



Guide to the Sarbanes-Oxley Act:
IT Risks and Controls

protiviti®
Independent Risk Consulting

Guide to the Sarbanes-Oxley Act: IT Risks and Controls

Frequently Asked Questions

protiviti®
Independent Risk Consulting

Business Risk

Technology Risk

Internal Audit

Table of Contents

Page No.

Introduction1

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

- 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. Is it possible to rely solely on manual controls, negating the need to evaluate IT risks and controls?4
- 4. How should Section 404 compliance teams define “IT risks and controls”?5
- 5. How does management identify and prioritize IT risks?6
- 6. What guidance does COSO provide with respect to IT controls?6
- 7. 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
- 8. How do COSO and CobiT facilitate a Section 404 compliance effort?7
- 9. If a 404 project strictly and only follows CobiT, will the project be compliant with the Section 404 compliance efforts?7
- 10. Should management consider other IT control guidelines and standards, such as ISO/IEC 17799, ITIL and CMM?8
- 11. Overall, what are the key areas that must be considered when evaluating IT controls?8

IT Control Considerations in Relation to Business-Process Controls

- 12. How does management get started using the approach outlined in Question 1?9
- 13. When should IT controls be considered during the overall Section 404 project?10
- 14. How does an ERP solution impact the evaluation of IT?10
- 15. How does a shared-service center impact the assessment of internal control?10
- 16. How does outsourcing of IT activities impact a company’s control evaluation approach?11

Entity-Level Considerations

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

Table of Contents (continued)

Page No.

Activity / Process-Level Considerations – General Control Issues

- 25. What are “general IT controls”?15
- 26. What types of controls are “general IT controls”?15
- 27. What does the Section 404 compliance project team look for when evaluating security administration?16
- 28. What does the Section 404 compliance project team look for when evaluating application change controls?17
- 29. What does the Section 404 compliance project team look for when evaluating data management and disaster recovery?18
- 30. What does the Section 404 compliance project team look for when evaluating data-center operations and problem management?19
- 31. What does the Section 404 compliance project team look for when evaluating asset management? . .20

Activity / Process-Level Considerations – The Role of Application and Data-Owner Processes

- 32. Who are the application and data owners?22
- 33. What are the roles and responsibilities of the application and data owners in relation to the IT organization?22
- 34. What process should the application and data owners have in place to facilitate compliance with Sections 404 and 302?22
- 35. What processes should be in place with respect to establishing proper security and segregation of duties?22
- 36. What processes should be in place with respect to periodic review and approval of access to critical and/or sensitive transactions and data?23
- 37. What processes should be in place with respect to business-impact analysis and continuity planning?23
- 38. 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?24
- 39. 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
- 40. 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

- 41. What are the application-level control considerations?25
- 42. How does the Section 404 compliance project team determine the critical applications for each key business process?25
- 43. How should the Section 404 compliance project team integrate the consideration of application-level controls with business-process controls at the activity/process level?26

Table of Contents (continued)

Page No.

- 44. What should management do if the Section 404 compliance project team finds strong application controls at the business-process level?26
- 45. What should management do if the Section 404 compliance project team finds weak IT process controls at the application level?26
- 46. How does management evaluate controls over spreadsheets and other technology tools deployed by users during the financial reporting process that are not subject to the general control environment?26

Documentation

- 47. 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?27
- 48. How should the Section 404 compliance project team document the IT controls at the entity level?27
- 49. How should the Section 404 compliance project team document the IT controls for the IT general controls at the activity/process level?28
- 50. How should the Section 404 compliance project team document the IT controls for the processes controlled by application and data owners and for the specific application areas?28
- 51. Given the emphasis the recent PCAOB exposure draft placed on the “initiating, recording, processing and reporting” of transactions, what is the best way to document transaction flows?28

Testing

- 52. How are IT controls tested?28

Addressing Deficiencies and Reporting

- 53. How should management address deficiencies and gaps in IT controls?29
- 54. How will the external auditor view IT controls during the attestation process?29

- About Protiviti Inc.**30



Introduction

In July 2003, Protiviti published the second edition of its well-received *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*. This guide, which addresses frequently asked questions about Section 404 of the Sarbanes-Oxley Act (“SOA” or “Sarbanes-Oxley”), was updated to reflect the SEC’s final rules. Section 404 requires management to file an internal control report with its annual report. The internal control report must articulate management’s responsibilities to establish and maintain adequate internal control over financial reporting and management’s conclusion on the effectiveness of these internal controls at year-end. The report must also state that the company’s independent public accountant has attested to and reported on management’s evaluation of internal control over financial reporting.

Guide to the Sarbanes-Oxley Act: IT Risks and Controls is a companion to Protiviti’s Section 404 guide. This new IT guide presumes that the reader understands the fundamental requirements of Section 404 and internal control evaluation and reporting, as detailed in Protiviti’s *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*. Issue 10 of *The Bulletin*, “Technology Risks and Controls: What You Need to Know,” provides an executive summary of the points in this publication for Section 404 project sponsors and other interested parties, including C-level executives and directors.

This publication provides guidance to Section 404 compliance project teams on the consideration of information technology 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 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 Protiviti’s 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 advisors 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.

