post” approvals, posting tolerances and balancing (debits equal credits)

The implementation of an ERP system can integrate journal entry activity between the subsidiary ledgers and general ledger and, if configured correctly, can significantly reduce the amount of time spent reconciling accounts. Most ERP systems are delivered with standard reports that facilitate and support the reconciliation process.

While reports support the review process, an ERP system does not eliminate the necessity to review key balance sheet and income statement accounts as well as processes that require judgment and/or manual intervention (e.g., determination of write-offs and reserve levels). In addition, key processes within the financial close require formal documented policies and procedures.
Documentation

Documentation is important in an evaluation of internal control over financial reporting. The SEC Interpretive Guidance states:

Management is responsible for maintaining evidential matter, including documentation, to provide reasonable support for its assessment. This evidence will also allow a third party, such as the company’s external auditor, to consider the work performed by management.

Our responses to the questions in this section provide guidance on documentation at various levels, including the entity level and activity/process-area level. Documentation of IT risks and controls needs to be consistent with the overall standards and approach set by the Section 404 compliance team. As noted by the SEC, documentation also must satisfy the requirements of the attestation process.

56. How much documentation should the IT organization and the application and data owners have in place to evidence the controls and functioning of the applications?

There are two considerations related to this question. The first relates to the documentation needed to evidence the effective functioning of the program and its related controls. The second addresses the technical documentation necessary to ensure that the application can be maintained such that the integrity of processing and controls can be assured.

Application documentation should specify where and how key components of the application operate. The key components should include the critical application controls discussed in the Activity/Process-Level Considerations – Application-Level Controls section. The documentation can take many forms: process flows and narratives, flowcharts that show the steps during program processing, other technical documents that show data relationships, and database designs. The technical documentation should be such that an unfamiliar (but technically competent) programmer could understand the program functionality as well as its critical interfaces, data handling and security features. The documentation should provide a reasonable basis for performing the required maintenance.

Documentation that includes only the base program code and technical database specifications is not considered adequate in most circumstances. If there is inadequate documentation of the application, it increases the risks that changes made may not be appropriate. If that risk exists, the implications of weaknesses in change management should be carefully considered.

57. How should the Section 404 compliance team document the IT controls at the entity level?

The approach to documenting controls in the IT area should be similar to the approach to documenting controls in other business areas. At the entity level, the documentation should focus on policies, procedures, corporate communications, minutes of management meetings, and questionnaires and other items specifying how the entity controls operate.
58. How should the Section 404 compliance team document the IT controls for the IT general controls at the activity/process level?

For the IT general controls applied at the activity/process level, we believe that process maps and risk-and-control matrices are the most appropriate tools for documenting the processes. This type of documentation is similar to the documentation for other business processes.

59. How should the Section 404 compliance team document the IT controls for the processes controlled by application and data owners and for the specific application areas?

For the processes controlled by the application and data owners, we believe that process maps and risk-and-control matrices are the most appropriate tools for documenting the processes. At the business-process level, the documentation of the application-level controls is best accomplished in an integrated fashion with the other business-process risks and controls. Integration is the best way to fully understand the dependency of internal controls on IT. It may be helpful to indicate when a business-process control is an application control so that those controls can be reviewed and tested, as necessary, by an individual with application-control expertise. There should be additional documentation around key applications such as system maps or data flows, matrices that indicate applications impacting the business process, and a matrix of key application-control considerations. The key control considerations would highlight complex calculations, key data validation and verification checks, significant and/or complex interfaces, etc. Accordingly, the appropriate skill set must be brought to bear to consider these risks and the related control implications.
Testing

The aforementioned discussion provides guidance relative to design principles for IT controls at all levels of the organization. Like all other controls, IT controls must be tested to ascertain they are operating as designed. The fourth edition of our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* provides comprehensive guidance on testing. Our response to the question below expands on that guidance to address IT-related controls.

60. How are IT controls tested?

IT controls should be tested in a manner similar to the controls in other process areas. There should be a combination of inquiries, observation, inspection and reapplication and/or reperformance techniques, which are further explained in the aforementioned *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*. In all instances, adequate documentation of the testing should be developed. A combination of testing is often appropriate to form a conclusion related to operating effectiveness.

