The Bulletin

protiviti®
Independent Risk Consulting

VOLUME 1 ISSUE 10

# Technology Risks and Controls: What You Need to Know

Disclosure and internal controls seem to be commanding the headlines these days, with particular emphasis on complying with Sections 302 and 404 of the Sarbanes-Oxley (SOA) legislation. Where do controls over information technology (IT) fit in this picture? Why is IT important? Why should directors and executives care? This issue of *The Bulletin* addresses these and other questions relating to technology risks and controls.

## What's required?

The impact of IT must be considered carefully during an evaluation of internal control over financial reporting. There are unique risks to be considered. The controls that mitigate these risks are important because of their pervasive effect on the reliability, integrity and availability of processing and relevant data.

## What are IT controls?

IT risks and controls must be evaluated from the top down. There are general controls and there are application controls.

*General controls* typically impact multiple applications in the technology environment and prevent certain events from impacting the integrity of processing or data. Computer operations, physical and logical security, program changes, systems development and business continuity are examples of processes where general IT controls reside. These IT controls are "pervasive" because they can have an impact on the organization's achievement of financial reporting objectives germane to many of its processes.

*Application controls* are more specific to individual business processes. These controls include policies and procedures designed and implemented in the business areas by the respective owners of the applications and data. They also include so-called "programmed controls" within the applications that perform specific control-related activities, such as computerized edit checks of input data, numerical sequence checks, validation of key fields, and exception reporting and related follow up on exceptions.

## Why are controls over IT important?

IT plays a key role in the financial reporting process. Many economic events are captured in application systems. These transactions are summarized and reported by applications to form the basis for preparing financial statements. For example, the revenue-reporting process in a long-distance telecom company begins with the capture of calls by individuals and businesses. The company bills for these calls based on the data from the telephone-usage system and the contractual terms maintained in the billing system. The individual billings are summarized and the corresponding revenue is recorded in the general ledger. The general ledger for the operating unit is consolidated with the results of other business units by the consolidation system, which then produces the consolidated revenue amounts reported in the financial statements. Thus applications perform many of the routine steps and calculations that are critical to financial reporting. The data in these applications and the calculations they perform must have integrity to ensure fairly presented and reliable financial statements.

Ignoring IT controls is not possible. Almost without exception, every company utilizes IT to record, summarize and report transactions. Unless a company has no computers or its operations are both small and simplistic, IT controls always must be considered when evaluating internal control over financial reporting. Even some manual controls are dependent on technology, e.g., comparing a computer-generated report to something, making sure the general ledger and sub-ledgers agree, using performance metrics to monitor certain activities, etc.

## What are examples of key risks in an IT context?

Given IT's vital role in the financial reporting process, the integrity of the programs (or applications) and data are critical control elements of the internal control environment. Integrity of applications addresses several assertions inherent to processing and reporting, such as effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information. These assertions provide a context for assessing IT risks. For example, the *effectiveness* assertion provides that information is relevant to the business process and is delivered in a timely, correct, consistent and useful manner. As another example, the *confidentiality* assertion emphasizes that sensitive information is protected from unauthorized disclosure. These assertions provide a context for assessing IT risks.

IT risks are the events that depict "what can go wrong" to cause failure to meet or achieve the fundamental assertions.

Risks provide a context for evaluating IT and manual controls. For instance, what controls exist to ensure initial data entry is accurate and complete? What controls exist over the technology environment where transactions and other accounting information are stored and maintained? What controls exist to mitigate risks unique to the IT environment? For example, there is a risk that data may be changed through "technical back doors" that exist because of inadequate computer security. The appropriate controls provide assurance that data is changed only in accordance with management's criteria.

## Who are the key players?

The *IT organization* consists of IT operations and the overall governance of the processes impacting IT. The IT organization typically consists of the chief information officer's (CIO) organization and impacts the effectiveness of general or pervasive controls. The CIO, who should be a member of the 404 compliance steering committee, communicates the importance of internal controls within the IT organization, understands and documents the IT organization's role in internal control over financial reporting, and determines where key risks are related to internal control based on how IT processes impact the integrity of applications and data. The CIO also documents controls mitigating these risks and develops monitoring mechanisms to identify control breakdowns on a timely basis.

*Application and data owners* are the business groups interfacing with business-process owners, and are responsible for business and accounting information that is generated by the applications. They decide and design the applications that fit the needs of the processes from a business standpoint, and monitor those applications to ensure they perform as expected. They determine the impact their applications have on key processes and periodically update this assessment. They work with the CIO to establish effective entity-wide controls to mitigate risks impacting the integrity and availability of application processing and data, particularly in such areas as change-control processes, segregation of duties (to promote access security) and business-continuity planning. They also develop and implement monitoring procedures to detect control issues, and ensure that controls over applications and data are effectively integrated with business-process controls.

