

Addressing Internal Controls in Your ERP Implementation - Working with Your System Integrator to Engineer Compliance

Despite the already heavy penetration of ERP software in the business marketplace, the parade of major ERP projects and upgrades continues. Many such systems were implemented as “Y2K” solutions over eight years ago. At that time, Congressmen Michael Oxley and Paul Sarbanes were fairly anonymous civil servants. The legislation that would eventually bear their name, and the crisis of confidence that would reshape corporate America, had not yet been envisioned. As “Y2K” era systems near the end of their useful lives, many companies are now launching new ERP implementation projects and conducting major upgrades to keep up with the rapid pace of technology and business change.

Clearly, times have changed with regard to internal controls. Prior to Sarbanes-Oxley (SOX), public companies employed varying strategies related to internal controls. Consideration of internal controls in major enterprise system implementation projects was often an afterthought, or overlooked altogether. SOX Section 404 has brought internal control considerations to the forefront of major system change programs at most public companies.

The major system integration (SI) firms that large companies often use to help deliver enterprise systems are still adapting to a business environment in which internal controls are so important. Some of these firms have struggled to understand the impact SOX has on their work and the associated implications for estimating, planning and delivering major systems. As a result, they may fail to recognize, or severely underestimate, the ERP programs and tasks and deliverables associated with internal controls. These knowledge gaps may lead to budget issues, project delays and compliance risks which further complicate an ERP implementation.

In this article, we will explore the implications of this significant ERP project risk and provide useful guidance to ensure compliance issues are addressed throughout a major system implementation project.

Why Does This Risk Exist?

There are several reasons why an SI firm may overlook internal controls in the ERP proposal, estimating and contracting process. These firms, by necessity, are built around a core of deep technology and software expertise. The senior leaders in these organizations tend to rise up through the ranks of technology implementers and make their living (and keep their jobs) by selling mega-technology deals. The consultants they bring to ERP engagements often have specialized and deep knowledge about specific modules or business functional areas. These consultants may lack a “big picture” perspective on compliance or how the functions and features of the software can be tailored to meet control objectives. Practitioners of internal audit and internal controls tend to rise up through finance, accounting and audit backgrounds. This domain of ERP controls and compliance knowledge has come to be known as governance, risk and compliance (GRC). GRC knowledge cuts across business processes and technology. As a whole, the revenue opportunity associated with GRC consulting projects is dwarfed by the size of major ERP implementation deals. This presents issues, both structurally and culturally, when integrating people who understand GRC into the big SI consulting industry model.

At the same time, the companies that contract with SI firms for large ERP engagements have contributed to this the of missed compliance expectations. Requests for Proposals (RFPs) typically do not clearly identify internal controls or compliance expectations for the proposed solution. RFPs are usually assembled by the information technology group, or a cross-functional business team, without involvement from the internal audit function. In the absence of information, SI firms tend to overlook these internal control requirements when submitting a competitive bid. In other words, if a company has not specifically identified its compliance expectations, it leaves this area dangerously open to interpretation as the SI firm plans and scopes its bid.

What Are the Implications?

As a result of the issues outlined above, SI firms may not completely understand or adequately plan for implementing internal controls and compliance requirements. Once they are contractually committed, they may be focused on “slamming in” the system to meet specified deadlines. Raising the issue of internal controls during later stages of a project can be perceived as painful additional work and a potential source of delay. Neither of these situations is welcomed with open arms.

Therefore, it is incumbent on buyers of SI services to ensure controls and compliance expectations are clearly specified in RFPs and addressed during early discussions with potential SI partners; active engagement of the internal audit function often helps to facilitate this dialog. Ultimately, expectations about delivery of internal controls should be reflected both contractually and within the SI implementation methodology. By aggressively addressing these topics up front, it is possible to engineer a “culture of compliance” into the project so that controls and compliance are understood and expected throughout the project entirety, rather than viewed as a hindrance when the project is operating at full speed.

What Are the Risks of Inaction?

