Who We Are

- Randy Roehm – Technology Risk Director
- Jason Brucker – Technology Risk Manager
- Zeb Buckner – Internal Audit Consultant
  - Zeb.buckner@protiviti.com
- Darcie Allen – Denver HR & Recruiting Lead
Protiviti Overview

Consulting
- Finance Transformation
- Operational Risks
- IT Strategy Services
- Business Intelligence
- Enabling Technologies
- Governance Risks and Controls

Internal Audit
- Internal Audit Start-Up
- Co-Sourcing
- Outsourcing
- Internal Audit Transformation
- Risk Assessment

Large Firm:
- Methodologies & tools
- Experienced professionals
- Depth of consulting services
- Financial stability
- Global presence

Specialist firms:
- Responsive client service
- Lack of SEC restrictions
- Independent from attest & tax services
- Better teaming
- Focus on core offerings

Protiviti combines the strengths of the Big Four and independent alternatives... without compromise.
About Protiviti

• Client engagements vary in size: typically $75K to several million.
• Protiviti's revenues for fiscal year 2006 were over $0.5 billion.
• More than 3,000 professionals worldwide.
• Wholly owned subsidiary of Robert Half International Inc.
• Protiviti was listed as one of Businessweek’s top 100 places to start a career in 2006 and 2007.
Example Clients

Our clients include more than 20% of all Fortune 1000 companies; more than 25% of all Fortune 500 companies; and more than 35% of all Fortune 100 companies.*

*All logos used with client permission
“Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance process.”

- The Institute of Internal Auditors
“Information Technology (IT) internal auditing helps a company understand the key technology risks and how well the company is mitigating and controlling those risks. IT internal audit also provides insight into the threats inherent in today's highly complex technologies.”

- Protiviti IT Audit Services
“Internal control is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of [business] objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.”

- Committee of Sponsoring Organizations (COSO)
Key Publications / Resources

- COSO
- COBIT
- ITIL
- Val IT
- ITPI
The IT Process Institute (ITPI) is a non-profit organization with the mission to “advance IT management science through independent research, benchmarking, and prescriptive guidance.”

- Differentiating Factors – Top Performers vs. Medium Performers
  - The activities that “sustain and continually improve their control systems”
  - These are activities such as enforcing processes and consistent use of other controls to proactively stabilize the IT environment
- Differentiating Factors – Medium Performers vs. Low Performers
  - The activities that organizations use to “build their control systems”
  - These are activities such as defining processes, roles and service levels
Protiviti Tools

- Protiviti Technology Risk Model
- Process Classification Scheme
- Capability Maturity Model
- 6 Elements of Infrastructure
- KnowledgeLeader
Process Classification Scheme (PCS)

Universal Processes
1.0 Understand Markets & Customers
2.0 Develop Vision & Strategy
3.0 Develop & Manage Human Resources
4.0 Manage Information Technology & Resources
5.0 Manage Financial, Accounting & Tax Functions
6.0 Manage Fixed Assets & Facilities
7.0 Manage External Relations
8.0 Manage Internal Audit & Enterprise Wide Risk

Industry Processes
- Communication
- Energy & Utility
- Financial Services & Real Estate
- Government, Education & Not-For-Profit
- Healthcare
- Manufacturing, Distribution & Technology
- Media, Hospitality & Professional Services
- Packaged Consumer Goods & Retail
- Other Industries / Generic

4.1 Define IT Strategy & Organization
4.2 Manage Security & Privacy
4.3 Deploy & Maintain Solutions
4.4 Manage IT Infrastructure
4.5 Manage IT Assets
4.6 Support End Users
4.7 Ensure Continuity

4.4.1 Manage Data Center Operations
4.4.2 Manage Technical Infrastructure
4.4.3 Performance Planning/Monitoring
4.4.4 Project Management Risk
6 Elements of Infrastructure