Protiviti Inc.
December 2003

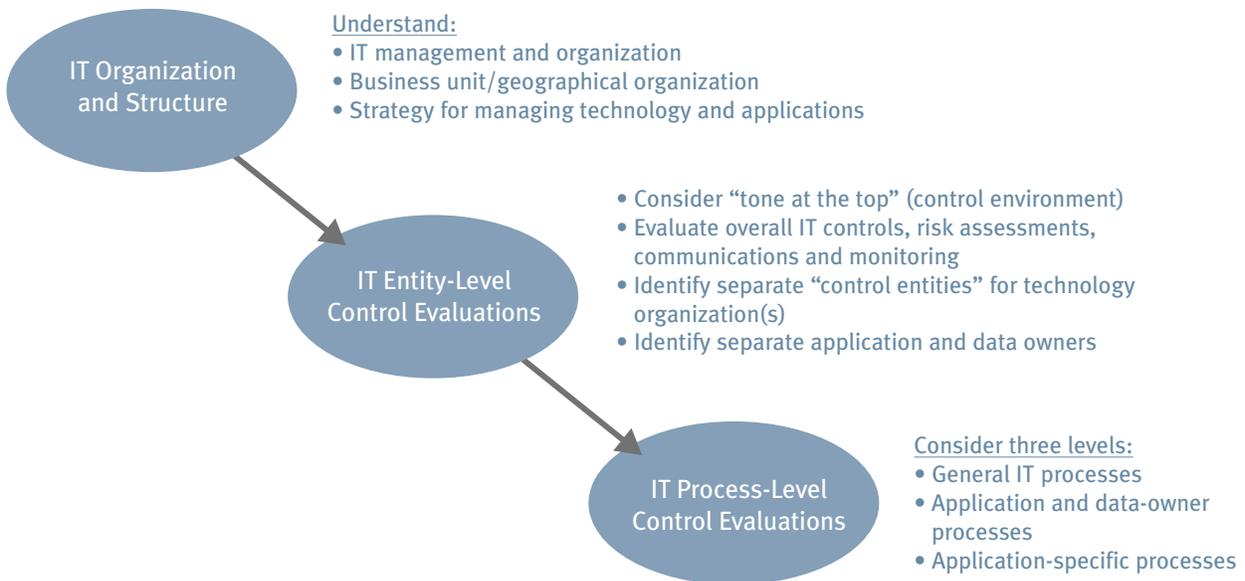
Overall IT Risk and Control Approach and Considerations When Complying With Sarbanes-Oxley

The impact of information technology (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 information technology when evaluating internal control, 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?

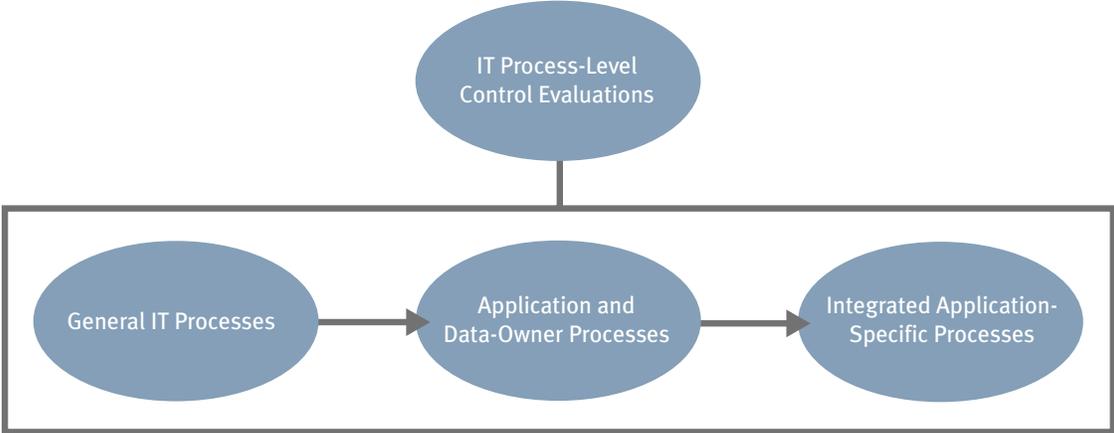
The obvious answer is “yes.” The rationale, a definition of key terms and each element of our suggested approach will be discussed in detail in the pages that follow. However, we have outlined this approach in order to present the context and “end game” for the IT risk and control evaluations.

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. 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 and extent 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 Processes

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 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 management and disaster recovery
- Data center operations and problem management
- Asset management

Application and Data-Owner Processes

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)
- Confirm/review access to critical transactions and data
- Develop and maintain business-impact analysis/business-continuity planning
- Develop and maintain business owner change control

Integrated Application-Specific Processes

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. 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.

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

- Application-programmed controls
- Access controls for critical transactions and data
- Data-validation/error-checking routines
- Error reporting
- Complex calculations
- Complete and accurate reporting
- Critical interfaces

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 often develop, maintain and have access to hardware, software and other parts of the technology environment. Unauthorized actions of 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. Is it possible to rely solely on manual controls, negating the need to evaluate IT risks and controls?