In today’s business environment, failure to address these internal control and compliance issues during the right project phase presents a multitude of risks, including:

- *Project Delays* – System testing or auditors’ pre-implementation reviews may uncover concerns about security and controls. Given the increased focus on security and controls as it relates to Sarbanes-Oxley compliance, this has become a significant factor in “go/no go” checkpoints prior to major conversions.
- *Data and Process Integrity Issues* - Issues with proper access and process controls may compromise the integrity of the underlying data. This introduces a host of potential risks, including: fraud, customer service issues, product quality problems and even a lack of acceptance of the new system as the users lack confidence in the information it provides.
- *Post Go-Live Rework* - Lack of understanding about compliance documentation requirements can lead to significant and costly rework of project deliverables (modifying formats or adding additional information).
- *Material Weaknesses* - Projects perceived as neglecting security and internal controls can expect additional auditor scrutiny in the months following go-live, requiring the investment of time and energy to respond to auditors’ questions and issues. Lack of controls in business processes may also lead to external audit findings that must be publicly disclosed under the requirements of SOX. Interestingly, a recent study reported by CFO magazine confirmed that there is a correlation between disclosure of material weaknesses and market capitalization. In other words, significant internal control issues can ultimately impact a company’s stock price.

What Security and Controls Activities Are Relevant At Each Stage of the Project?

At each stage of an ERP implementation project, activities related to internal controls can be engineered into the project plan and deliverables. Attention to these items can help manage the risk associated with project delivery and the associated internal controls.

During the early stages of the project, focus on aligning project plans, methodology and timelines in order to deliver both the project’s business and compliance objectives. In Steven Covey’s bestseller *The Seven Habits of Highly Effective People*, Covey encourages us to “begin with the end in mind.” That concept is very relevant to ERP projects as the team must constantly think ahead and understand the related end-state compliance requirements. The associated project charter, standards, deliverable formats, tasks and work plan all should align with these expectations.

Figure 1 below, highlights significant risk management activities relevant to the various stages of the ERP implementation lifecycle, and aligns closely with SAP’s ASAP methodology. As the project moves forward into the design activities commonly called “blueprinting,” it is important to make sure that various work teams engaged in this effort understand the reengineering and internal control objectives of the project. For example, as process flows are developed, they should capture significant control points and “who does what” from a role perspective.

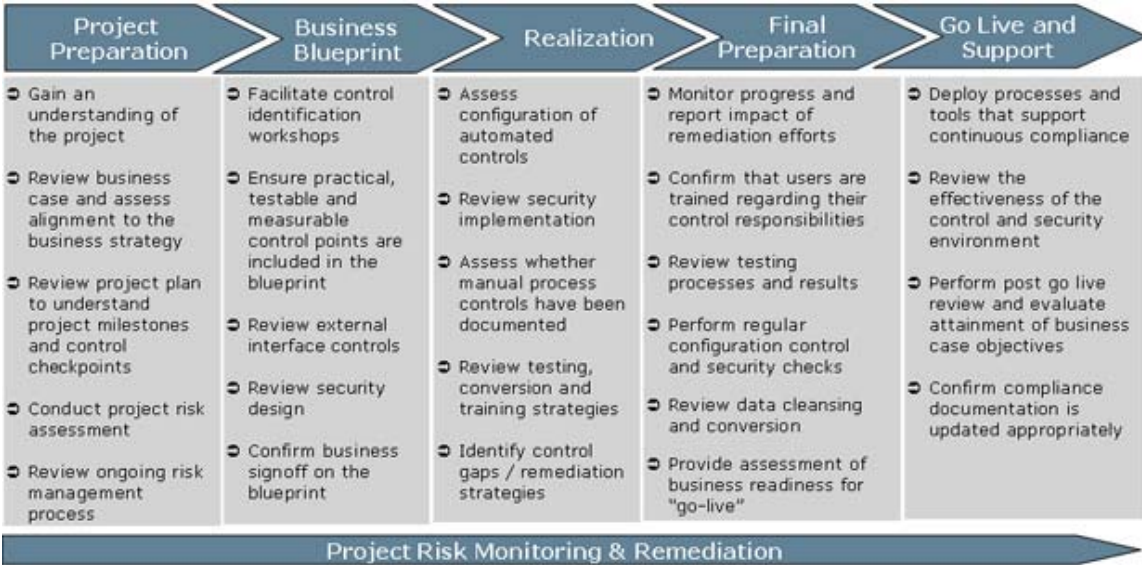


Figure 1 – ERP Significant Risk Management Activities

It can be incredibly useful to engage the internal or external auditors at this stage. These parties may be able to provide insight on items such as specific segregation of duties and sensitive access risks associated with the new system. Also, based on their unique perspective of risks in the business, these audit parties are able to highlight specific processes or transactions critical from an internal controls perspective.