## Entity-level controls are important

IT risks and controls should be integrated with the overall assessment of financial reporting risks and the controls that mitigate those risks. There are two types of controls – entity-level controls and process-level controls. These controls are designed to reduce IT risks to an acceptable level.

Entity-level controls provide the environment that helps to assure, maintain and monitor processing and data integrity. Overall entity-level controls relevant to IT often would 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. They include the processes used by management, process owners and application and data owners to identify and assess risk. They include the overall organizational structuring considerations around centralized processing and controls, such as shared-services environments. They also include processes for monitoring performance of controls, including monitoring exception reports (e.g., security breaches). Management also should have oversight processes in place to ensure effective control of the specific processes that directly impact the integrity of applications and data.

Management may need to evaluate entity-level controls for multiple locations and units within the organization. Management structure and the span of control are often the primary criteria used to define these entities. For many companies, in considering the organizational structure from an internal control standpoint, the IT organization is a separate entity because it creates its own goals and objectives and is managed as a specific unit. In large entities, there could be multiple IT entities requiring review.

## Process-level controls must be considered

There are three broad areas of so-called process-level controls. The *IT general controls* constitute the IT processes that could have a direct impact on the integrity of applications and data. In order of their relative importance, these processes include application maintenance and change control, security administration, computer operations and problem management, data management, disaster recovery, and asset management.

*Application and data-owner processes* are the business-unit or process-owner activities that directly relate to the integrity of applications and data. In order of their relative importance, these processes include:

- Application maintenance and change control
- Definition and maintenance of application-level security
- Definition and maintenance of roles that must be segregated from one another
- Overall review and approval of security roles, including authorization limits
- Periodic review of personnel possessing "need to have" authority to execute and view critical transactions and data
- Development and maintenance of a current business-impact analysis and business-continuity plan, which should consider the regulatory impact of the SOA rules

Although there are related functions carried out in the IT organization(s) for each of the above activities, there is also a need for the business-process owners to have processes in place to ensure applications supporting business functions and controls are properly designed, maintained and managed in accordance with their requirements. These processes cannot be executed effectively by the IT organization alone.

*Application-specific controls* are programmed into specific applications as control features or to facilitate controls around the business process. In this area, it is important to identify and evaluate the important programmed controls for each business process considered critical to Section 404 compliance. Process owners should obtain an understanding of the application's programmed controls when they evaluate the manual

controls. If automated and manual controls are not evaluated on an integrated basis, gaps in controls or unjustified reliance on undocumented controls may result. Programmed controls assure the complete, accurate, timely and consistent processing and reporting of transactions by financial reporting applications. These control considerations arise around critical process flow points at which the application makes calculations, performs data validation and edit checks, interfaces electronically with other systems, limits access to transactions and data, and sorts, summarizes and reports critical financial information that is relied upon as complete and accurate by management.

These automated controls are premised on two underlying principles:

- They are properly designed and are operating in accordance with management's design.
- Neither the programmed controls nor the application around the programmed controls are changed, resulting in the controls no longer performing as or when intended by management.

## Pay attention to outsourcing situations

When all or part of the IT function or any significant transaction processing is outsourced, it does not alter management's responsibility to assess controls over processing that is 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. 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 (1) processes and applications that the company operates, and (2) processes and applications that the company outsources to external service providers.

With respect to outsourced applications, management may seek from the service organization a report from the service organization's auditor. The service auditor's report must meet certain criteria to be acceptable to the company's auditors. It is also important to understand the terms of the service agreement because it sets expectations as to what is controlled and what is not. Management cannot outsource the application and data-owner roles, as those individuals are responsible for the application-specific controls and how they are used in the business process.

## What if there are deficiencies in IT controls?

In a weak entity-level control environment, overall policies and guidance setting forth expectations for developing and maintaining strong process-level controls often are nonexistent or lacking. Communications emphasizing the need for strong controls are usually not evident. The goals and objectives (and the tone set by management) of the IT organization are often focused on reducing costs and staying within budget, instead of emphasizing service quality or risk management.

If there are weak entity-level controls, the likelihood of consistently strong IT general controls is greatly reduced. While this does not mean that strong controls cannot exist within the company's processes, it does mean that upper management has not communicated clearly the need for such controls, nor is there consistent monitoring of the environment. The lack of leadership at the entity level can foster an ad hoc and inconsistent control environment in which management and process owners may not focus adequately on the need for appropriate IT-related controls.