The "6 Elements of Infrastructure"
- Describes the components needed to ensure quality & risk management
- Are generally designed *from left to right* as shown above
- Each component contributes to the overall process maturity of each area
- Describes the "necessary ingredients" for mitigating risk to strategies the business deems critical

Resulting Business Risk if component is deficient:
- Process does not achieve strategy
- People cannot perform process
- Reports do not provide information for effective management
- Methodologies do not adequately analyze information
- Information is not available for analysis and reporting
## Capability Maturity Model

<table>
<thead>
<tr>
<th>Capability Level</th>
<th>Capability Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Optimizing</strong></td>
<td>CONTINUOUS IMPROVEMENT</td>
</tr>
<tr>
<td></td>
<td>Continuously improving controls enterprise-wide</td>
</tr>
<tr>
<td><strong>Managed</strong></td>
<td>QUANTITATIVE</td>
</tr>
<tr>
<td></td>
<td>Risks managed quantitatively enterprise-wide</td>
</tr>
<tr>
<td></td>
<td>“Chain of accountability”</td>
</tr>
<tr>
<td><strong>Defined</strong></td>
<td>QUALITATIVE/QUANTITATIVE</td>
</tr>
<tr>
<td></td>
<td>Policies, process and standards defined and institutionalized -- “Chain of certification”</td>
</tr>
<tr>
<td><strong>Repeatable</strong></td>
<td>INTUITIVE</td>
</tr>
<tr>
<td></td>
<td>Process established and repeating; reliance on people continues -- Controls documentation lacking</td>
</tr>
<tr>
<td><strong>Initial</strong></td>
<td>AD HOC/CHAOTIC</td>
</tr>
<tr>
<td></td>
<td>Control is not a priority -- Unstable environment leads to dependency on heroics</td>
</tr>
</tbody>
</table>

Derived from Carnegie Mellon capability maturity model
KnowledgeLeader

• Overview of KnowledgeLeader (KL)
  – Subscription based information website
    • Free to students and professors
  – Aids the Internal Auditor by providing
    • Audit programs
    • Checklists
    • Tools
    • Resources
    • Best practices
  – Risk management professionals can save time, manage risk, and add value
  – KL Demo at end of presentation (time permitting)
Protiviti IA Methodology

Embrace IIA Standards

Attribute Performance Implementation Practice Advisories

Plan and Create Infrastructure

COSO ERM

Identify and Assess Risk

Create Overall Internal Audit Plan

Identify Controls and Evaluate

Test Controls

Report

Monitor and Follow-up

Oversight Insight Foresight

Add Value

Planning Execution / Field Work Reporting

Entity Level Process/ Location/ Transaction/ Level

Entity Objectives Change

Identify and Assess Risk

Control Self Assessment

Plan and Create Infrastructure

Understand Analyze Activity

Set Objectives and Plan

Identify and Prioritize Risks

Identify Controls and Evaluate

Test Controls

Report

Create Overall Internal Audit Plan

© 2008 Protiviti Inc. This document is for your company’s internal use only and may not be distributed to any third party.
Audit Planning

Objective

Understand project environment, objectives, and scope. Identify process best practices. Identify information needed to carry out the audit.

Approach

- Understand and Analyze Activity
- Set Objectives and Plan
- Identify and Prioritize Risks

Value

A risk-based audit approach focuses an audit on significant risk areas, efficiently utilizing resources to produce effective results that ultimately add value to the client’s organization.
Key Audit Planning Activities

- Conduct the planning meeting with the client to:
  - Determine objectives and scope
  - Understand the key risks (e.g., questionnaires)
  - Request relevant background information / documentation (e.g., past audit findings, org charts, system diagrams, etc.)

- Create the planning and scoping memo
- Create work program
- Determine budget and resource allocation
- Send audit notification letters
Key Planning Documents / Outputs

• Meeting notes / minutes
• Planning memo
• Work program
  – Examples:
    • IT General Controls
    • IT Change management
    • Disaster recovery
    • Windows security
• Budget / staffing plan
• Notification letter
Execution / Field Work

Objective

Perform an evaluation to verify that, for each control objective / risk, controls are designed and operating effectively so there is reasonable assurance that the risk is mitigated to an acceptable level.