At the IT entity level, one would expect most of the testing to be related to inquiries, observation and inspection because reperformance and reapplication cannot typically be accomplished for many of these types of controls. For the processes in the general IT controls area and for application and data-owner controls, there is a need for all four types of testing, including reperformance and/or reapplication. For these processes, the process-level control design ordinarily should provide evidence that certain parts of the process were completed (e.g., signatures or other sign-offs on forms).
Addressing Deficiencies and Reporting

If there are internal control deficiencies, they must be remedied if significant. The fourth edition of our Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements provides guidance on addressing internal control deficiencies. Our responses to the questions below expand on that guidance to address IT-related controls.

61. How should management address deficiencies and gaps in IT controls?

There are two possible ways for management to address IT control deficiencies. The first and most obvious approach is to perform a gap analysis of the process or control that is either designed or operating ineffectively, and develop an action plan to close the gap. The other possibility, which may be appropriate at least in the short term, is to make sure there is a thorough risk analysis of the deficiency and of the surrounding compensating controls, if any, to determine the extent of the risk to the financial-reporting assertions and whether the risk is adequately mitigated. In addition, management should demonstrate how it is comfortable with the control environment during the period the deficiency existed. For example, if a segregation of duties issue existed in the accounts payable process, management could perform an investigation to determine if any users created and approved payments to the vendor that the user created. These steps are vital in the short term because gap analysis and closure could take an extended period of time to improve IT controls. In many cases, there is likely to be a significant increase in the need for manual detective controls that identify and correct specific items that could result in errors or omissions at the business-process level. In situations involving high transaction volumes or highly complex transactions, this could present a significant and costly challenge.

62. How will the external auditor view IT controls during the attestation process?

This obviously is a question that each external audit firm will address with each of its audit clients. It is safe to say, however, that the independent accountant will have IT-related risks and controls in mind when evaluating the basis for management’s assertions in the internal control report. The general IT controls are pervasive controls that impact the integrity of most, if not all, transactions, as well as most, if not all, of the internal financial reports from which the financial statements are derived. A weakness in general IT controls potentially could have an effect over significant transactions and accounts. If there are gaps in the general IT controls, it is possible that the external auditor could insist that those gaps be addressed before an overall opinion is reached on the effectiveness of the internal controls. For example, we are aware of instances in which an external audit firm has informed its audit client that the company must develop stronger controls over application security, in particular with respect to the administration of security roles and the security over access by users, before it could attest to a positive assertion by management on the control environment. When issuing guidance for interpreting reports on internal control
over financial reporting, Moody’s took the position that not all material weaknesses were alike. Some material weaknesses may be so pervasive, the external auditor may conclude that an overall opinion on the effectiveness of internal control over financial reporting cannot be expressed. To illustrate its point, Moody’s cited a material weakness in general IT controls as an example of a potentially pervasive material weakness. For this reason, Section 404 compliance teams should assess the IT control environment, including the general IT controls, as early as possible in the process to determine whether there are gaps that must be addressed. Failure to do so could expose the company to difficulty with the attestation process.

The IT controls at the application and data-owner process level and for specific applications could have a similar impact on the overall internal control structure for applications deemed to be significant to the financial statements. This is why a company’s approach to complying with Section 404 should integrate the consideration of controls over applications and data at the process level. Section 404 compliance teams should ensure that this integration takes place.
About Protiviti Inc.

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE® 1000 and Global 500 companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Information Technology Internal Audit Co-Sourcing and Information Technology-Related Sarbanes-Oxley Compliance Services

Protiviti provides a broad range of IT internal audit co-sourcing and outsourcing solutions. Our IT internal auditors have broad expertise to assist in all aspects of IT audit services, from the definition of the audit universe and performing the risk assessment, the annual planning and scoping process to the execution of all types to technology-related internal audits. We also provide consulting services around the technology risk and control aspects of Sarbanes-Oxley compliance services. We provide expertise in documenting critical business processes, identifying risks and mitigating controls, analyzing performance gaps, and recommending and implementing action plans to improve controls. Our Certified Information Systems Auditors, Certified Internal Auditors and Certified Public Accountants add value by helping companies comply with the information technology risk and control-related requirements of Sarbanes-Oxley, primarily Section 404. In each of these areas we help companies understand and evaluate technology-related risks related to:

