Proactively Managing ERP Risks

January 7, 2010
Introductions and Objectives

• Establish a structured model to demonstrate the variety of risks associated with an ERP environment
• Discuss control areas that can help manage these risks and understand how to proactively ensure they’re utilized
• Share ideas for increasing value through effective control deployment strategies
Defining the Risk Universe
ERP Risk Universe

- Project Risk
- Business Process Risk
- Security Risk
- Enterprise Data Risk
- Environment Risk
- SOX / Compliance Risk

Responsible Parties
# ERP Risk Universe

## Project Risk
- Business Strategy Alignment
- Project Change Management
- Organization Change Management
- Testing Strategy
- Go / No Go Decision
- Post Go-Live Stabilization

## Business Process Risk
- Spreadsheet Rationalization & Controls
- Configurable Application Controls
- Manual Process Controls
- IFRS adoption

## Security Risk
- Segregation of Duties & Sensitive Access
- User / Role Provisioning Processes
- Overall Security Architecture
- IDM Integration

## Enterprise Data Risk
- Master Data Standards
- Data Governance Process
- Data Migration Quality Review

## Environment Risk
- IT Infrastructure Controls
- Application Interface Controls
- Application Change Management

## SOX / Compliance Risk

---

© 2010 Protiviti Inc

protiviti®
ERP Risks and Implementation Stages

Net New
- Implementing ERP for the first time
- Replacing legacy systems
- Developing new interfaces and implementing new processes

Rollout
- Applying ERP template/model to different locations or business processes or outsourcing entities

Upgrade*
(Technical / Functional)
- Re-engineering ERP processes and/or configuration
- Consolidating ERP instances

Maintenance
- Live with ERP for some time; focus is maintenance
- Will most likely upgrade soon

Where are you now?

Each of the above project stages introduces risks
Project Risk

Project Risk

Business Strategy Alignment
Project Change Management
Organization Change Management

Testing Strategy
Go / No Go Decision
Post Go-Live Stabilization

Business Process Risk

Security Risk

PMO
Steering Committee
Implementation Teams
Audit / Compliance
Controls Teams
BPOs

Enterprise Data Risk

Environment Risk

SOX / Compliance Risk

Powerful Insights.
Proven Delivery.™
What Are Your Odds for Success in Difficult Implementations and Transformational Initiatives?

1. Success is Rare …

- LATE - 93% took longer than expected / 68% took “much longer”
- OVER BUDGET - 65% were over budget – 17% were >15% over – 16% were 50% or more over
- MISSED BENEFITS - Only 21% realized 50% of the benefits
- IMPAIRED THE BUSINESS - 57% experienced major operational disruptions

2. … and Your Odds Don’t Improve …

- Inexperience Yields Optimism – Seasoned veterans know what can go wrong will
- Failures in Project Management – Leadership falls victim to being in the fray vs. seeing it clearly
- Resistance to Change – Org. change mgmt. makes technical work look easy
- Loose Governance – With this much at risk, these initiatives require special structures and processes
- Strategic and Tactical Misalignment – Challenged to meet the budget and schedule vs. the business case
- Conflicts of Interest – Every player in the initiative has a “dog in the hunt”
The application of knowledge, skills, tools and techniques to project activities in order to meet or exceed stakeholder needs and expectations.

The processes that are applicable to whatever the project is intended to accomplish: strategy, selection, design, implementation, or support.

The management and integration framework within which a project operates.

The internal and external environment within which a project operates.
Sample Framework Areas & Categories

Initial and ongoing project risk assessments that consider key control areas across the strategic initiative form the foundations for conclusions and recommendations.

### Project Management

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Rating</th>
<th>Status Change</th>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Project Office</td>
<td></td>
<td></td>
<td>o 8</td>
</tr>
<tr>
<td>B. Scope</td>
<td></td>
<td>+ 5</td>
<td>5</td>
</tr>
<tr>
<td>C. Time</td>
<td></td>
<td>o 5</td>
<td>5</td>
</tr>
<tr>
<td>D. Cost</td>
<td></td>
<td>o 4</td>
<td>4</td>
</tr>
<tr>
<td>E. Quality</td>
<td></td>
<td>o 3</td>
<td>3</td>
</tr>
<tr>
<td>F. Human Resource</td>
<td></td>
<td>o 3</td>
<td>3</td>
</tr>
<tr>
<td>G. Communication</td>
<td></td>
<td>- 3</td>
<td></td>
</tr>
<tr>
<td>H. Risk</td>
<td></td>
<td>o 4</td>
<td>4</td>
</tr>
<tr>
<td>I. Procurement</td>
<td></td>
<td>o 6</td>
<td>6</td>
</tr>
</tbody>
</table>

