protiviti®
Face the Future with Confidence

The Role of the Internal Audit Function in System Implementation

Responses to Key Risks Throughout the Organization

Although every large-scale system implementation is unique, the risks inherent in these programs are largely consistent across all programs. The internal audit (IA) function can help significantly reduce these risks by playing a role that is educational, consultative or audit in nature, and by bringing deep independent subject-matter expertise to the most common risk areas. IA's ability to operate across the enterprise and across all individual work streams in a program provides visibility to risks that might otherwise be lost between silos. A selection of the more common system implementation risks and the related focus of IA are summarized below.

Business Process Readiness and Solution Design

1. **Risks**

- The requirements and design of the future solution emerge over time (if at all), leading to rework, changes, delays and missed user expectations both pre- and post-go-live.
- System design and business process requirements are not aligned, leading to potential business disruption and/or lack of transformation of business processes.
- The business is unable to envision potential future optimized business processes and to understand or critically assess "designs" proposed by system integrator.
- The lack of a complete integrated data architecture design leads to process inefficiencies and a proliferation of business processes outside the system.

2. **IA Focus**

- Planned implementation methodology includes a level of design definition and documentation that details the future state design at the process, organization, application and data levels.
- Parties responsible for providing design leadership are clearly identified and have the appropriate skills.
- Business partners take ownership for detailed review and sign-off of proposed design, with corresponding commitment to operational improvement.
- Critical gaps in the technical design are identified (if any) and addressed immediately.
- Manual workarounds are thoroughly evaluated and managed throughout the project lifecycle.

Program Management and Governance

1. **Risks**

- Governance structures fail to enable timely decision-making, issue identification and issue resolution at the right levels in the organization.
- Ineffective project and resource planning leads to delays in project execution, missed dependencies, and key activities lacking ownership or resource-delivery capacity.
- There is a lack of ownership and accountability of critical components of the program (e.g., the focus is exclusively on system design, configuration and system-testing activities).

2. **IA Focus**

- An effective project management office (PMO) has been established with structure, roles and responsibilities defined.

- An overall program governance structure has been established, beginning with the critical roles and responsibilities expected of business, IT and vendor personnel involved in the implementation.
- The PMO and program governance effectively and efficiently identify and resolve critical risks across all functional areas within the program (e.g., UAT, data validation).
- Project stakeholders have developed and reviewed the program plan for completeness to ensure it appropriately represents all parties and the true critical path.

Data Conversion and Governance

1. **Risks**

- Data conversion is treated as technical, with no business involvement, resulting in incorrect mapping of data and poor data quality that cause delays in implementation and impact operational effectiveness of the new system.
- Data ownership and the processes for authoring and approval of master data are not defined, and data quality is not monitored, resulting in incomplete master data that impacts the operational effectiveness of the ERP system.

2. **IA Focus**

- The data conversion strategy and plan have been established and formal sign-off has been received from business owners of the data, as well as from the system integrator and the IT department.
- Data conversion design documentation has been developed and includes data rules and attribute-mapping in sufficient detail. Stakeholder sign-off has been received.
- A data cleansing plan has been developed that outlines clear responsibilities for cleansing and validating source data.
- Data conversion validation procedures have been developed for each data object.
- A defect management process has been established to ensure the conversion process does not miss key data.
- A comprehensive data governance plan has been developed and stakeholder-approved with a framework of organization roles, a "data dictionary," defined metrics and documented policies.

Organization Change Enablement

1. **Risks**

- Users and business process owners are unprepared to participate effectively on the project, business requirements, design, testing, training and adoption.
- A lack of focus on building user and management support, adoption and readiness leads to ineffective and inefficient processes and post-go-live disruptions, regardless of the quality of the system implemented.

2. **IA Focus**

- The organizational impact of system and process changes has been determined, assessed and planned for to ensure that anticipated benefits are realized.
- Analysis of stakeholders and their needs has been performed. Change enablement strategies and activities have been developed to ensure changes are implemented effectively.
- A change enablement plan has been developed with buy-in from key stakeholders, with their commitment to support the changes and the initiative's performance-improvement objectives.
- The change enablement plan includes training for the remaining user community outside of the subset of users the system integrator typically trains toward the end of an implementation.

Testing Strategy

1. **Risks**

- Testing strategy and plans are not appropriately defined and prioritized as part of the project, resulting in inadequate testing scope and resources and, ultimately, unvalidated requirements.

2. **IA Focus**

- Test plans provide comprehensive coverage of the end-to-end processes, the full range of business scenarios and a representative set of real-life data variations.
- An effective metrics framework and tracking process allow for governance, corrective actions and re-planning.
- Testing entry and exit criteria are clearly defined and then satisfied and approved.
- There is an effective defect management and prioritization process.
- Regression testing is performed consistently to assess the impact of fixes for failed tests on cases already passed.

Reporting and Analytics

1. **Risks**

- Reporting requirements are not captured, reports are not validated during testing and a broader information strategy is not developed, resulting in a lack of visibility into business performance and disruption of business processes.

2. **IA Focus**

- Stakeholders have verified a complete inventory of key reports.
- The enterprise has reviewed and validated the overall architecture, tools or technologies being put in place for reporting to ensure they will meet future business needs.
- The new system delivers the critical analytics capabilities the business requires.
- The business has considered a formal governance program to sustain the business intelligence environment.

Security and Internal Controls

1. **Risks**

- Project planning and execution fail to incorporate security and internal control project activities (i.e., design, documentation and testing), and costly remediation is required post go live.
- Expensive manual workarounds are required to compensate for the failure of the new system to deliver security and internal controls that meet audit and regulatory compliance requirements.

2. **IA Focus**

- The program organization, methodology and plan include comprehensive coverage of security and internal controls.
- Security and internal controls are integrated into core program activities, including architecture, design, configuration and testing, with interdependencies considered and managed.
- Security and internal controls design provide for a high degree of automation.

IT and Business Operational Readiness

1. **Risks**

- The IT and business organization(s) responsible for maintaining the new system are not prepared to assume ownership and maintenance responsibilities.
- Failure to support the new system results in a lack of confidence in and adoption of the new system; inefficient and ineffective communication, prioritization and resolution of issues; and a high cost of maintenance and support.

2. **IA Focus**

- A strategy and plan for post-go-live support in IT and the business are developed early in the program lifecycle.
- Preparation and implementation of systems, processes, organization and training for support are managed and governed as part of the system implementation program (and not as an afterthought).

How Protiviti Can Help

Protiviti can help your internal audit functions reduce risk by developing and delivering enterprise-wide support for your system implementation. Contact us to schedule a complimentary session where we will provide your internal audit team with guidance to perform its critical support role.

Contacts

Toni Lastella
Managing Director, NYC
+1.212.399.8602
toni.lastella@protiviti.com

Carol Raimo
Managing Director, NYC
+1.212.603.8371
carol.raimo@protiviti.com

Aric Quinones
Managing Director, Atlanta
+1.404.240.8376
aric.quinones@protiviti.com

Martin Nash
Managing Director, Tampa
+1.813.348.3374
martin.nash@protiviti.com

John Harrison
Managing Director, Houston
+1.713.314.4996
john.harrison@protiviti.com

Tom Luick
Managing Director, Chicago
+1.312.476.6342
thomas.luick@protiviti.com

Steve Cabello
Managing Director, LA
+1.213.327.1470
steve.cabello@protiviti.com

Ronan O'Shea
Managing Director, SF
+1.415.402.3639
ronan.oshea@protiviti.com