- Technology audit planning and risk assessments
- Application control reviews and internal audits
- Security assessments and internal audits
- Technology process controls reviews and internal audits
  - Change control and management
  - Security administration
  - Data center operations and problem management
  - Data management and disaster recovery
  - Asset management

Our Information Technology Consulting Services

Security and Privacy

Protiviti approaches enterprise security and privacy from a business perspective. We understand your core business processes, your industry, the regulations, and the technology that supports your current and future business
strategies. We then implement sustainable solutions using our expertise and a structured approach that includes proven methodologies and tools. Our approach allows us to:

- Assess vulnerabilities and risk.
- Develop policies.
- Design architecture.
- Deploy solutions.
- Create awareness.
- Monitor compliance.

**Business Continuity Solutions**

Protiviti works with you to manage the continuity and availability of your key business processes and technology assets. We capture your business requirements and create a solution based on proven processes. From crisis management to business continuity and IT disaster recovery, our professionals have helped companies overcome their limitations to come out stronger than ever. Our approach allows us to:

- Assess vulnerabilities and impact.
- Design and develop processes to maintain availability.
- Implement procedures and integrate with business operations.
- Test and validate continuity and recovery procedures.
- Build confidence in your team’s ability to recover.

**Change Management Solutions**

Technology change management is the practice of managing and controlling changes to the technology environment from the initial request through deployment. Protiviti helps organizations harness productive changes to information systems through a consistent and enforceable process. Our holistic approach focuses on improving coordination, efficiency and control. This minimizes the risks to the availability, integrity, scalability, performance and security of our clients’ information systems. Our approach allows us to:

- Assess current state for baseline measurement going forward.
- Design a solution to meet your business objectives.
- Implement tools to enable effective change management.
- Integrate change management with technology operations management.
- Define performance metrics and implement mechanisms to report and analyze root causes.

**IT Asset Management Solutions**

Protiviti works with companies to maximize the value of their IT assets. By effectively managing your costs, licensing agreements, performance and IT infrastructure complexity, you can manage your assets from the places that drive their value. We partner with leading software firms to deliver solutions to fit your business situation and goals. Our approach allows us to:

- Build cost-optimization strategic plans.
- Prepare assessments and root-cause analysis.
- Design and implement solutions.
- Measure operations and performance.

**Program Management Solutions**

Protiviti’s project risk management service provides you with a roadmap to identify, mitigate, and source to the
root cause of risks related to the management, execution, and control of projects. We provide a range of services and tools to assist you in implementing strategies, processes, and controls for improving your project environment. We will help you effectively manage the projects critical to your business success. And we tell it like it is so that you can manage now, not react later. Our approach allows us to:

- Assess risk management and control environment.
- Design and implement project management.
- Manage enterprise-wide projects.
- Develop and implement office dashboards.
- Perform pre- and post-implementation reviews.

Application Effectiveness Solutions

Protiviti helps you ensure success through effective solutions management. With our technical and business process expertise, we get to know your business objectives and identify exposures. We help you mitigate risk in your existing applications and design-in controls during the implementation of your new applications. Our approach allows us to:

- Assess company-specific control priorities.
- Evaluate the design controls and identify gaps.
- Observe and test operating effectiveness of controls.
- Implement controls to help you meet your objectives.
- Design methods and tools to monitor ongoing effectiveness.

Other Thought Leadership from Protiviti

Visit [www.protiviti.com](http://www.protiviti.com) to obtain copies of these and other thought leadership materials from Protiviti.

