Why ERP Implementations Fail: Beyond the Obvious

By Jeffrey T. Hare, CPA, CISA, CIA

Much has been written over the years about why ERP implementations fail or are less than optimal. In this article, we explore some of the less obvious issues that drag down projects. Our vantage point is from one that primarily focuses on risk management, internal controls and security in the context of Oracle E-Business Suite application, but we think you'll find that many of the points in the argument are applicable to any ERP system implementation. Let's first recognize that project success and failure is a spectrum. Our goal is not just to help you avoid failure, but to make decent projects even that much more successful. With that in mind, let's get started.

The goal is to have a square peg in a square hole and a round peg in a round hole.

The "obvious" things that are necessary to avoid a sub-optimal implementation are things like having a sufficient budget, appropriate level of support from senior management, an experienced systems integration partner, well-trained staff and a strong program/project management group. While these are all important elements for a successful project, there are three topics that are often overlooked or underemphasized:

- Failure to consider additional software in the project's budget.
- Inability to fully consider the impact of internal controls throughout the project.
- Failure to take into account common application deficiencies in the project's requirements.

1 Failure to Consider Additional Software in the Project's Budget

Oracle's suite of software has evolved significantly since I first started using the applications in 1998 – both through internal development and through acquisitions. However, a complete ERP system requires additional software components to ensure its successful implementation and ongoing operation. Here are some common "additional" software tools that may be necessary if you run Oracle E-Business Suite:

- **Impact analysis** – analyzes the impact of patches on the current environment, between environments and on customizations by looking for changes during the patching process.
- **SOD** – Segregation of duties and single function risk detective and preventive controls during the user provisioning process; manage quarterly attestation process.
- **Advanced audit trail** – ability to create before/after values for changes to critical transactions, master data and configurations; provide the system-based audit trail for quality assurance of your change management process.
- **Instance comparison** – compare application data such as configurations and master data between two or more instances to help analyze support issues.
- **Query tools** – SQL-based query tools for DBAs, developers, auditors, analysts, etc.
- **Additional security/obfuscation/encryption** – provide additional security or encryption on critical sensitive data that is not adequately encrypted or secured by Oracle out-of-the-box.
- **Code management and migration** – object management and migration from development instances to production instance.
- **Controls automation** – ability to rapidly deploy forms personalization on professional forms.
- **Controls monitoring** – examples include the ability to monitor critical transactions and compliance with system configuration such as server settings, generic logins, resetting passwords of seeded users (applications and database), monitoring privileges of database users.
- **Archive and sub-set tools** – ability to archive data and sub-set data when cloning.
- **Clone and backup automation** – fully automate clone, backup and disaster recovery processes.
- **Emergency access management** – ability to manage emergency access to the applications and track related activity.

Much of this software is considered critical for organizations that have been running the software for any significant length of time. Having it budgeted for during the initial implementation and as part of the original implementation scope will be very helpful. Some of these categories of software can be purchased from Oracle and some from other vendors. There are pros and cons related to buying

> **"There are pros and cons related to buying software from Oracle versus third party vendors that need to be properly evaluated."**

software from Oracle versus third party vendors that need to be properly evaluated. We also recognize that some of these categories of software may not be appropriate for smaller installations and/or may not be affordable for all organizations. The important thing for management to consider is the cost/benefit and the risks that wouldn't be addressed if the software wasn't purchased.

2 Failure to Fully Consider the Impact of Internal Controls During the Project

In spite of the plethora of compliance requirements, including the US Sarbanes-Oxley legislation, we find that internal controls considerations are often not fully accounted for in many projects. Some of this can be traced to a lack of maturity by the organization as a whole while some are specific to what happens during an implementation. Typically these are the components we like to see in a project with regard to internal controls:

