ERP Auditing Concepts for Financial Auditors

Dallas IIA CAST Meeting
March 1, 2012

Presented by: Terry Hartzog, Protiviti Director
Introduction of Presenters

Terry Hartzog
Protiviti
Director
Internal Audit

• Terry is founding member and current Director with Protiviti, Inc., a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Terry has provided internal audit and consulting services for over 13 years across a variety of industries and sizes of organizations. Terry’s experience encompasses traditional financial and operational internal audit and SOX as well as significant experience in building and enhancing controls and security during the design and implementation phases of major ERP projects including SAP and Oracle. Terry’s internal audit experience ranges from providing specific singular audits to serving as the acting Director of Internal Audit for a mid-size company leading the integration of the audit and SOX functions.

• Terry is a graduate of Texas A&M University with a degree in Accounting and Information/Operations Management. Terry is a CPA, CIA and current Board of Governor/former President of the Fort Worth IIA chapter. Outside of work, Terry enjoys spending time with his wife and 4 children and promoting all things Aggie.
Today’s Discussion Topics

Many Internal Auditors tend to rely on IT Audit specialist to audit “settings” in ERP environments because they may not be comfortable with technical aspects or fully understand the technology. This approach can severely limit the value potential you can bring to your organization. This training will provide Financial Internal Auditors with ERP auditing concepts that will allow them to better evaluate how well their organization’s ERP enables and controls key business processes.

Learning Objectives:

➢ Understand the type of business process risks that can be mitigated by ERP control automation
➢ Learn key concepts about a four-pronged approach to auditing business process risk in an ERP environment that includes assessing:
  ✓ Preventive Security/SOD Controls
  ✓ Preventive Process Configurable Controls
  ✓ IT General Controls
  ✓ Detective Data/Transaction Analysis
Which process areas should internal auditors consider user access/SOD controls and configurable controls?
The Changing Business Focus

Where we’ve been

- Reactive
- Historical Results
- Internal Control
- Budgeting
- Financial Statements
- Variance Analysis

Expanding Competencies

- 72% Transaction Processing
- 28% Strategic Activities

Sharing Knowledge

- 75% Strategic Activities
- 25% Processing

Initiating Change

Tomorrow’s Goal

- Proactive
- Key Performance Indicators
- Business Analysis
- Future Projections
- Manage Business Risks
- Integrated Models Linking Strategy and Forecasting

28% Strategic Activities

72% Transaction Processing

75% Strategic Activities

25% Processing
Enabling Sustained Compliance

### Maximize / Optimize Automated Controls

<table>
<thead>
<tr>
<th>Configured Controls</th>
<th>Security/SOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Understand Existing Control Environment</td>
<td>• Design security rule-set</td>
</tr>
<tr>
<td>• Design/Assess “to be” controls</td>
<td>• Assess designed roles and assignments</td>
</tr>
<tr>
<td>• Identify impact, opportunities &amp; potential gaps</td>
<td>• Identify potential gaps</td>
</tr>
<tr>
<td>• Recommend control &amp; process changes (automated &amp; manual)</td>
<td>• Evaluate gaps and mitigating controls</td>
</tr>
<tr>
<td></td>
<td>• Facilitate role redesign</td>
</tr>
<tr>
<td></td>
<td>• Clean up assignments</td>
</tr>
</tbody>
</table>

### Continuous Monitoring & Automated Testing

<table>
<thead>
<tr>
<th>Various Tools available</th>
<th>Various Tools available</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Configuration/setup change management</td>
<td>• Continuous or periodic independent audit / testing</td>
</tr>
<tr>
<td>• User setup request and approval</td>
<td>• Master data change management and monitoring</td>
</tr>
<tr>
<td>• SOD monitoring, analysis, mitigation documentation</td>
<td>• Transaction monitoring</td>
</tr>
</tbody>
</table>

### Prepare

- Attain
- Maintain

©2012 Protiviti Inc. This document may not be copied nor distributed to any third party. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.
Who needs to be engaged and when?

<table>
<thead>
<tr>
<th>Analyze</th>
<th>Standardize &amp; Automate</th>
<th>Monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan and Scope</td>
<td>Determine Action Plans</td>
<td>Enable Continuous Monitoring</td>
</tr>
<tr>
<td>Analyze Business Processes</td>
<td>Implement Changes</td>
<td></td>
</tr>
</tbody>
</table>

- **Objective**
  - Evaluate the current state health of the environment and supporting processes
  - Prioritize and then remediate vulnerabilities and weaknesses
  - Build efficiency, sustainability, & continuous monitoring into processes and controls

- **People**
  - Project Managers, ERP Consultants, Business Process Owners, *Internal Audit*
  - Business Process Owner, ERP Consultants, IT Management, Compliance, *Internal Audit*
  - IT Management, ERP Consultants, Compliance, *Internal Audit*

- **Systems**
  - Core ERP Application, ERP Add-Ons, Legacy Applications
  - Core ERP Application, ERP Add-Ons, Legacy Applications
  - Governance Risk and Compliance Applications

© 2012 Protiviti Inc. This document may not be copied nor distributed to any third party.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.
How well has your company leveraged your ERP? Data analysis can give you an indicator.