Projects often employ process walkthroughs and integration checkpoints during this stage allowing internal control considerations to be worked into the agenda with minimal additional overhead. Some examples include:

- *Provide design teams with lists of control-related configuration and set-up decisions relevant to their area of the system.* Internal control subject matter experts can provide guidance on the software's internal control features and functions during these meetings. Examples may include critical error checking, tolerances and controls-sensitive transactions.
- *Use internal audit or other subject matter experts to be a "controls conscience" during process walkthroughs and integration checkpoints.* It is easy to get carried away with slick software features and elegant reengineering solutions. As teams are presenting their process flows, for example, it can be helpful (and minimally intrusive) to have the right people in the room to ask questions about internal controls.

As the project proceeds toward realization of the solution, it is important to continue championing activities that result in a robust security and controls capability. It is also wise to plan for checkpoints to assess and verify whether the controls expectations specified at the beginning of the project were implemented. Some projects deploy a "controls team" to facilitate development of internal controls across the various teams. At these later stages, this team can be key when assessing internal control implementation. One method of accomplishing this is to look for evidence in design documentation. However, increasingly automated tools make it possible to continually evaluate the implementation status of controls configured in the system.

A common pitfall during these mid-project stages is getting a late start on developing application security roles and profiles. The project often hits its peak staffing during this stage, and there are tremendous demands on the team. However, it is important to appropriately staff a function that works across the project and is charged with the important task of facilitating the development of application security roles. This process is iterative, tedious and requires dedicated focus.

Segregation of duties testing should also be included in these early stages of application security design, as issues impacting the design of the business process or system configuration may be identified. In addition, dialog with the business during security development presents an excellent opportunity to discuss possible mitigating controls that address segregation of duties issues.

Final preparations for "go-live" include various rounds of testing. During this phase, it is important for test scripts to ensure key control features are operating effectively. A potential role for a controls-focused project team is to review these test scripts and validate control features are being tested.

The later stages of testing, frequently called *integration testing*, are intended to pull together various business processes into end-to-end scenarios that demonstrate the system meets the defined business requirements. Perform these tests using the security roles planned for post-go-live. This is the real "test" of application security, to verify that the defined roles include the access necessary to perform a job. In addition to addressing risks around security, this important task is critical to managing the volume of security-related issues that inevitably arise after the go-live date.

Final Preparations

There are several other risk management activities to address prior to going live. A common mistake is to train users on specific system transactions but not the overall business process in which they will work. Training that provides an overview of the business process should include discussion of the control points and associated compliance expectations. If mitigating controls have been assigned to address segregation of duties or sensitive access issues, include these in the training as well.

Most projects invest significant time and energy into providing user support during the critical few weeks following a major system conversion. In addition to traditional contingency planning and fallback procedures, it is important that these plans adequately address application security. This is frequently the single most significant source for post go-live issues. Most projects are very flexible during this period, granting (for the most part) whatever access is necessary to service customers and keep the business operating. This approach is fine, as long as all the changes during this period are appropriately scrutinized once system stability is achieved. When embracing this “flexible” approach, it is highly recommended to plan for an additional round of segregation of duties testing (usually 6-8 weeks after go-live). Execute this testing once the system is stable and the enterprise completes its first month-end close cycle.

After several months of operating with a new enterprise system, users will better understand the system. This is a good time to refresh their knowledge on internal control expectations. These expectations may have been lost in the “noise” leading up to go-live and will now be more readily absorbed as the users have more hands-on experience with the new system. Practical system experience increases the relevancy of internal controls to these users.

Putting It All Together

There are many pieces to the ERP compliance puzzle; we only scratch the surface in this article. Continued focus is required throughout the project lifecycle to manage the risks of project success and embed necessary activities to ensure effective internal control over financial reporting. Major ERP implementation projects are risky endeavors and require tremendous commitment of organizational focus and resources. In today’s business environment, effective internal control over financial reporting is a requirement for public companies. Careful attention to controls throughout the ERP lifecycle, by “beginning with the end in mind,” offers a path for organizations to manage this risk and engineer compliance into the systems delivery process.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

About Protiviti Inc.

Protiviti (www.protiviti.com) is a global consulting and internal audit firm composed of experts specializing in risk and advisory services. The firm helps clients solve problems in finance, operations, technology, litigation and GRC. Protiviti's highly trained, results-oriented professionals serve clients in the Americas, Asia-Pacific, Europe and the Middle East and provide a unique perspective on a wide range of critical business issues.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

© 2008 Protiviti Inc. An Equal Opportunity Employer