### Project Support

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Rating</th>
<th>Status Change</th>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>P. Program Office</td>
<td></td>
<td></td>
<td>o 5</td>
</tr>
<tr>
<td>Q. Integration with Common Business Functions</td>
<td></td>
<td></td>
<td>o 5</td>
</tr>
<tr>
<td>R. Strategic Alignment</td>
<td></td>
<td></td>
<td>o 3</td>
</tr>
<tr>
<td>S. Corporate Culture</td>
<td></td>
<td></td>
<td>o 4</td>
</tr>
<tr>
<td>T. Stakeholders</td>
<td></td>
<td></td>
<td>- 4</td>
</tr>
<tr>
<td>U. Business Environment Risk</td>
<td></td>
<td></td>
<td>o 11</td>
</tr>
<tr>
<td>V. Process Alignment</td>
<td></td>
<td>+ 4</td>
<td>4</td>
</tr>
<tr>
<td>W. Portfolio Management</td>
<td></td>
<td></td>
<td>o 4</td>
</tr>
</tbody>
</table>

### Project Environment

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Rating</th>
<th>Status Change</th>
<th>Risk Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>J. Planning and Initiation</td>
<td></td>
<td></td>
<td>o 6</td>
</tr>
<tr>
<td>K. Current State Assessment</td>
<td></td>
<td></td>
<td>o 4</td>
</tr>
<tr>
<td>L. Requirements Definition</td>
<td></td>
<td>+ 7</td>
<td>7</td>
</tr>
<tr>
<td>M. Solution Selection</td>
<td></td>
<td>+ 8</td>
<td>8</td>
</tr>
<tr>
<td>N. Implementation Planning</td>
<td></td>
<td>+ 8</td>
<td>8</td>
</tr>
<tr>
<td>O. Business Case To Proceed</td>
<td></td>
<td>+ 7</td>
<td>7</td>
</tr>
</tbody>
</table>

### Risk Status

1. Unlikely to occur and low impact of risk occurring.
2. Unlikely to occur and moderate impact or risk occurring.
3. Possible chance and/or moderate impact of risk occurring.
4. Possible chance and/or significant impact of risk occurring.
5. Likely chance and/or significant impact of risk occurring.

Key:
+ Risk has increased since prior review
- Risk has decreased since prior review
° Risk unchanged since prior review
Addressing Project Risk

<table>
<thead>
<tr>
<th>Control Focus Areas</th>
<th>Net New</th>
<th>Rollout</th>
<th>Upgrade</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Establish project risk profile and assessment plans</td>
<td>• Same as Net New with scope limited</td>
<td>• Same as Net New with scope limited</td>
<td>• As requests for changes are converted into approved projects with significant risks, same as Net New with scope limited</td>
<td></td>
</tr>
<tr>
<td>• Infuse project management with importance of controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Review project artifacts, milestones, approvals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Assess adherence to project management standards and practices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Provide independent reporting to PMO and leadership on effectiveness of project risk management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Assess attention to achievement of business case</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Provide input to PMO standards development</td>
<td>• Keep auditors (internal, external, compliance) aware of project changes</td>
<td>• Assess organizational readiness plans for changes coming</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Business Process Risk

- Spreadsheet Rationalization & Controls
- Configurable Application Controls
- Manual Process Controls
- IFRS adoption

- Enterprise Data Risk
- Audit / Compliance Controls Teams
- BPOs

- Project Risk
- PMO
- Steering Committee Implementation Teams

- Security Risk
- Environment Risk

SOX / Compliance Risk

Powerful Insights. Proven Delivery.™
Controlling Business Process Risk

Control Options
- Application (Configurable) Controls – e.g. field edits, workflow, data validations, default values, tolerances, account mappings, and error messages
- Manual Controls – e.g. policies and procedures, reviews and approvals, reconciliations, and management reporting

Investing in appropriate design and implementation of automated controls provides multiple benefits, including:
- Improved reliability
  • reduced “human error” factor
  • consistent performance
  • improved auditor reliance
- Less costly to perform
  • reduced man-hours
  • less re-work for issues discovered downstream
- Significantly less costly to test
  • test of one vs. transaction testing
  • reduced need for periodic confirmation
  • increased ability to test with automated tool(s)
## Spreadsheet Control Considerations