<table>
<thead>
<tr>
<th>Process</th>
<th>Data Analysis Testing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>Useful Life Analysis</td>
</tr>
<tr>
<td>Assets</td>
<td>High privileged users maintaining asset details</td>
</tr>
<tr>
<td>Assets</td>
<td>Duplicate assets</td>
</tr>
<tr>
<td>Assets</td>
<td>Asset integrity analysis</td>
</tr>
<tr>
<td>HR</td>
<td>Duplicate employee analysis</td>
</tr>
<tr>
<td>HR</td>
<td>Employee master record integrity analysis</td>
</tr>
<tr>
<td>HR</td>
<td>Vendor versus employee bank accounts</td>
</tr>
<tr>
<td>HR</td>
<td>Employee master records maintained by a privileged user</td>
</tr>
<tr>
<td>Order to Cash</td>
<td>High privileged users creating customer records</td>
</tr>
<tr>
<td>Order to Cash</td>
<td>Customer integrity analysis</td>
</tr>
<tr>
<td>Order to Cash</td>
<td>Duplicate customer analysis</td>
</tr>
<tr>
<td>Order to Cash</td>
<td>Inactive customers</td>
</tr>
<tr>
<td>Order to Cash</td>
<td>Customer records created by non approved users</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Benfords law analysis of invoice payments</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Duplicate invoice assessment</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Invoice and vendor processing breaches of segregation of duties</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Duplicate vendor analysis</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>High privileged user processing invoice transactions</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Changes to vendor bank account details</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Large and one off vendor payments</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Invoices paid to alternative vendors</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Vendors without any recent activity in the vendor master</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>High privileged users performing vendor maintenance functions</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Vendor maintenance transactions performed by non approved users</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Payments without a reference to a PO</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Vendors with only post box addresses</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Differences in terms of payment allocated to the vendor compared to invoice payments</td>
</tr>
<tr>
<td>Procure to Pay</td>
<td>Invoice processing in conflicting companies</td>
</tr>
</tbody>
</table>
Case Study:

Managing Procure to Pay Risks via ERP Controls
Procure to Pay Overview and Key Risks & Controls

**Supplier Management (Vendor Master File)**
- Duplicate Vendors
- Unauthorized Vendors
- Incorrect 1099 reporting
- Unrealized vendor discounts
- Undocumented vendor quality/rating/analysis

**Purchasing**
- Unauthorized Purchases
- Inaccurate Purchase Order Processing
- Unauthorized returns, adjustments, and allowances

**Accounts Payable**
- Incomplete or inaccurate payment information from PO/Invoice
- Duplicate payments
- Liabilities and disbursements are not completely recorded in G/L
- Paid invoices do not represent good / services actually received

**ERP Controls**
- **Preventive Security / SOD Controls**
- **Preventive Process Configurable Controls**
- **Detective Data / Transaction Analysis**

**Other Controls**
- Manual Controls (Approvals)
- General IT Controls
- Policies and Procedures
Vendor Master Risk and ERP Controls

Vendor Master Risks

- Duplicate Vendors
- Unauthorized Vendors
- Incorrect 1099 reporting
- Unrealized vendor discounts
- Undocumented vendor quality/rating/analysis

Potential ERP Controls

- User access restrictions to perform vendor maintenance is restricted to a limited # of Master Data Team Members*
- Automated SOD rule set that prevents users from having conflicting functions to create a vendor and create a PO*
- Required / suppressed fields for vendor master data **
- Duplicate check settings for new vendors**
- Dual authorization for sensitive field changes (e.g., bank accounts)**
- Warning messages for potential duplicates before vendor creation**
- Duplicate check settings for exception reporting and data analytics for potential duplicates after vendor creation**

* Control relies on security administration ITGC
** Control relies on change management ITGC
PO and Invoice Processing (Invoice Processing Risk)

**Common Optimization Opportunities**
- Incomplete or inaccurate payment information from PO/Invoice
- Duplicate payments
- Liabilities and disbursements are not completely recorded in G/L
- Paid invoices do not represent good / services actually received

**ERP Controls**
- User access restrictions to create PO’s or post invoices is restricted to a limited # of Procurement and A/P personnel, respectively*
- Automated SOD rule set that prevents users from having conflicting functions to create a PO and post an invoice*
- Tolerance level settings – allowing/rejecting PO pricing and quantities variances to invoices**
- Tolerance level message settings – warning and error messages**
- Exception reporting and data analytics for invoices paid that do not comply with 3-way match requirements requiring goods ordered by to match goods received to match vendor invoices**

* Control relies on security administration ITGC  
** Control relies on change management ITGC
So What? Is it worth it?

In a recent engagement including control optimization for all business processes (Procure to Pay, Order to Cash, Human Resources, and General Ledger), we were able to transform the overall internal control framework from primarily manual (68%) to primarily automated and semi-automated (64%).

Additionally there was a 40% control count reduction due to increased reliance on the new automated SAP controls.
So What? How much is it worth?

**Overall Annual SOX Cost Savings:**

<table>
<thead>
<tr>
<th>SOX Control Performance Cost Savings</th>
<th>+ SOX Control Testing Cost Savings</th>
<th>= Total Estimated ANNUAL SOX Cost Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>$207,698</td>
<td>$419,875</td>
<td>$627,523</td>
</tr>
</tbody>
</table>

**SOX Control Performance Cost Savings:**

\[
\left( \frac{\text{# Manual Control Reductions}}{\text{# Semi-Auto Control Increases}} \right) \times \text{Control Performance Hours} \times \text{Average Hourly Rate} = \text{Control Performance Savings}
\]

- \(197\) Manual Control Reductions - \(16\) Semi-Auto Control Increases
- \(25.5\) Control Performance Hours
- \($45\) Average Hourly Rate

\[
197 \times 25.5 \times 45 = \$207,698
\]

**SOX Control Testing Cost Savings:**

\[
\text{(Testing Rate)} \times (\text{SOX Hours Reduction})^* = \text{SOX Testing Cost Savings}
\]

- \($125\) Testing Rate
- \(3,359\) SOX Hours Reduction

\[
125 \times 3,359 = \$419,875
\]

*SOX Control Testing Hours Reduction was jointly determined by Client Compliance & Protiviti.*
Q & A