



The Critical Role of Risk and Control Assessments in ERP System Implementations

Introduction

Enterprise resource planning (ERP) implementations have become a critical component of organizational transformation as organizations navigate acquisitions, mergers, and growth-driven change. While replacing or upgrading core systems can streamline operations, improve data quality, and enhance decision-making, it can also introduce significant risks.

Changes to established processes, however well intentioned, can undermine the integrity of financial data and disrupt regulatory and audit compliance if not carefully managed. Without disciplined planning and proactive risk management, organizations may emerge with complex systems that fail to deliver reliable, accurate information, putting both operational performance and financial reporting at risk.

How Important is Planning for a System Implementation?

Whether driven by a transaction or the need to replace outdated technology, decisions made during the planning stage shape the success of the entire system implementation. Effective planning requires early alignment with organizational goals, strategy, and stakeholder needs, supported by clear objectives, strong project governance, business process alignment, and proactive change management.

Realistic timelines, phased rollouts, early staff engagement, adequate training, and sufficient technical and financial resources help minimize disruption, support adoption, and maintain business continuity. Without this disciplined approach, organizations risk avoidable challenges at go-live, including data issues, lack of user adoption, delayed reporting, and operational strain that can undermine the value of the new system.



How Can a System Implementation Affect Financial Statements?

When organizations implement new enterprise applications, a range of risks can arise that directly affect financial statements and the reliability of financial reporting. Inadequate testing may cause systems, interfaces, controls, or financial reports to function improperly, resulting in unreliable outputs and weakened internal controls. In addition, data migration issues—such as incomplete, inaccurate, or misclassified data—can compromise the accuracy of financial statements and reports compiling financial data. Misconfigured system controls and poorly designed user access matrices can further increase the risk of errors, unauthorized changes, data breaches, and ineffective segregation of duties, creating opportunities for undetected fraud or discrepancies.

For an ERP system implementation, “changes to other processes and controls” means impacts beyond the core system build—e.g., redesigned workflows, changed approvals/segregation of duties, altered data interfaces, revised reports/spreadsheets, new reconciliations, changed close/tax/treasury/inventory processes, and controls moved from manual to automated or dependent on Information Technology General Controls (ITGCs). Also, use of agentic AI embedded within new ERP systems further complicates the governance of system controls.

From financial statement risk perspective, consider whether the change creates a risk of material misstatement through incomplete/inaccurate data migration, broken interfaces, unauthorized access/SOD conflicts, report logic errors, ineffective management review controls, missing compensating controls during cutover, lack of AI agent identity management, and ineffective ITGCs over change control, access, and operations that support automated controls and system-generated reports.

With careful planning and disciplined execution, organizations can manage these risks while realizing the benefits of a system implementation.

Early and continuous involvement of key stakeholders - including external and internal auditors, IT, accounting, and finance teams - throughout the pre-implementation, go-live, and post-launch phases is critical to identifying and addressing issues before they escalate. Failing to address pre-implementation risks can increase costs and negatively affect financial statements and audit readiness, underscoring the importance of conducting a comprehensive system implementation assessment before go-live.

To proactively identify and mitigate potential issues, **evaluate these five key risk areas** ►



Project Governance and Risk Management

Successful system implementation is grounded in robust project governance and comprehensive risk management, with a strong focus on effective project controls. These controls are essential to maintaining project alignment and facilitating the timely identification and mitigation of potential risks. Key elements of project controls include:

Change Management

Rigorous oversight of change management practices helps confirm that all modifications to project scope, timelines, or deliverables are authorized and documented. A formal change management process should govern all proposed changes to the ERP system implementation, including changes to scope, requirements, solution design, configuration, integrations, data migration, security, controls, timelines, budget, and deployment plans. The process should promote informed decision-making, maintain alignment with business objectives, and prevent unauthorized or inadequately assessed changes from introducing operational, financial, compliance, or technology risk.