- 2012 IT Audit Benchmarking Survey
- Using High Value IT Audits to Add Value and Evaluate Key Risks and Controls
- Powerful Insights (Protiviti’s podcast series)
  - IT Audit – Assessing and Managing Risks Effectively within the IT Environment
  - The Importance of Strong IT Governance During a Financial Crisis
  - Social Media Use in Companies – Managing the Risks Effectively
  - Technology-enabled Audits – Increasing Productivity and Delivering More Timely and Reliable Results
  - Internal Audit Quality Assessment Reviews – Required as well as Beneficial
  - Sarbanes-Oxley Compliance: Where U.S.-listed Companies Stand Today
  - The Benefits of Outsourcing the Internal Audit Function
- 2012 Internal Audit Capabilities and Needs Survey
- Testing the Reporting Process – Validating Critical Information
- Internal Auditing Around the World (Volumes 1-8)
KnowledgeLeader® is a subscription-based website that provides information, tools, templates and resources to help internal auditors, risk managers and compliance professionals save time, stay up to date and manage business risk more effectively. The content is focused on business risk, technology risk and internal audit. The tools and resources available on KnowledgeLeader include:

- **Audit Programs** – A wide variety of sample internal audit and IT function audit work programs are available on KnowledgeLeader. These work programs, along with the other tools listed below, are all provided in downloadable versions so they can be repurposed for use in your organization.

- **Checklists, Guides and Other Tools** – More than 1,000 checklists, guides and other tools are available on KnowledgeLeader. They include questionnaires, best practices, templates, charters and more for managing risk, conducting internal audits and leading an internal audit department.

- **Policies and Procedures** – KnowledgeLeader provides more than 300 sample policies to help in reviewing, updating or creating company policies and procedures.

- **Articles and Other Publications** – Informative articles, survey reports, newsletters and booklets produced by Protiviti and other parties (including Compliance Week and Auerbach) about business and technology risks, internal audit and finance.

- **Performer Profiles** – Interviews with internal audit executives who share their tips, techniques and best practices for managing risk and running the internal audit function.

Key topics covered by KnowledgeLeader:

- Audit Committee and Board
- Business Continuity Management
- Control Self-Assessment
- Corporate Governance
- COSO
- Fraud and Ethics
- IFRS
- Internal Audit
- IT Audit
- IT Governance
- Sarbanes-Oxley

KnowledgeLeader also has an expanding library of methodologies and models – including the robust Protiviti Risk ModelSM, a process-oriented version of the Capability Maturity Model, the Six Elements of Infrastructure Model, and the Sarbanes-Oxley 404 Service Delivery Model.

Furthermore, with a KnowledgeLeader membership, you will have access to AuditNet Premium Content; discounted certification exam preparation material from ExamMatrix; discounted MicroMash CPE Courses to maintain professional certification requirements; audit, accounting and technology standards and organizations; and certification and training organizations, among other information.

To learn more, sign up for a complimentary 30-day trial by visiting www.knowledgeleader.com. Protiviti clients and alumni, and members of The IIA, ISACA and AHIA, are eligible for a subscription discount. Additional discounts are provided to groups of five or more.

KnowledgeLeader members have the option of upgrading to KLplusSM. KLplus is the combined offering of KnowledgeLeader’s standard subscription service plus online CPE courses and risk briefs. The courses are a collection of interactive, Internet-based training courses offering a rich source of knowledge on internal audit and business and technology risk management topics that are current and relevant to your business needs.
### Protiviti Internal Audit and Financial Controls Practice – Contact Information