<table>
<thead>
<tr>
<th>Ref</th>
<th>Control</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>All “critical” end user applications are maintained in a current and accurate inventory.</strong> Define scoping criteria for spreadsheets that support Statutory Financial Reporting and/risk-rank spreadsheets. <strong>Focus on key controls for the end-to-end process</strong>, not just spreadsheet controls. Consider broadening scope to address operational risk i.e. non-financial reporting spreadsheets. Use of software is emerging as a leading practice.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Spreadsheets are subject to a <strong>logic inspection to baseline functionality</strong>. Identified errors and significant design issues are remediated. Use of software to facilitate logic inspection is a leading practice. Focus on design and formula logic &amp; consistency.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>File naming conventions and storage locations are implemented to enforce <strong>version control</strong>.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><strong>Input controls</strong> are in place to ensure complete, accurate and valid data input. Programmed control totals and data validation are leading practice.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Changes are recorded</strong> in a centralized log and are subject to review to ensure they function as intended. Changes to high risk/highly complex spreadsheets should be subject to <strong>testing/validation</strong>.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td><strong>Access</strong> to spreadsheet files is restricted** based on job roles and to enforce segregation of duties. Further restriction and password controls at the file, sheet and cell level is leading practice. Use of document management and spreadsheet management solutions is emerging as leading practice.</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Spreadsheets are subject to <strong>periodic backup</strong> to ensure recoverability.</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Critical spreadsheets are supported by current and accurate <strong>documentation</strong>. Documentation should include purpose of spreadsheet, instructions for use, key assumptions, authorized users, logic for key calculations, description of VBA, inputs/external links and key outputs. Good practice is to include documentation as part of the spreadsheet or in a document management/spreadsheet management solution. Good documentation will significantly reduce the risks associated with staff turnover/insufficient succession planning.</td>
<td></td>
</tr>
</tbody>
</table>

Any approach should be **risk-based** and not all controls may be required for each spreadsheet.
## Addressing Business Process Risk

### Net New
- Provide input to process controls design – e.g. approvals, reconciliations, configurations, spreadsheets, etc.
- Identify and document control requirements – manual, automated, business
- Educate business process teams around functionality & supporting controls
- Test controls throughout the implementation phases
- Provide input on control monitoring tool implementation

### Rollout
- Define control parameter customization
- Define control monitoring processes, roles and responsibilities
- Assess local control environment to confirm adherence with standards
- Test reports from a controls perspective
- Help identify and assign mitigating controls
- Review/adjust control monitoring standards and tools

### Upgrade
- Review control enhancements
- Confirm that control changes were approved by proper monitoring processes
- Assess change control environment to confirm adherence with standards
- Review/adjust control monitoring standards and tools
- Update control documentation

### Maintenance
- Review control changes
- Perform transactional data analysis to identify control gaps (e.g. duplicate invoices)
- Conduct periodic assessments to review adherence to process control standards, potential enhancements, or data integrity issues
- Keep auditors (internal, external, compliance) aware of control changes
- Monitor process indicators, delays / breakdowns

© 2010 Protiviti Inc
Security Risk

Security Risk

Segregation of Duties & Sensitive Access
User/Role Provisioning Processes
Overall Security Architecture
IDM Integration

Business Process Risk

Project Risk

PMO
Steering Committee
Implementation Teams

Audit/Compliance
Controls Teams
BPOs

Enterprise Data Risk

Environment Risk

SOX/Compliance Risk
Controlling Security Risk

- Security Administration
  - Provisioning user IDs
  - Documented approvals
  - Password parameters
  - Monitoring security reports and audit logs
- Segregation of duties
  - Separation of incompatible functions
  - Monitoring access levels
- Sensitive access & privacy
  - Limiting access based on business need
  - Controlling powerful authorities
  - Limiting access to comply with privacy regulations (e.g. PCI, HIPAA)
- Technologies and tools
# Addressing Security Risk