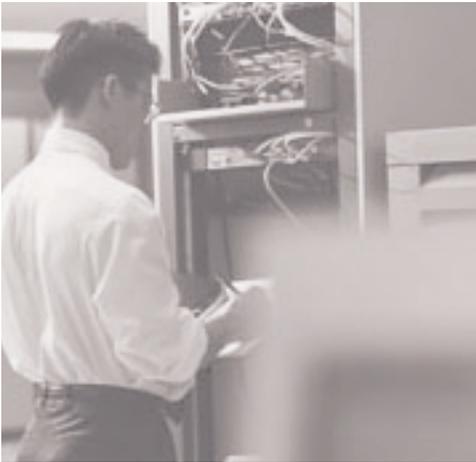
No, not if your company has any accounting systems, unless the accounting system is very simple, used mainly for compilation and the data is easily validated by the users of the system. The PCAOB issued its proposed auditing standard in October 2003 with several specific references to IT systems and the IT environment. While the PCAOB's release was in the proposal stage at the time this publication went to print, we do not expect any substantive changes in the Board's positions with respect to IT-related matters given

the importance of IT to today’s business and internal control environment. 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 “tracing transactions through the information systems relevant to financial reporting.” The PCAOB also states elsewhere that the auditor must “understand the flow of transactions, 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.

With respect to identifying relevant financial reporting assertions, the PCAOB indicates there are a number of factors in determining whether an assertion is relevant. For example, the Board includes “the nature and complexity of the systems, including the use of information technology by which the company processes the controls information supporting the assertion.” The Board also indicates the auditor must consider “the extent of information technology involvement in each period-end financial reporting element” when evaluating the period-end financial reporting process. Finally, the PCAOB requires the auditor to perform walk-throughs of significant processes. In this connection, “the auditor should trace all types of transactions and events ... from the origination through the company’s information systems until they are reflected in the company’s financial reports.” The Board goes on to state that walk-throughs “should encompass the entire process of initiating, recording, processing and reporting individual transactions.”

Given the numerous references to applications and the related IT controls, it should be crystal clear that the PCAOB considers IT and the IT-related controls a significant aspect in the evaluation of internal control over financial reporting. Clearly, auditors will be concerned with IT. The IT-related controls cannot be ignored nor can they be given only minimal consideration in most, if not all, of today’s businesses.

Some may argue that when there are poor IT controls, there is no need to document and evaluate them. We believe that even when there are poor IT controls, they should be evaluated. If 404 compliance teams have knowledge as to where control weaknesses exist, they will more effectively identify the nature and extent of the irregularities that could exist. This type of risk assessment will enable the project team to evaluate the appropriate compensating controls and, where necessary, the additional controls designed to detect and correct the specific errors at the source where they are most likely to occur.



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

Section 404 compliance project teams should consider those risks and controls that either (a) exist through technology (programmed controls within applications, for example), or (b) impact the integrity of processing or data. 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 two broad areas — general controls and application controls.

General 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. In other words, general controls prevent certain events from impacting the integrity of processing or data. (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 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.

5. How does management identify and prioritize IT risks?

The framework and approach for identifying and prioritizing risks should be the same overall framework and approach as used for identifying and prioritizing 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.

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 completeness and accuracy, consistency, and timeliness of financial reporting objectives), and to the proper access to data programs and specific transactions (which supports achievement of the authorization objective and the access to assets objective). Developing an understanding of how these technology areas impact (or could possibly impact), either directly or indirectly, achievement of the financial reporting assertions helps to focus the risk and control evaluations that need to be performed in the general and application controls areas.

6. 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.

(There are specific discussions of IT controls in the Internal Control – Integrated Framework in the "Control Activities" and "Information and Communications" sections.)

7. 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 CobiT framework is composed of the IT processes that make up a large part of the “general 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 404 approach must focus primarily on the achievement of the assertions that are inherent in reliable financial reporting.

CobiT was developed and intended for use in the achievement of the broader definition of COSO’s overall internal control objectives. If a Section 404 compliance project team decides to use the CobiT framework, specific consideration should be given to understanding how the company’s IT organization is structured so that CobiT’s objectives can be matched with the entity’s IT organization and structure. In addition, there should be a linkage created between the CobiT objectives and the financial reporting assertions. By creating this linkage, there would be a direct relationship between the financial reporting risks and achieving the CobiT objectives.

In October 2003, ISACA and the IT Governance Institute published a white paper, “IT Control Objectives for Sarbanes-Oxley - The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting.” In this document, ISACA and the IT Governance Institute attempted to apply the CobiT framework and objectives to the financial reporting objectives of Sarbanes-Oxley. The white paper presents an overall discussion of IT controls and then lists the control objectives relevant to Sarbanes-Oxley compliance efforts. The control objectives presented in this document have resulted in an important contribution to the auditing literature because they focus the overall control objectives in the broader CobiT framework on those objectives germane to Section 404 compliance efforts. However, the white paper states, “A one-size-fits-all approach is not the way to proceed. Each organization may want to tailor it to fit its specific circumstances.” We believe this approach is indeed the appropriate one, as each entity must tailor any approach to its particular organizational structure, processes and risks.