<table>
<thead>
<tr>
<th>Country</th>
<th>Contact</th>
<th>Phone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UNITED STATES</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Region</td>
<td>Michael Thor</td>
<td>+1.312.476.6400</td>
<td><a href="mailto:michael.thor@protiviti.com">michael.thor@protiviti.com</a></td>
</tr>
<tr>
<td>Eastern Region</td>
<td>James Armetta</td>
<td>+1.212.399.8606</td>
<td><a href="mailto:james.armetta@protiviti.com">james.armetta@protiviti.com</a></td>
</tr>
<tr>
<td>Western Region</td>
<td>Anthony Samer</td>
<td>+1.415.402.3627</td>
<td><a href="mailto:anthony.samer@protiviti.com">anthony.samer@protiviti.com</a></td>
</tr>
<tr>
<td><strong>AUSTRALIA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ewen Ferguson</td>
<td>+61.2.8220.9500</td>
<td><a href="mailto:ewen.ferguson@protiviti.com">ewen.ferguson@protiviti.com</a></td>
</tr>
<tr>
<td><strong>CANADA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Marc Poirier</td>
<td>+1.514.871.2348</td>
<td><a href="mailto:marc.poirier@protiviti.com">marc.poirier@protiviti.com</a></td>
</tr>
<tr>
<td><strong>CHINA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Michael Pang</td>
<td>+852.2238.0499</td>
<td><a href="mailto:michel.pang@protiviti.com">michel.pang@protiviti.com</a></td>
</tr>
<tr>
<td><strong>GERMANY</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Thorsten Ruetze</td>
<td>+49.69.9637.68.142</td>
<td><a href="mailto:thorsten.ruetze@protiviti.de">thorsten.ruetze@protiviti.de</a></td>
</tr>
<tr>
<td><strong>INDIA</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sandeep Gupta</td>
<td>+91.22.6626.3333</td>
<td><a href="mailto:sandeep.gupta@protiviti.co.in">sandeep.gupta@protiviti.co.in</a></td>
</tr>
<tr>
<td><strong>JAPAN</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Yasumi Taniguchi</td>
<td>+81.3.5219.6600</td>
<td><a href="mailto:yasumi.taniguchi@protiviti.jp">yasumi.taniguchi@protiviti.jp</a></td>
</tr>
<tr>
<td><strong>SINGAPORE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ivan Leong</td>
<td>+65.6220.6066</td>
<td><a href="mailto:ivan.leong@protiviti.com">ivan.leong@protiviti.com</a></td>
</tr>
<tr>
<td><strong>UNITED KINGDOM</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mark Peters</td>
<td>+44.207.389.0413</td>
<td><a href="mailto:mark.peters@protiviti.co.uk">mark.peters@protiviti.co.uk</a></td>
</tr>
</tbody>
</table>

David Brand
Managing Director Leader
IT Audit Practice
+1.312.476.6401
david.brand@protiviti.com

Brian Christensen
Executive Vice President
Global Internal Audit
+1.602.273.8020
brian.christensen@protiviti.com

David Brand
Managing Director Leader
IT Audit Practice
+1.312.476.6401
david.brand@protiviti.com
### THE AMERICAS

**UNITED STATES**
- Alexandria
- Atlanta
- Baltimore
- Boston
- Charlotte
- Chicago
- Cincinnati
- Cleveland
- Dallas
- Denver
- Fort Lauderdale
- Houston
- Kansas City
- Los Angeles
- Milwaukee
- Minneapolis
- New York
- Orlando
- Philadelphia
- Phoenix
- Pittsburgh
- Portland
- Richmond
- Sacramento
- Salt Lake City
- San Francisco
- San Jose
- Seattle
- Stamford
- St. Louis
- Tampa
- Washington, D.C.
- Woodbridge

**ARGENTINA**
- Buenos Aires*

**BRAZIL**
- Rio de Janeiro*
- São Paulo*

**CANADA**
- Kitchener-Waterloo
- Toronto

**ASIA-PACIFIC**

**AUSTRALIA**
- Brisbane
- Canberra
- Melbourne
- Perth
- Sydney

**CHINA**
- Beijing
- Hong Kong
- Shanghai
- Shenzhen

**INDIA**
- Bangalore
- Mumbai
- New Delhi

**INDONESIA**
- Jakarta**

**JAPAN**
- Osaka
- Tokyo

**SOUTH KOREA**
- Seoul

**FRANCE**
- Paris

**ITALY**
- Milan
- Rome
- Turin

**THE NETHERLANDS**
- Amsterdam

**EUROPE**

**FRANCE**
- Paris

**GERMANY**
- Frankfurt
- Munich

**ITALY**
- Milan
- Rome
- Turin

**THE NETHERLANDS**
- Amsterdam

**MIDDLE EAST**

**BAHRAIN**
- Manama*

**OMAN**
- Muscat*

**KUWAIT**
- Kuwait City*

**UNITED ARAB EMIRATES**
- Abu Dhabi*
- Dubai*

* Protiviti Member Firm
** Protiviti Alliance Member

© 2012 Protiviti Inc. An Equal Opportunity Employer. PRO-1212-101063
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.