## Control Focus Areas

<table>
<thead>
<tr>
<th>Net New</th>
<th>Rollout</th>
<th>Upgrade</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide input to security standards and/or develop Security Governance strategy</td>
<td>• Review/signoff on role design and assignment</td>
<td>• Review/signoff on role design and assignment</td>
<td>• Review effectiveness of security monitoring procedures</td>
</tr>
<tr>
<td>• Review/signoff on role design</td>
<td>• Test SOD and sensitive access during rollout to confirm adherence with compliance standards</td>
<td>• Test new role design (i.e. UAT) prior to migration to production</td>
<td>• Assess SOD/sensitive access exposures</td>
</tr>
<tr>
<td>• Educate security and process teams around controls</td>
<td>• Identify and assign mitigating controls</td>
<td>• Test SOD and sensitive access during upgrade to confirm adherence with compliance standards</td>
<td>• Review/adjust SOD rules, to reflect new transactions and functionality</td>
</tr>
<tr>
<td>• Test SOD and sensitive access throughout project (role and user level) and provide remediation feedback</td>
<td>• Confirm that security monitoring tools are used properly – procedures, roles and responsibilities are defined</td>
<td>• Review/adjust security monitoring tool, to reflect new transactions and functionality</td>
<td>• Confirm end users are executing assigned mitigating controls</td>
</tr>
<tr>
<td>• Provide input on security monitoring tool implementation</td>
<td></td>
<td>• Update documentation</td>
<td>• Monitor access to powerful roles and transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Keep auditors (internal, external, compliance) aware of security standard changes</td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Data Risk
Controlling Enterprise Data Risks

- Data Migration
  - Data Conversion
    - data mappings
    - conversion design
    - conversion testing
    - reconciliations
  - Data Cleansing
    - inactive data
    - duplicative data
    - erroneous data
    - “business relevant” data
  - Technologies and tools

- Data Governance
  - Master Data Maintenance
    - data ownership
    - data standards
    - policies and procedures
    - impact analysis
  - Data Archiving
    - performance and storage requirements
    - data access requirements
    - data redundancy
  - Technologies and tools
Sample Benefits of Strong Data Governance

a. Streamlined future data conversions and implementation of reporting capabilities
b. Improved reporting accuracy and data reliability for ongoing strategic and operational management decisions
c. Efficiencies gained from use of “single book of record”
d. Improved visibility into revenue and cost drivers for management review and decisions
e. Improved capabilities to leverage information for vendor / customer negotiations and risk management
f. Reduction in ongoing master data maintenance efforts
g. Improved litigation readiness (e-Discovery)
h. Improved ability to identify, retrieve, use, preserve, and purge electronic information
i. Alignment of enterprise information management with security, legal, compliance, audit, operations, and training
j. Improved sustainability of SOX and operational compliance
k. Increased ability to perform high-value audits
# Addressing Enterprise Data Risk

<table>
<thead>
<tr>
<th>Control Focus Areas</th>
<th>Net New</th>
<th>Rollout</th>
<th>Upgrade</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Review conversion standards / documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Analyze data conversion testing results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Test data controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Validate user acceptance of data results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Confirm archiving is adequately addressed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Validate legacy systems are appropriately decommissioned/ archived and access is appropriately limited</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Assess local control environment to confirm adherence with standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Test reports for data consistency</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Confirm appropriate controls are in place for sensitive data</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Review data management enhancements</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Assess change control environment to confirm adherence with standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Review /adjust data management standards and tools to reflect new functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Conduct periodic assessments to review adherence to data governance standards, potential enhancements, or data integrity issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Implement passive and active data governance processes to improve data quality</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Work with data management organization to obtain data needed for additional audits</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Update control documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Keep auditors (internal, external, compliance) aware of data control changes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Review noted issues and resolutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2010 Protiviti Inc
Planning for ERP Risk Management

**Business Context**
- Prior implementations
- Risk appetite
- Outside assistance
- Business complexity
- Application scope

- Assess your risk
- Determine IA role
- Identify resources
- Develop plan
- Participate in GRC tool selection and deployment
- Execute plan and monitor progress
Summary

• Understand implementation and project plans
• Get involved in early stages of projects by providing input from a risk and compliance perspective
• Ensure proper control ‘ownership’ is defined and communicated within organization
• Bring the right skills – configuration, business, security, audit, data management, etc.
• Use tools – it is time consuming to properly assess these risks and controls manually
• Your goals when assessing and providing recommendations should include:
  – Standardize control design and achieve incremental value
  – Help find the right balance between automated and manual controls
  – Help address potential control gaps
  – Confirm that right people have authority to approve changes design changes impacting your control environment
  – Tools used by implementation or compliance teams are built the right way to test and monitor security exposures
  – Assess your environment periodically and with the right depth of analysis
Thank you for your attention.

*Powerful Insights.*
*Proven Delivery.*™