8. 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 the framework in the final Section 404 rules. CobiT also provides useful guidance and background material, and may be considered in the execution of a Section 404 compliance project.

9. If a 404 project strictly and only follows CobiT, will the project be compliant with the Section 404 compliance efforts?

As discussed in Question 7, 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 that related to 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 41-46 in order to fully comply with the 404 compliance efforts.

As discussed in Question 7, if the approach outlined in the new IT Governance Institute publication is followed, it must be tailored (a) to the specific organization, (b) around the specific applications that can significantly impact the reliability of financial reporting information and disclosure, and (c) to the IT-related and application and data-owner processes that support those applications.

10. Should management consider other IT control guidelines and standards, such as ISO/IEC 17799, ITIL and CMM?

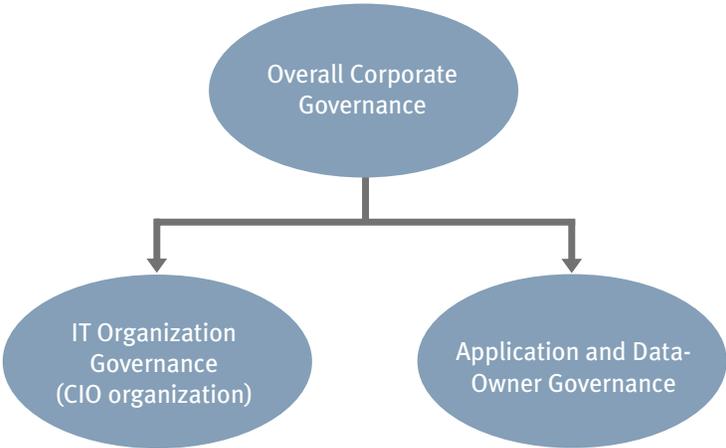
In addition to CobiT, there are a number of frameworks and materials that provide guidance on risk and controls in the IT area. Each of these frameworks offers specific guidance aimed at assisting organizations in “improving” their IT operations and processes. In addition, each framework provides excellent 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.

11. 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 impact 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 17 through 31.)

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 32 through 40.)

IT Control Considerations in Relation to Business-Process Controls

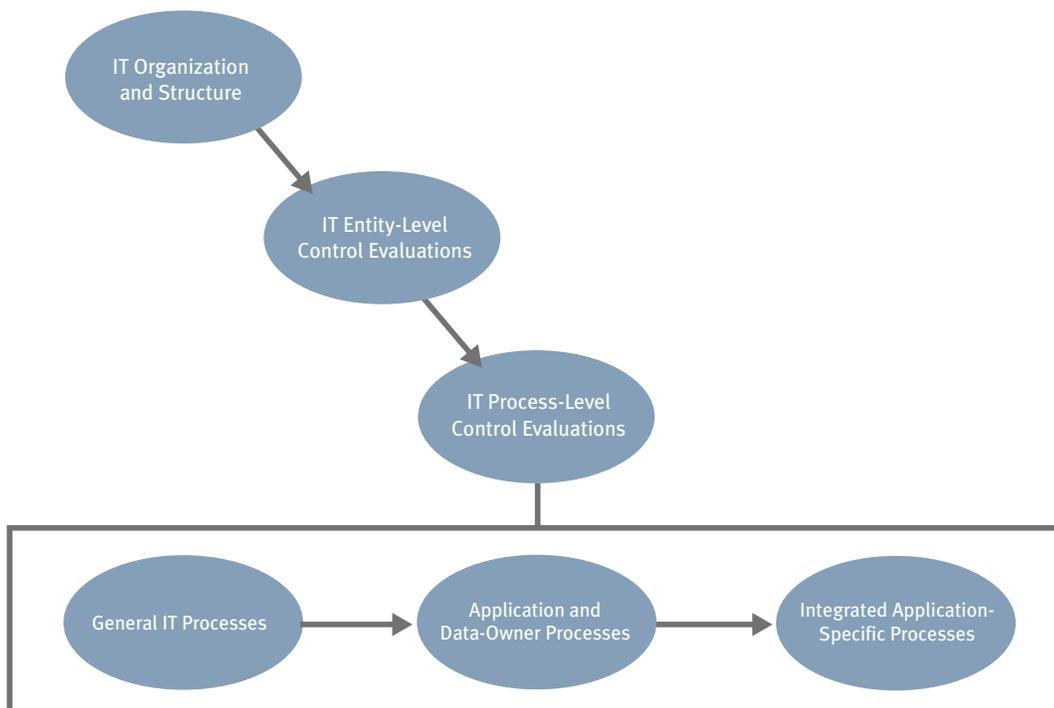
Since technology today is integrated more than ever into business processes, technology-specific controls, i.e., those embedded and designed into the applications that support the processes, must be considered when evaluating controls at the process or activity level. In most cases, there is significant 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. The questions 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.

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

The approach outlined in Question 1 provides management with the overall framework to begin its IT risk and controls evaluation. 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 Question 1, presents a practical way to begin considering IT risks and controls. 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.

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 controls (see Question 25) that provide assurance of processing and data integrity for the key applications. Once those components and general controls are identified, the associated documentation and evaluation work is linked to the associated business processes (as well as to the related applications).