Go/No Go Summary Checklist

Maintaining a detailed go/no go checklist provides a comprehensive record of key decision points and confirms readiness for each phase of implementation.

User Security Approvals

Properly documenting user security approval or user permissions verifies that access controls are both established and validated.

User Acceptance Testing Results and Sign-Offs

Recording and retaining outcomes and approvals from user acceptance testing demonstrates that the system satisfies user requirements prior to full deployment.

Project Governance and Decision Making

Conducting regular reviews of project governance structures is vital for sustaining clear roles, responsibilities, and lines of authority throughout implementation. Clearly defined escalation paths for decision making and approvals are critical for timely progress of the implementation.

Issue Management and Resolution

Consistent tracking and resolution of project issues enables prompt risk identification and mitigation, supporting successful project delivery. Maintaining an issue tracker assists with ongoing monitoring and facilitates effective resolution of challenges.

Project Plan

Maintaining a comprehensive project plan is critical for tracking progress and ensuring accountability.



Data Migration

During system implementations, data migration demands careful attention to validate completeness, accuracy, and alignment with organizational standards. Key considerations include thorough validation of master and transactional data testing results with management sign off and formal approval of reconciled conversion balances. By addressing these aspects, organizations can validate the integrity and reliability of migrated data within their new systems.

One of the most critical elements during a system implementation is the process of capturing, documenting, maintaining, and leveraging the schema designed to migrate data from the legacy system(s) to the new system. Well designed mappings and crosswalks, together with disciplined data profiling and cleansing, can support data restructuring and a more effective data migration. These artifacts should be complete and receive sign-off from authorized stakeholders before they are identified and referred to for directional use during the system design and build. If data mappings or crosswalks are flawed, or if duplicate, incomplete, or inconsistent records are migrated, preventable issues may arise when loading and reconciling data in the new database.

Data cleansing should be planned as a formal activity within the data migration lifecycle or completed in advance of the implementation. This exercise can correct errors, standardize formats, remove duplicates and obsolete records before data conversion begins. Implementation for enterprise platforms necessitates the data imported to be actively managed throughout the project lifecycle to avoid errors and delays at go-live. Best practice guidance highlights that successful implementation depends on the quality of the legacy data being converted and migrated. Investing time in data cleansing early reduces rework during mapping, cross walking, and testing cycles. It can improve data reconciliation and reporting accuracy in the new system and increases user confidence and adoption. The business processes would be operating on trusted, consistent master and transactional data providing greater assurance to the business.

DATA MIGRATION FOCUSES ON SEVERAL KEY AREAS



Master Data Migration Testing Results

Examining the results of master data migration testing and verifying that management has provided official sign off, thereby confirming the validity and completeness of the converted data.



Transactional Data Testing Results

Reviewing the outcomes of transactional data testing and verifying that management sign off has been obtained indicates the reliability and accuracy of transactional data after conversion.



Reconciliation of Conversion Balance Results

Assessing the reconciliation of conversion balances to validate that results are accurate and have been formally approved by management evidences the integrity of the converted balances.

Collectively, these components are vital for verifying that data migration activities conducted during system implementation are executed completely and accurately.

A key aspect of validating the accuracy of financial statements involves a thorough assessment of business process risks and the associated controls. This procedure involves the identification of potential misstatement sources and an evaluation of whether existing controls are adequately designed to mitigate those risks. It is imperative to review the entity's documentation concerning control design and user acceptance testing (UAT) outcomes. The review should concentrate on areas with direct relevance to the financial statement audit and include management's formal approval. Particular focus should be given to the following aspects:



Automated Application Controls: Both programmed and configurable controls within an organization's systems must be evaluated for effectiveness and proper configuration, validating they function as intended.



IT Dependent Manual Controls: It is necessary to validate manual controls that rely on information produced by IT systems (i.e., system generated reports), specifically those pertinent to the financial statement audit. Comprehensive documentation and rigorous testing of their design and operation are required.