- Well-defined ownership of the risk and controls library. While this may seem intuitive, we see a wide variance of ownership of risk and controls, depending on the size of the organization, the definition of internal audit's role and the presence or absence of a corporate governance department.
- A risk advisory partner that understands risk and controls specific to the ERP system being implemented. While this could come from internal resources, we think the best model is a firm independent of the system integrator and external auditor.
- Integration of the development of controls definition with the overall process sufficiently early in the project. This should be identified as a separate thread on the project plan and, in some cases, a separate project in the program as a whole. In either case, controls should be designed as part of the overall process design, not as an afterthought. Too often we see internal controls being defined during UAT or so late in the project that any significant changes are difficult to manage.
- Ability to balance operational effectiveness and development of strong internal controls in the development of the business process and use of the applications.
- Design of application security should take into account the business process design AFTER internal controls have been developed and after a risk assessment process has been applied to risks such as segregation of duties, single function risks and sensitive data risks.
- Common configurations and master data shared across the application need to be adequately discussed and considered in process and application security design.
- Policies and procedures related to change management need to be adequately defined – patching, development, security, configurations – and a robust Quality Assurance process implemented to ensure compliance.

3 Failure to Take into Account Common Application Deficiencies

Finally, our last topic related to knowing and compensating for common application deficiencies. While it may seem reasonable that your system integrator understand the applications well, we've found that these requirements are often overlooked on projects:

- Workflow security risks – how to manage delegation of workflow approval authority.
- Workflow history retention – retention requirements related to workflow approval history.
- Read-only configurations – lack of inquiry access to configurations throughout the application.
- Lack of system-based audit trail for critical system changes – to support the quality assurance of your change management process.
- SQL Forms – how to monitor activity in forms that allow SQL statements to be embedded in them.

- Seeded users – vendor supplier application and database users.
- Business processes that cannot be secured via normal function security such as:
  - Approval of transactions in the Receivables module.
  - Approval of orders in the Order Management module.
  - Managing credit in the Receivables module.
  - Entering of negative orders in the Order Management module.
  - Entering of negative transactions in the Receivable module.
  - Approval of POs in the Purchasing module.
  - Maintenance of Salaries in the HR module.
  - Maintenance of Direct Deposit information in the HR module.

Oracle, like most software companies, has design flaws in their software and technology that often gets identified by their end user community. Oracle has a strong relationship with the OAUG's Special Interest Groups (SIGs) and the SIGs provide invaluable feedback to Oracle on bugs and enhancement requests. OAUG membership includes involvement in the SIG communities and allows you to interact with other Oracle customers through the OAUG's various forums (conferences, listservers, etc). Therefore, your OAUG membership helps to identify and resolve these types of deficiencies.

Conclusions

The previous three topics represent some of the more common challenges we see that go unaddressed or not fully addressed during an ERP implementation such as Oracle E-Business Suite. Organizations must ensure that requirements are complete and all requirements are adequately addressed by one or more vendors or by internal staff. Systems integrators and software providers will only respond to RFPs to the extent that they can meet the requirements identified. The inability of management to clearly identify requirements and ensure that each of the requirements is addressed is a common downfall in a project.

To adequately address these requirements an organization must have a well-seasoned group of advisors that focus on the various areas. You wouldn't, as an example, want ERP Risk Advisors to help ensure that infrastructure requirements are identified and met since we specialize in internal controls and security. In the same way, you probably wouldn't want a system integrator to ensure that internal controls requirements are identified and met. The goal is to have a square peg in a square hole and a round peg in a round hole. With these three common challenges that we've outlined, we hope we've identified a few things for you to be aware of and compensate for when implementing your ERP system.

"Oracle has a strong relationship with the OAUG's Special Interest Groups (SIGs) and the SIGs provide invaluable feedback to Oracle on bugs and enhancement requests."

Jeffrey T. Hare, CPA, CISA, CIA is a highly respected author, analyst and consultant regarding internal controls and security for companies running Oracle E-Business Suite. Jeffrey's extensive background, certifications and experience allow him to provide unique insight into overwhelming challenges faced by organizations in designing and implementing Oracle E-Business Suite. ERP Risk Advisors provides risk advisory services for Oracle Applications including project QA/audit services, internal controls design and audit, and security design and audit.