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

The IT risk and controls evaluation should start at the same time as the overall Section 404 compliance project. It is critical this evaluation be done as early as possible in the 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 the controls over business processes.



The nature of the strengths and weaknesses in these entity and general IT controls will determine the level of application and business-process controls that 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 the general controls area of computer-security administration would require increased emphasis on documenting and evaluating additional detective (or supervisory or monitoring) controls at the business-process level. However, if strong preventive computerized 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.

14. 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. 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 ERPs 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.

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

A shared-service environment has some of the characteristics discussed in Question 14 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 25 through 31, 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.

16. How does outsourcing of 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. 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 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, etc.). 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. The PCAOB has 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 through either an SAS 70-type report provided by the outsourcer (assuming the issues noted below are addressed), or by having independent testing performed by the company's designee (e.g., internal audit, outside consultant, etc.).

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

- The contents of an SAS 70 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 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.
The service organization merely executes directions given by the user organization, consistent with the view that under most outsourcing arrangements the user is buying expertise and competence and not transferring process risk. Therefore, the user organization's controls will need to be evaluated and tested along with the service organization's controls.
- In the past, SAS 70 reports typically were 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 SAS 70-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 SAS 70-type report is to be used by management, there are several considerations to keep in mind:

- First, a reading of an SAS 70 report clearly indicates that it is an auditor-to-auditor communication, so it is possible that the Auditing Standards Board did not intend for it to be used for management reliance from a regulatory standpoint. While this may not be an issue, management should consult with legal counsel to review the legal aspects of this reliance. If the outsourcing service agreement is

appropriately modified to articulate the SAS 70 report requirements, then the letter and the reporting relationship can be conformed to satisfy those requirements.

- Second, the scope of the SAS 70 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. For example, the SAS 70 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, output, 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 financial statements.
- We expect companies and their service providers to capitalize on the SEC's extension of the Section 404 transition period by renegotiating their service agreements. For example, management may specify its testing requirements in the outsourcing agreement, and the report issued by the service provider's auditor can refer to those requirements. Many outsourcing service providers may, in fact, look to coordinate these types of requirements with all of their clients and their independent accountants in order to avoid an impracticable and time-consuming case-by-case approach.
- 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 report year-end.¹ An SAS 70 report may cover either a point in time or a period of time, with a warning about projecting the results into the future. 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 SAS 70 report differs significantly from that date? At a 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., quarterly) SAS 70 reports that they can provide to interested user organizations.

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 SAS 70 report is a good starting point, but the SAS 70 reporting process will 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 SAS 70 reports for management's purposes.

The guidance given for questions under the headings: Activity/Process Level Considerations - The Role of Application and Data Owner Processes and Activity/Process Level Considerations - Application Level Controls should be fully considered. These areas cannot be outsourced effectively – they remain the direct responsibility of the entity's management.

¹ As explained in our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements*, a point-in-time assessment is required as of the end of the fiscal year to comply with Section 404. Companies meeting certain conditions as of the end of their fiscal year (such as a market capitalization of at least \$75 million as of the last business day of the most recently completed second fiscal quarter), are deemed to be "accelerated filers" and must comply with Section 404 beginning in years ended on or after June 15, 2004. Other companies, such as "small-business issuers," must comply beginning in years ended on or after April 15, 2005.

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 the 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 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.

17. What is the IT organization?

As noted in Question 11, 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-management and disaster-recovery processes, and the data center operations and problem management areas. 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.

18. 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 17). 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.

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

In Question 18, 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 differs 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.

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

As discussed in Question 11, 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 27-31 and 35-38. 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.

21. 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 has made effective mitigation of risks and implementation of controls 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 controls activity/process level and at the application level.

22. How would management know if the entity 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, as well as 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 usually will 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.

23. 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 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 effective achievement of financial reporting internal control objectives.

24. What are examples of a weak entity 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 management and disaster recovery, data-center operation, problem management, and asset management.

25. What are “general IT controls”?

General 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 controls level” refers to processes impacting multiple applications; therefore, the controls over those processes are general controls.

General 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.

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

General IT controls are pervasive or overall process-level controls. COSO defines general controls as, “Policies and procedures that help ensure the continued, proper operations of computer information systems. They include controls over data-center operations, systems software acquisition and maintenance, access security, and application system development and maintenance. General controls support the functioning of programmed application controls. Other terms sometimes used to describe general controls are general computer 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 management and disaster recovery, data-center operations, problem management, and asset management. These IT processes will have the types of controls one would typically find in all business processes. There will be a combination of manual and systems-based control activities. 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 and accuracy, consistency, and timeliness of financial reporting objectives), and the proper access to data programs and specific transactions (which directly relates to the authorization objective and to the access to assets objective).

Our responses to Questions 27 through 31 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 27 through 31, 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

27. 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 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 sub-processes 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.

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 controls level (as explained in Question 25) 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 35 and 36) and at the application-specific level (as explained in Question 41) to fully evaluate the objective.

Impact of Weak Controls

- a) Weak general controls over access to information assets (transactions, data and systems resources) cause 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 proper, how would I know if an unauthorized modification, addition or deletion has been made?”
- b) If there are overall weaknesses in the general 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.

