

Risk Management When Implementing ERP Systems

Jeffrey T. Hare, CISA, CPA, CIA, is the chief executive officer and founder of ERP Risk Advisors. ERP Risk Advisors provides risk advisory services and training for companies that run Oracle Applications. Hare is a respected authority on the subject and is the author of the book *Oracle E-Business Suite Controls: Application Security Best Practices*. He can be contacted at jhare@erpra.net.

Organizations implementing new enterprise resource planning (ERP) systems make a major investment in their enterprise. Much of the impetus for such an investment comes from a desire to streamline their business processes and adopt best practices in the use of applications. Unfortunately, the trail is littered with case studies of failed or less-than-perfect implementations. Choosing the right ERP system that will best meet an organization's business requirements is obviously the first and most important decision toward accomplishing a successful implementation. The second most important decision is the choice of the systems integrator to shepherd the implementation process.

During the implementation of an ERP system, an organization has several significant challenges to overcome, including the reconfiguration of existing controls and the adoption of new internal controls. This article focuses on the types of risk advisory services that are common during an ERP implementation. In doing so, the importance of integrating a robust risk management methodology is recognized as one of the keys to success for all ERP system implementations. Also discussed are approaches to risk management, including the use of a risk advisory firm.

It is important to first define what is meant by risk advisory services in the context of an ERP implementation. In a typical implementation cycle, the project management office (PMO) is engaged in a variety of risk assessment processes. The PMO may use a variety of approaches and frameworks to help mitigate risks within the project. Some of the more common risk management standards are ISO 31000:2009 from the International Organization for Standardization and the Committee of Sponsoring Organizations of the Treadway Commission's *Enterprise Risk Management—Integrated Framework* (COSO ERM).

Perhaps the most obvious risk that the PMO assesses is whether a project is ready to go live. In a most simplistic view, risk advisory services

assess various types of risks throughout the life of a project and help management determine whether and how to mitigate such risks. The outcome of a risk assessment process is often the development of policies and procedures to help mitigate the risk(s) or the automation of controls to eliminate the risk. Management can also decide to do nothing and assume the risk after considering the organization's risk capacity and risk appetite.

FRAUD RISKS

There are three different risk scenarios related to fraud risk that may be addressed during an ERP implementation (see **figure 1**).

Figure 1—Risk Scenarios

Scenario	Type of Risks	Risk Mitigation
Accounts payable fraud	Financial loss, reputational damage	Segregation of duties
Purchasing fraud	Financial loss, reputational damage	Configurable automated control
Purchasing fraud	Financial loss, reputational damage	Embedded automated control

First, the risk of fraud in the payables department whereby a payables clerk has the ability to enter a new supplier and enter an invoice related to that supplier should be considered. In response, management may develop two policies to help mitigate the risk. The first policy requires new suppliers to be approved by someone outside of the payables department. The second policy requires supplier data entry to be audited by someone apart from the data entry process to ensure that only approved suppliers are entered. Once these policies are developed, procedures, such as a supplier maintenance procedure to address the first policy and a supplier maintenance audit procedure to address the second policy, would need to be defined.



Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.

Next, in a case of the use of an automated control to prevent or detect fraudulent purchases, the risk is that a purchasing agent can approve or enter a receipt of an item or service that they procured. In response, management should establish a policy that all purchase orders (POs) must be independently verified and a receipt must be entered against the PO by someone other than the buyer. This is commonly referred to as a “three-way match”—the PO must be matched with a receipt that must be matched to an invoice for it to be paid. Some ERP systems allow the automation of this control by configuring the ERP application. Once the configuration is set, the system does not allow an invoice to be paid without a receipt being entered against the PO. In other words, the control is automated.

A configurable control is automated via the setting of a particular configuration. One risk associated with configurable controls is that the automation of this control is dependent on the underlying configuration. Therefore, to maintain the integrity of the automated control, one must ensure that the configuration is not changed. A common response to the risk of the change in this configuration is to place it under change control, i.e., it must go through the change management process for the change to be made. In some ERP systems, the configurations can be changed manually, and in some systems, the configuration can be put under change control whereby it cannot be changed manually through the user interface.

The third example continues the thread related to configurable controls, and considers a case in which management may decide to accept a risk (likelihood x consequence). In some systems, configurable controls can be changed through the application’s user interface. Therefore, there is a risk that the configuration can be changed without going through the change management process. Because the cost of automating the control (i.e., preventing a change from being made through the user interface) exceeds the perceived risk, management may decide to accept the risk (i.e., not do anything about it). In this case, management would trust those employees who have access to the user interface that can change the configuration to follow the change management process.