If a weak control environment results in weak general IT controls or if there are weaknesses in the application and data-owner controls, management will need to evaluate and understand whether there are alternative or compensating controls at the business-process level relating to segregation of duties and the accuracy and completeness of processing. If application-level controls are weak, management must look for compensating detective and monitoring controls. These detective and monitoring controls would need to be highly detail-oriented and extensive in nature and scope. They must not depend on computer processing to operate effectively and must be documented, evaluated and tested.

Weaknesses in the IT environment at the entity level, or in the general or application controls at the process level, may result in a conclusion that there is a significant deficiency or material weakness. For example, in a complex environment with significant transaction volumes, reliance on detective and monitoring controls may not be effective or feasible. This would give rise, at a minimum, to a significant deficiency and possibly even a material weakness in internal control. A material weakness determination will result in an assertion that internal control over financial reporting is ineffective. It also will result in an adverse opinion from the auditor – something no one wants to see happen.

## How are deficiencies addressed?

Depending on the nature and severity of the identified weaknesses, management addresses IT control deficiencies in two ways. First, management performs a gap analysis of the process or control that is either designed or operating ineffectively, and develops an action plan to close the gap. With respect to IT controls, analyzing and closing gaps could take an extended period of time to remedy. Following are two points to consider during the remediation process:

- Internal controls, pervasive and specific, are either preventive or detective. They can be positioned at either the source of the risk (preventive) or downstream from the risk source within a process (detective).
- Internal controls are either applications-based (i.e., programmed controls) or people-based. As transaction volumes and the velocity and complexity of risk increase, applications-based controls are often more reliable than people-based controls. Applications are less prone to mistakes than human beings, if designed, operated, maintained and secured effectively. Applications-based controls often require more time to design and build.

The implication of the above points is that companies should shift their controls design toward a more proactive approach to controlling IT and other risks. This shift requires greater emphasis on preventive and applications-based controls versus the reactive "find and fix" approach embodied in detective controls or the inefficiencies inherent in cumbersome and excessive manual controls. That said, there is often a need for an effective blend of these control types in the overall design.

The second approach to evaluating IT deficiencies, which may be appropriate at least in the short term, is to identify risks that IT control weaknesses have created and document or design appropriate manual compensating controls. A risk analysis of the deficiency and of surrounding mitigating controls may gain the company some time over the short term. However, given the volume and complexity of transactions, compensating controls may not be possible.

### What about the independent auditor's approach?

It is safe to say that the independent auditor will have IT-related risks and controls strongly in mind when evaluating the basis for management's assertions in the internal control report. A weakness in general IT controls potentially could have an effect over significant transactions and accounts. If there are gaps in general IT controls, the external auditors could say that those gaps need to be addressed before they can reach an overall opinion that internal controls are effective. 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, including the security over access by users, before they could attest to 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 any gaps exist.

### Don't forget business continuity

There is a presumption in financial reporting that public companies are 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 reliable, current 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 relating to public reporting. The company's ability to meet its obligations to file timely, complete and accurate reports with the SEC could be impacted if it is not prepared to deal with unexpected events through comprehensive, up-to-date business-continuity and disaster-recovery plans. While 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 ordinarily 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.

### Move beyond compliance

We have focused on the relevance of IT risks and controls to a company's meeting the internal control objectives over the reliability of financial reporting. IT impacts virtually everything a company does in generating information for decision-making. It is difficult to think of any business activity that is not impacted in some way, directly or indirectly, by an effectively functioning IT organization. IT impacts the achievement of operating effectiveness and efficiency and compliance-related objectives as much as it impacts financial reporting objectives. Further, organizations' dependency on IT continues to increase as business models evolve. That is why the reliability, integrity and availability of applications and data should be of paramount concern to executives and directors.

## Key Questions to Ask

### Board members:

- Should the CIO report to the audit committee on the state of the IT internal control environment?
- What do the internal and external auditors think about our IT controls? If the auditors have given us numerous recommendations to improve the company's IT controls, how concerned should we be?
- If we outsource any part of the IT function, how has management exercised its responsibility to assess controls over outsourced processes that are significant to the company's accounting systems and controls?
- How focused is the company's internal audit function on IT? If internal audit resources and audit plans are light on IT, does that create additional exposure to the company?
- How much do we spend on IT relative to our peers? If our spend is significantly less than the industry average, is that a positive or a potential risk?

### Management:

- Does the CIO know what he or she needs to do to foster a strong technology control environment for purposes of complying with SOA Sections 302 and 404?
- Does the CIO submit requests to spend more money, with part of the explanation because additional spend is needed to comply with SOA? If so, how can we know that this is correct?
- How concerned should we be that a publicized hacker or other IT incident will be construed as an internal control deficiency that should have been considered or disclosed in the 302 certification or 404 report?
- If we outsource more or all of our IT organization, how do we fulfill our IT-related 404 compliance issues?
- If we have several new systems projects underway, how does that impact our compliance with SOA?