28. 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 include appropriate procedures to initiate, monitor, test, approve and move 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 disclosure.
- 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. This may allow for intentional or unintentional changes to applications or data that could go undetected through normal control activities.

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.
- 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.

29. What does the Section 404 compliance project team look for when evaluating data management and disaster recovery?

Background

Data management is critical to the effective and efficient workings of a technology organization. For discussion purposes, "data management" relates to the processes around the backup, recovery and restoration of data. 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 management also includes the considerations around the criticality of the application, and the appropriate timing and frequency of the back-up process. The frequency and reliability of this process often reflect a cost/risk/benefit judgment around how much data (or how many transactions) a company can afford to lose without negatively impacting the business (in many different ways).

The process and procedures around disaster recovery are related to data management. Business continuity and IT disaster recovery relate mainly to the company's abilities to continue to accurately and timely file its required financial and other reports with the SEC under the Commission's rules and regulations. As discussed in Question 37, disaster recovery needs to be responsive to a company's business-impact analysis and business-continuity plans.

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. As noted in Question 37, this practice is an important aspect of managing business risk.

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 and disaster-recovery processes.
- 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 the business-continuity and disaster-recovery plans are not comprehensive and up-to-date.

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.
- 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 and appropriate action taken.

30. What does the Section 404 compliance project team look for when evaluating data-center operations and problem management?

Background

The data-center operations and problem-management areas could impact the applications and data in much the same way as the data-management process discussed in Question 29. These processes impact the integrity of data and the completeness and accuracy of processing. The data-center operations and problem-management areas impact the normal operation of the applications and intercede when problems occur. In these instances, such as interfaces not processing completely or programs interrupted, there is a higher risk that processing of transactions or data may be incomplete or inaccurate. The computer-operations and problem-management areas are designed to provide procedures to appropriately handle these issues. These processes often involve an interface and communication with the data and application owners for resolution of issues and problems.

In addition, the personnel in these areas often are granted extensive access to the data and applications in order to troubleshoot problems as they arise. This introduces additional risk that transactions or data have been accessed outside normal and formally approved processing channels.

Impact on Financial Reporting Assertions

- a) The completeness, accuracy and consistency of reporting can be impacted directly by computer operations and problem-management processes.
- b) Access to information assets is directly impacted if computer-operations and problem-management areas are not appropriately restricted and monitored.

Impact of Strong Controls

- a) There is assurance that these processes do not impact the completeness, accuracy and consistency of processing.
- b) 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) There is a need to document and evaluate compensating control procedures related to potential errors or omissions that may result from weaknesses in the data-operations or problem-management areas. More detailed detective and monitoring controls are needed when there are overall weaknesses in the computer-operations area. These additional procedures should include steps that would alert users to potential problems (triggered, for example, when there are applications issues to be addressed by computer-operations personnel), so that additional manual detective and monitoring controls could be specifically implemented.
- b) 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 computer-operations and problem-management 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.



31. What does the Section 404 compliance project team look for when evaluating asset management?

Background

The asset-management area is an important one to IT organizations today. Not only are the costs of hardware and software rising, but this area is one that traditionally has been poorly managed. From the standpoint of a Sarbanes-Oxley Section 404 compliance project, the important aspects of asset management relate to the proper accounting for IT asset acquisition, operations and retirements. In this area, there are also potential issues around the appropriate use and monitoring of software licenses. The improper use of software could result in unrecorded liabilities and potential

disclosures around the proper use of software and compliance with software usage laws. Another area of concern from a public reporting perspective is the periodic substantiation of asset existence and evaluation of recorded balances as well as the realization of assets over their useful lives.

The main reporting issues surrounding the management of IT assets are not dissimilar to those relating to all fixed assets. The reason they are selected for this discussion is that the process and accounting for these assets are

often associated with processes in the IT organization that are separate and distinct from the oversight and procedures for other fixed assets. IT assets include hardware and software along with user desktops and workstations that often are significant investments in today's technology environment.

Impact on Financial Reporting Assertions

- a) Assets should be properly reported in the financial statements. This means that they have been properly capitalized or expensed in accordance with generally accepted accounting principles and that any capital leases have been properly accounted for. In addition, any and all required disclosures are reported in the financial statements.
- b) Asset balances are periodically substantiated through observation or some other means to verify their existence. In addition, the carrying value of the assets is periodically evaluated and the estimated useful lives of the respective asset categories are reviewed for reasonableness.
- c) Access to the assets is safeguarded in an appropriate manner to provide reasonable assurance of existence as of any given reporting date.

Impact of Strong Controls

- a) There is assurance that the IT assets are properly stated and accounted for; the balances have been periodically evaluated and substantiated.
- b) There is assurance that any necessary disclosures that may be required (around lease obligations, commitments and contingencies related to potential legal and regulatory matters, etc.) are appropriate, and the necessary support has been documented appropriately.

