EVOLUTION OF THE ROLE OF RISK AND CONTROLS TEAM IN AN ERP IMPLEMENTATION

GLORIN SEBASTIAN

School of Public Policy, Georgia Institute of Technology, Atlanta, GA, USA

ABSTRACT

The evolution of Controls team from being responsible only for Compliance to being responsible for the entire Project Risk and Controls during an ERP implementation is testimony to the realization by Business on the value that the Controls team brings in. It is also indicative of the rise to prominence of this team among the various component implementation teams from a mere check the box item or an afterthought to an integral part of the entire ERP implementation cycle, right from requirements elicitation through development, testing, go-live and production support.

There are four key reasons why risk and controls team is indispensable in an ERP implementation. Risk and controls team in each stage of ERP implementation lifecycle namely, project planning, requirements, testing and post-production support. An incorrect implementation could affect the daily business operations severely and could seriously jeopardize the future of the company. Hence any project that involves IT and Business transformation is to be approached with meticulous planning and preparation to ensure successful transformation aligns to the business objectives.

KEYWORDS: ERP implementation, business & planning

1. INTRODUCTION

Enterprise resource planning (ERP) is designed to provide seamless integration of processes across functional areas with improved workflow, standardization of business practice, and access to real-time, up-to-date data. As a consequence, ERP systems are complex and implementing them can be a challenging, complex, time-consuming and expensive project for any company [1,2]. The evolution of Controls team from being responsible only for Compliance to being responsible for the entire Project Risk and Controls during an ERP implementation is testimony to the realization by Business on the value that the Controls team brings in. It is also indicative of the rise to prominence of this team among the various component implementation teams from a mere check the box item or an afterthought to an integral part of the entire ERP implementation cycle, right from requirements elicitation through development, testing, go-live and production support.

This shift in importance has led to the various major System Integration Firms who are often tasked for the deployment of ERP solutions via multiyear implementations to regularly include controls team for reviewing the Risk and Controls associated with each IT and business process, thereby ensuring that sufficient controls exist to mitigate the risks prior to the system go-live. This is in sharp contrast to earlier times when compliance team used to be an afterthought or not even consulted during the system implementation process. Usually including the risk and controls team as an afterthought leads to serious operations related issues after go-live, and given that in most cases the warranty period after go-live extends only a couple of months, most issues found after the go-live needs to
be fixed by the client at additional expense.

In many ways, the rise in prominence of risk and controls team in system implementation projects and software development lifecycles is similar to that of cyber security and privacy teams, that used to be an afterthought or most times not even considered during any stage of the SDLC cycle, as opposed to now when Cyber security and privacy requirements are inbuilt into systems right from the requirements phase.

**Key reasons why risk and controls team is indispensable in an ERP implementation:**

1. **The Risk and Controls team reviews implementation at overall Governance level:**

Most system integration teams consist of individual component teams, each specializing in a particular business process such as RTR (record to report), PTP (purchase to pay) or OTC (order to cash) or the FICO Module if you consider SAP implementations, each team bringing in their specific business process related expertise, however fails to see how it all comes together. This is true not just at a business process level but also at a system level. For example, in the case of SAP system implementation there are many sub systems that are also being implemented and require to work in tandem with the SAP system such as SAP BPC- business planning and consolidation, that helps in planning and forecasting, as well as ensures compliance with financial reporting standards during budget and closing cycles and SAP Concur which is an expense management application.

This high-level governance view of the project is achieved via GRC (governance risk and compliance). GRC transcends business processes, technology and sometimes even helps visualize cross system risks and thus provides an overall view of the risk and controls for the organization. This makes risk and controls team an extremely important component from a management perspective since it provides direct insights into the various organizational risks from both business and technology process perspectives and details the controls in place to effectively mitigate these risks.

1.2 **Prevents cyber security issues**

One of the major risks that the risk and controls team includes in the RACM (risk and control matrix) and tries actively to remediate is users with inappropriate logical access. Most logical access designs are based on the principle of ‘Least privilege’ and RBAC (role based access controls) to ensure the access to various critical functions is restricted-- examples below:

- GRC and security administration access
- Access to powerful SAP profiles such as SAP_ALL, SAP_NEW
- Robust firefighter access controls
- Controls around GRC rule set changes

With human error cited as the main reason for data breaches[3], restricting the access based on least privilege and role based principles help control the end user mistakes.

1.3 **Avoids compliance failures**

If the business and technology risks are not mitigated appropriately, there could be compliance issues including audit findings and potential material weaknesses. Thus proper mitigation of the applicable risks are required for efficient functioning of the compliance function.
1.4 Prevents operational issues prior to go-live

As mentioned, the risk and controls team ensure not just compliance but also that the logical access, change management and operations related risks are appropriately mitigated via robust controls. Unmitigated risks especially operations related issues can severely impact the go or no-go decisions prior to the go-live activities.

2. Role of risk and controls team in each stage of ERP implementation lifecycle:

2.1 Project planning and design:

Even before the project planning and design, the risk and controls team perform the pre-implementation review of the existing system and the business level governance activities to ensure the enterprise is ready for the implementation. This pre-implementation review matches the business needs and requirements to the proposed system specifications to ensure the alignment of the system updates to the business objectives.

The controls team also reviews the project plan once the project has been finalized to understand the various project milestones and decides the applicable control related checkpoints.

2.2 Requirements phase:

In the requirements phase, the risk and controls team take part in the requirement workshops which help identify the relevant control points in each process.

The controls points could be within the business and technology processes as well as between external interface controls to ensure completeness and accuracy of the data transfer between the system being implemented and the systems that it communicates to, within the IT Environment. The controls for this could range from manual procedures to count the data items transferred between systems or could be a custom report that lists the line items transferred with the required details. Either ways, it is the risk and controls team responsibility to ensure that the controls are well documented.

Finally, it is also mandatory to ensure that the risk and controls team should be one of the teams providing the final sign off on the project requirement documents.

2.3 Development and testing phase:

During the project development and testing phase, the controls team provides support for questions relating to the control requirements as well as ensures that the configuration of automated controls and role design by the application security team follows the design documents.

Also, as mentioned in the requirements phase, risk and controls team also ensure that the data completeness and accuracy controls which could be either manual or automated are in place. Once the development is complete the risk and controls team actively participates in the SIT (System integration testing) and UAT (User acceptance testing) prior to signing off to confirm that the control requirements have been met. During this period, the risk and controls team also ensures that the end users have been appropriately trained for any control related processes.

2.4 Go-live and post production support:

Once the SIT and UAT testing has been completed and signed off, the project enters the code freeze stage, which is governed by an effective cutover plan. Cutover plan essentially includes the steps to successfully transition and move the
final tested code from test environment to production environment and it includes preparation activities for cutover, the deployment i.e. the go-live, and the post-deployment activities.

Most times, the involvement of risk and controls team in go-live and post go-live phases are limited. However, the risk team does make sure via post-implementation review that all the control related requirements documented in the control requirement documents have been successfully migrated and is available in the production environment.

CONCLUSIONS

Most ERP implementations are projects of extreme significance to business clients. This is because an incorrect implementation could affect the daily business operations severely and could seriously jeopardize the future of the company. Hence any project that involves IT and Business transformation is to be approached with meticulous planning and preparation to ensure successful transformation aligns to the business objectives.

It should be clear from the points mentioned in this paper that the risk and controls team has evolved from just a compliance function which was considered a check the box activity to an active advisor on business and technology risks for the client during large transformation projects.

REFERENCES