Agentic AI Identify Management: As organizations increasingly embed agentic AI capabilities within ERP platforms to automate decisions, execute transactions, and support business processes, it is critical to assess how AI agents are identified, authenticated, authorized, and governed within the control environment. Agentic AI identities should be clearly defined, uniquely identifiable, and subject to the same rigor as human and system accounts, including role-based access, segregation of duties, and logging of activities. Organizations must evaluate whether controls exist to prevent excessive or autonomous access, validate that AI agents operate within defined business rules, and confirm appropriate oversight, monitoring, and accountability mechanisms are in place. Weaknesses in AI identity governance can introduce heightened risks related to unauthorized transactions, data integrity issues, and ineffective management review controls that directly impact financial reporting reliability.



Interim Workaround Design: Any temporary measures implemented to address control gaps must be examined for their effectiveness until a permanent resolution is implemented.



Interface Controls: Interface controls validation is a critical element of ERP system implementations, helping organizations ensure that data is processed completely, accurately, and consistently across system jobs and interfaces. In highly integrated ERP environments, automated jobs and interfaces often support critical financial processes, making it essential to confirm that the related controls are properly designed and function effectively. Validating these controls helps organizations address the risk of processing failures, duplicating or missing data, unauthorized changes, and other issues that can undermine system reliability and reporting integrity.

4

Application Security

Application security validation entails a comprehensive assessment of the application's security design, including Segregation of Duties (SOD), sensitive access controls, and role definitions. The process needs to include a detailed review of documentation related to the configuration of application roles, validating that these roles are clearly defined, appropriately structured, and consistent with the organization's security policies.



Sensitive Access and Segregation of Duties (SOD) Rules

Documentation concerning sensitive access and SOD rules need to be reviewed to validate that rights are properly assigned to roles and that there are no conflicts that may jeopardize security or regulatory compliance.



User Access Provisioning and Administration Process Design

Documentation regarding user access provisioning and administration processes need to be examined to confirm procedures for granting, modifying, and revoking user access are robust, well-structured, and effectively implemented.



Review of User Provisioning Prior to Go-Live

Assessment of users provisioned before go-live must be reviewed to confirm that only authorized personnel were granted access prior to system go-live.



Security and Privileged Access Management During Hyper-Care

The final stage focuses on the monitoring of privileged access, especially amongst support teams during the hyper-care period, to confirm elevated rights are appropriately managed and associated risks are properly mitigated.

5

IT General Controls

As part of system implementation, a thorough evaluation needs to be conducted on the organization's documentation related to the design of IT general controls for application, database, and operating system layers to validate that control measures are effectively designed and implemented. The evaluation aims to confirm that fundamental IT control is established and operate as intended across all relevant layers.

Additionally, the evaluation verifies whether segregation of duties is adequately maintained within the application layer. This includes assessing controls over access, such as distinguishing application administrators from business users. Validating proper allocation of responsibilities among distinct individuals or roles mitigates the risk of unauthorized access and reinforces the overall control environment.

Is Your Company Considering ERP System Implementation?

System implementations are transformative but inherently risky. Success depends on strategic alignment, disciplined project management, robust change management, and rigorous audit readiness. Internal and external audit teams increasingly play an important role throughout the project lifecycle, providing timely insights and helping to identify control gaps before they escalate.

Organizations planning or executing a system implementation should take action early - engaging experienced technology risk assurance professionals before go live can help identify gaps, strengthen controls, and validate the system supports business and reporting objectives from day one. For further support, contact [BDO's Technology Risk Assurance](#) team to discuss tailored solutions for your next system implementation.



Have questions or want to learn more? CONTACT US!

At BDO, our purpose is to be the people you count on to grow with confidence and achieve what matters most. Our professionals provide assurance, tax and advisory services for a diverse range of clients across the U.S. and in over 160 countries through our global organization. We are proud to be an ESOP company, inspiring an ownership mindset that enables our collective success.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C., a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. For more information, please visit: www.bdo.com.

© 2026 BDO USA, P.C. All rights reserved.