Impact of Weak Controls

- a) Asset balances and related expenses may not be properly stated. Therefore, compensating and additional controls may be necessary. The compensating controls would concentrate on substantiating balances and the existence of assets. They may include various ad hoc and stop-gap controls over the evaluation of asset balances.
- b) There may be inadequate support for and identification of disclosures relating to fixed assets. Additional controls and procedures would be necessary to ensure disclosure information is appropriately identified and supported. Over the longer term, a well-defined disclosure process is most likely the way to assure achievement of relevant financial reporting assertions. The short-term fix, however, may be manually intensive and ad hoc in nature.

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.

32. Who are the application and data owners?

Typically, application and data owners are part of the business process. Often they also own the overall business process from a controls design and operations perspective. The overall process owner can delegate this ownership to someone, but the process owner must clearly communicate what is expected out of the delegate. The application and data owner must take responsibility to understand, design and maintain the controls within the application. These individuals must understand computerized controls so that they can knowledgeably design such controls and communicate these needs to IT personnel. The application and data owner 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 general controls for certain IT processes.

33. 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 related internal controls, with 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 adjustment 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 the internal control objectives over financial reporting.

34. What process 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. 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.

35. 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 owners' responsibility to document the system requirements for application security purposes.

On an ongoing basis, it is also the application and data owners' responsibility to update and maintain this "transaction and segregation list" as the various applications evolve and change.

36. 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 owners' 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 27), a root-cause analysis should be undertaken and the matters resolved on a timely basis.

37. What processes should be in place with respect to business-impact analysis and continuity planning?

The application and data owners should be the same as the business-process owners or, at a minimum, be a direct report to them. It is the process owner who has the overall responsibility for the appropriateness of the business-impact analysis and for the development and maintenance of the business-continuity plan resulting from the impact analysis. It is the responsibility of the IT organization to develop a disaster-recovery plan to enact the business-continuity plan.

An important aspect of managing a company's overall business risk, including its continuation as a going concern, is its ability to effectively address business continuity and disaster recovery. In light of the events of September 11, 2001, this is clearly an important business risk to be managed. The power outage of 2003 in the eastern United States points out the vulnerabilities of organizations dependent on their country's critical infrastructure (i.e., telecommunications, utilities, water supplies, banking systems, transportation, etc.).

The SEC has issued a policy statement setting forth its view that a self-regulatory organization operating trading markets (SRO Markets) and electronic communication networks (ECNs) should apply certain basic principles in its business-continuity planning. For example, the SEC's principles include:

- Planning for the resumption of trading no later than the next business day following a wide-scale disruption
- Geographic diversity between primary and backup sites
- Assuring the full resilience of important shared information systems (such as the consolidated market data stream)
- Confirming the effectiveness of backup arrangements through testing

The SEC is requesting each SRO Market and ECN to implement plans reflecting these principles as soon as practicable, and has set the end of 2004 as the timeframe for getting it done. This activity indicates that even regulators are responding to these risky times by advocating standards for business-continuity planning.

Sections 302, 404 and 906 of Sarbanes-Oxley require companies to design and maintain procedures and controls to identify in a timely manner all material information for action and disclosure, and provide fairly presented financial information and disclosure to the public in periodic and current reports. There is a presumption in financial reporting that public companies will be able to meet their reporting deadlines and have available all material information needed for fair presentation and disclosure, including the update of accounting estimates with current and reliable information. These requirements create obligations suggesting a need for companies to have an adequately documented business-impact analysis, with management's agreement and sign off, addressing the company's broader business risks as well as its regulatory and compliance risks, including those risks relating to public reporting. Once an adequate business-impact analysis is completed, the company can evaluate whether changes are needed in its business-continuity and disaster-recovery plans. These plans must be kept up to date and periodically tested to maintain their adequacy in ensuring the company can fulfill its obligations under Sarbanes-Oxley.

38. 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.

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.

39. 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 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 environment, both the general IT controls and the application and data-owner controls must be designed and operating effectively.

40. 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 39 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 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.

41. What are the application-level control considerations?

Application-specific control considerations relate primarily to the controls programmed within an application (the so-called “programmed controls”) 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. Examples include computerized edit checks of input data, numerical sequence checks and manual procedures to follow up on items listed in exception reports.”

For purposes of responding to this question, we will concentrate on the programmed procedures and controls. These programmed controls assure the complete, accurate, timely and proper transaction processing and reporting of transactions by applications related to financial reporting. These control considerations arise around critical business process flow points at which the application:

- a) Makes calculations
- b) Performs data validation and edit checks
- c) Interfaces electronically with other systems
- d) Sorts, summarizes and reports critical financial information that is relied upon as complete and accurate by management
- e) Limits access to transactions and data

These application-level control considerations arise around the proper design of the application controls and the fact that they operate as and when intended by management. They also are based upon the presumption that neither the programmed controls are changed nor the application around the programmed controls is changed, such that the controls no longer perform as or when intended by management.

The application level is also where the segregation of incompatible duties is a critical issue. In the application systems, this segregation is achieved through the limitation of access to transactions and data based on strict business rules. These rules prevent a user from having access to transactions or to data that are incompatible from an internal control standpoint. For example, if the same person can set up a vendor and then initiate payment of invoices to that vendor, the two functions are incompatible and should be segregated.