OPTIONS WHEN EVALUATING FIRMS TO PROVIDE RISK ADVISORY SERVICES

Over the past few years, people have associated risk advisory services with US Sarbanes-Oxley Act compliance. Sarbanes-Oxley compliance has been a significant effort for

many organizations; however, risk management goes well beyond compliance with Sarbanes-Oxley. There are significant risks beyond Sarbanes-Oxley compliance that need to be evaluated. Some examples are:

- Compliance with regulations such as the Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA)
- Compliance with various national, state and local data security and privacy laws
- Risk that business requirements will not be fulfilled during the implementation
- Risk that business requirements are not properly confirmed during the testing process
- Stability of the application, such as when patches are applied
- Internal and external security threats

It is also necessary to recognize that compliance requirements are not the same for every organization. Some organizations may be private, and some may be heavily reliant

on manual controls. Therefore, the scope of each engagement has to be tailored to each organization.

Having given an overview of the problem, this article now turns to the solution. How can one effectively identify and manage risks in the context of

an ERP implementation? The following are three suggested approaches and their positives and negatives.

Option 1: Allow the System Integrator to Be the Sole Risk Advisor

Not all system integrators (SIs) are the same. Some SIs have qualified risk advisory staff and appropriate methodology, and some do not. If an organization is relying on its SI to provide risk advisory services as well as traditional SI services, the organization must make sure that it gets qualified references and resumes for both areas of expertise.

Pros of option 1 include:

- Project planning is integrated within the overall project. The project plan is more seamless because it includes traditional SI tasks and risk advisory tasks.

Risk management goes well beyond compliance with Sarbanes-Oxley.

- Resource coordination is more integrated compared to dealing with consultants from two different firms. This may be even more relevant when considering that customer resources are typically underallocated in a large ERP project.

Cons of option 1 include:

- The skills of risk advisory consultants are not typically found in traditional SI resources. Risk advisors often require advanced certifications, such as Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA) and even Certified Public Accountant (CPA). Real-world internal controls/security/business process experience is not often found in those who perform system integration work.
- Contracts with SIs typically cause inherent conflicts of interest. Integral to coming in on-time and on-budget is the management of scope. The SI's focus on "on-time and on-budget" can lead to quality issues and risks left unidentified and unaddressed.
- Using the same firm to provide risk advisory and SI tasks eliminates independence and objectivity when analyzing go-live readiness.

Option 2: Have an Audit Firm Provide Assurance or Risk Advisory Services

Although this is a common approach, it too has its pros and cons. One of the most significant challenges audit firms face is evaluating risks below the materiality level.

Pros of option 2 include:

- Many of the large audit firms are well-known commodities. They are a "safe bet" because they know what their peers expect from their Sarbanes-Oxley audit.
- If an independent risk advisory firm is used to provide quality assurance (QA) over the SI, having a third party review the project status, deliverables and results can protect the organization from stakeholders (SIs and internal stakeholders) saying that they are ready to go live (to save face or to prevent an increase in budget), when in fact they may not be ready.

Cons of option 2 include:

- The skill set of many audit firms is geared toward risks related to Sarbanes-Oxley compliance (i.e., material fraud and misstatements).
- Some consultants may be less experienced in specific applications and have little, if any, real-world experience in implementation or using the applications.

- Typically, costs are higher even when using less-experienced consultants.

Option 3: Use an Independent Risk Advisory Firm

Independent risk advisory firms can offer focused expertise and financial advantages.

Pros of option 3 include:

- Typically, such firms have more experienced niche consultants and experts in specific applications.
- These firms generally have lower costs and less management overhead on the team.
- An independent risk advisory firm provides QA over the SI. Having a third party review the project status, deliverables and results can protect the organization from stakeholders (SIs and internal stakeholders) saying that they are ready to go live (to save face or to prevent an increase in budget), when in fact they may not be ready.

Cons of option 3 include:

- Such firms may not have the brand credibility and perceived security of the major audit firms.

What types of services are typically needed, apart from those already provided by the organization's SI?

WHAT SERVICES ARE REQUIRED?

Regardless of the chosen option, what types of services are typically needed, apart from those already provided by the organization's SI? Following is a summary of some of the more common risk advisory services.