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

Part of the understanding of the business processes that must be undertaken is identifying the applications that transact or interact with the critical processes impacting the priority financial reporting elements. As part of understanding the process, the project team should document the key inputs, processing activities and process outputs, which should include a description or map of the application systems that are an integral part of the process. In other words, the project team should select the applications that (a) are integral to making the process perform, and/or (b) expose the process to increased risk of not achieving the relevant financial reporting assertions.

Some factors to consider include:

- a) The volume of transactions processed (the higher the volume, the more critical the application)
- b) The dollar amount of the transactions (the larger, 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 of the calculation (the more complex, the more critical the application)
- d) The sensitivity of the data and transactions (the more sensitive, the more critical the application)

In addition, when the applications are being prioritized, it is important to identify all applications used, including worksheets, spreadsheets, user-database programs (such as Access), and web-based programs and calculators. These types of programs need to be documented and the change control, security, back-up and recovery procedures need to be separately evaluated, particularly if the applications have an impact on the overall financial reporting process.

43. How should the Section 404 compliance project 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 business-process controls. The project team needs to consider the process risks and key control points, and determine which controls are programmed application controls and which controls rely upon computer-generated information to operate effectively. The team then needs to consider what steps are necessary to fully understand and document the key controls within the application (i.e., use a specialist to understand the design and operations of application systems).

Controls and process activities in many situations depend upon reliable computer-generated information to be identified and understood. For purposes of justifying reliance on these controls and activities, the Section 404 compliance team should assess the controls surrounding the applications generating the information. This assessment will often be linked to the impact of effectively functioning general controls, as discussed in Questions 25 through 31.

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

If there are strong application level controls, then generally there should be strong preventive and programmed detective controls in place. In such 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.

45. What should management do if the Section 404 compliance project team finds weak IT process controls at the application level?

If there are weak application-level controls, 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 not depend on computer processing to operate effectively. 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.

46. How does management evaluate controls over spreadsheets and other technology tools deployed by users during the financial reporting process that are not subject to the general control environment?

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, back-up and recovery which 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, back-up 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.

Documentation

Documentation is important in an evaluation of internal control over financial reporting. 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.

47. 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 is what documentation is needed to evidence functioning of the program and its controls. The second is what technical documentation is necessary to ensure that the application can be maintained such that the integrity of processing and controls can be assured.

These two considerations obviously are related. Application documentation should specify where and how key components of the application operate. The key components should include the critical application controls discussed in Questions 41-46. The documentation can take many forms: process flows and narratives, flowcharts which show the steps during program processing, other technical documents which show data relationships and database designs. The technical documentation should be such that an unfamiliar (but technically competent) programmer could understand how the program operates, and its critical interfaces, data handling and security features, and on a reasonable basis perform the required maintenance.

Documentation which 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 may not be appropriate and the guidance in Questions 28 and 38 on weaknesses in change management should be considered.

48. How should the Section 404 compliance project 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.



49. How should the Section 404 compliance project 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.

50. How should the Section 404 compliance project 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 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 by an applications-control expert as needed. 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.

51. Given the emphasis the recent PCAOB exposure draft placed on the “initiating, recording, processing and reporting” of transactions, what is the best way to document transaction flows?

We believe the best way to document transaction flows is through application and data-flow diagrams. These diagrams provide a picture of the significant data flows through the company’s various applications from the point of origin until they ultimately affect the financial statements and disclosures. We believe there is a need to begin these diagrams initially at a high level and then provide more detail for the most significant transactions and applications. In the more detailed diagrams, it would be useful to highlight the inputs, processing and outputs, as this documentation demonstrates the understanding that the PCAOB requires the auditor to obtain of the “significant business processes” through walkthroughs.

Testing

Like all other controls, IT controls must be tested to ascertain they are operating as designed. The second edition of our *Guide to the Sarbanes-Oxley Act: Internal Control Reporting Requirements* provides guidance on testing. Our response to the question below expands on that guidance to address IT-related controls.

52. 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, inspection, observation and reapplication and/or reperformance. 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, inspection and observation because reperformance and reapplication cannot typically be accomplished for many of these types of controls. For the processes in the general 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 for evidence that certain parts of the process were completed (i.e., signatures or other sign-offs on forms, etc.).

Addressing Deficiencies and Reporting

If there are internal control deficiencies, they must be remedied if significant. The second 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.

53. 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. This step may be 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.

54. 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 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. 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.

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 take place.

About Protiviti Inc.

Protiviti is a leading provider of independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. Protiviti assists companies with Sarbanes-Oxley compliance efforts by helping them to document their internal control over financial reporting and disclosure controls and procedures, design and recommend improvements in processes and controls, and organize and manage projects for complying with the Sarbanes-Oxley Act.

Protiviti, a wholly owned subsidiary of Robert Half International Inc. (NYSE: RHI), has more than 30 locations in North America, Europe and Asia.

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 defining of the audit universe and performing the risk assessment, the annual planning and scoping process to the execution of all types of technology-related internal audits. We also provide consulting services around the technology risk and control aspects of Sarbanes-Oxley compliance. 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.

We help companies understand and evaluate technology 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 Technology Risk Consulting Services

Security and Privacy Solutions

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 enterprisewide 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

Protiviti is the leading provider of independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of internal audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.