Comprehensive Risk Assessment

The cornerstone of the engagement should be a comprehensive risk assessment. A well-defined risk assessment helps management identify strategic and tactical risks associated with the project and should identify those that require controls to be revised or additional controls to be put in place.

Risks during an ERP implementation can be generic in nature or specific to an ERP system. Following are examples of generic risks that need to be considered:

- Business requirements not being adequately understood and documented, leading to the risk that the system may not meet the business objectives

- Technology changes not being able to be supported with current staff
- The PMO allowing an application to go live when the organization is not ready to do so
Following are examples of risks specific to an ERP system:
- Detailed changes of application configurations not being tracked
- Forms that allow Structured Query Language (SQL) statements and operating system (OS) scripts to be executed within them
- Three-way matching requirements being overridden when a buyer initiates a PO
- An accounts payable clerk overriding a hold placed on an invoice, such as a “quantity received” or a “price tolerance” hold

Targeted Risk Assessment Services

Management and/or the PMO may want to focus on specific risks, rather than perform an overall risk assessment process. In those cases, following are some of the more common services that can be provided:

- **Internal controls design**—Services related to the design of internal controls are traditionally provided by a risk advisory firm. This includes reviewing the current risk and controls library and redesigning such controls for the new environment (e.g., applications, technology). Controls should be designed for known compliance initiatives such as Sarbanes-Oxley and PCI DSS, but should also take into consideration fraud risk below the materiality level (submaterial fraud risk) and operational risks specific to the organization.
- **Business process design**—The risk advisory firm should optimize the process design to meet the organization’s internal control objectives. This includes design of the to-be controls in conjunction with the to-be business process. It is important to take advantage of all the automation capability that comes with the applications, and to take into account key activities that happen outside the system and that influence the design of effective internal controls and security for the organization. Some risk advisory firms also have consultants with implementation experience who can help provide QA related to the SI’s recommendations.
- **Software configuration and change management**—Tangential to the business process design is the configuration of technology and software. This includes

Enjoying this article?

You may also find value in...

- *Security, Audit and Control Features SAP ERP, 3rd Edition*, ISACA
- *Security, Audit and Control Features Oracle E-Business Suite, 3rd Edition*, ISACA
- *Security, Audit and Control Features PeopleSoft, 2nd Edition*, ISACA

www.isaca.org/bookstore

- Related audit programs and ICQs that are posted as Word files for ISACA members

www.isaca.org/auditprograms

the initial configuration of the application as well as the design of a change management process to comply with best practices. Controls that are defined as application controls should be baselined as part of the initial configuration approvals. Then, the organization should work with its IT department to define change management policies and procedures to ensure the integrity of the application controls on an ongoing basis so that external auditors can rely on the automated controls.

- **Security role definitions and assignment**—Security role definitions and the related role provisioning process are critical to the proper development of internal controls and to the ongoing integrity of the organization’s applications. It is important to go beyond the traditional concern about segregation of duties and take into account sensitive processes and access to sensitive data. Further, the design of the role definitions should consider key processes outside the system as well, including the supplier approval and validation process, collections process, account reconciliations, and manual journal approvals. The risk assessment process related to application security and role design is critical to maintain the integrity of the system’s processes and applications. The role provisioning process and validation process should be covered in the design of the organization’s internal controls.
- **Testing**—The risk advisory firm should be expected to examine the final user acceptance testing results

and interview key subject matter experts, as necessary, to confirm production readiness. Concerns and recommendations should be escalated to the PMO throughout the project.

- **Controls-related software**—No ERP system is complete out of the box. Each one requires additional software to help supplement what is provided for internal controls and security automation and monitoring. A risk advisory firm can help in understanding the common deficiencies and how to fill the gaps with other software. Common software requirements, beyond the core ERP system, address issues such as segregation of duties, audit trail development, hardening/penetration testing, testing automation, SQL query and *ad hoc* reporting tools, patch impact analysis, and control automation. Unfortunately, organizations often underestimate the impact of additional software requirements outside the core ERP system in relation to their budget and in their project planning. This often leads to a less-than-ideal implementation and a less-than-perfect control environment.

CONCLUSION

When implementing a new ERP system, an organization makes a substantial investment in its enterprise applications with an expectation that it will implement a system that meets both its operational objectives and its control objectives. An independent risk advisory firm can assist by performing traditional risk advisory services as well as providing a QA role for the implementation.

The *ISACA Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2011 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org