Approach

- Identify Relevant Controls
- Assess Control Design Effectiveness
- Develop Test Plans for Controls Designed Effectively
- Evaluate Control Operating Effectiveness

Value

Field work provides internal auditors with the opportunity to identify findings and value added recommendations to the client. These form the basis for well supported conclusions and recommendations.
Key Field Work Activities

• Gain a detailed understanding of the audited area

• Identify and document risks & controls:
  – Determine control characteristics
  – Populate a risk & control matrix (RCM)

• Evaluate control design effectiveness, including linkage to control objectives / risks

• Identify testing steps to validate control operating effectiveness

• Execute testing:
  – Acquire and evaluate data / control evidence
  – Create workpapers
  – Document observations & findings
  – Validate findings with auditee
Documenting Controls

• **What** - What does the control do? Is it preventative or detective?
• **How** - How is the control performed? What is the evidence?
• **Who** - Who performs the control? What is their title?
• **Why** - What is the objective of the control?
• **When** - How frequently is the control performed?
Characteristics of Effective Controls

• Relevant to the control objective / risk under review
• Performed frequently enough
• Personnel performing them have adequate knowledge and experience
• Appropriate segregation of duties exist
• Errors are identified and remediated in a timely manner
• Reliable information is used to perform the control
## Relative Strength of Controls

<table>
<thead>
<tr>
<th>Weaker</th>
<th>Stronger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual control</td>
<td>Automated control</td>
</tr>
<tr>
<td>Performed by junior personnel</td>
<td>Performed by senior personnel</td>
</tr>
<tr>
<td>Detective control</td>
<td>Preventative control</td>
</tr>
<tr>
<td>Complex: many steps</td>
<td>Simple: one step</td>
</tr>
<tr>
<td>High Level</td>
<td>Transactional Level</td>
</tr>
<tr>
<td>Uses Sampling</td>
<td>100% Coverage</td>
</tr>
<tr>
<td>Takes place later</td>
<td>Performed real time</td>
</tr>
</tbody>
</table>
Develop a Test Plan

• A well-developed test plan:
  – Considers control objectives / risks and how controls accomplish those objectives or mitigate the risks
  – May test numerous controls
  – Identifies the population, sample size, and sample selection methodology for the test
  – Describes each step the auditor is to perform
  – Verifies the reports used for sample selection are accurate and reliable
  – Includes only effectively designed controls from the RCM; ineffectively designed controls should be noted as audit findings
### Types of Tests

<table>
<thead>
<tr>
<th>Testing Technique</th>
<th>Explanation</th>
<th>Documentation Requirements</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inquiry</td>
<td>Ascertain whether a control is in place by asking specific oral or written questions</td>
<td>Who was interviewed, when the interview took place and information they provided</td>
<td>Interview key personnel to understand the controls surrounding a particular process</td>
</tr>
<tr>
<td>Observation</td>
<td>Direct viewing of control being performed</td>
<td>Who, when &amp; what was observed</td>
<td>Automated: Observe all field edit check works when invalid data entered Manual: Security of blank check stock</td>
</tr>
<tr>
<td>Inspection/Examination</td>
<td>The inspection of records, documents, reconciliations, and reports for evidence that a control has been properly applied.</td>
<td>Who, when &amp; what. Details of items tested. Level of detail must be sufficient to support conclusion and allow someone else to re-perform your test.</td>
<td>Select a sample of contracts and verify that key controls were performed: • Contract was signed (Validity) • All key fields were completed (Completeness)</td>
</tr>
<tr>
<td>Re-performance</td>
<td>The repetition of a control performed by an employee or a computer or system.</td>
<td>What &amp; how. Details of items tested. Level of detail must be sufficient to support conclusion and allow someone else to re-perform your test.</td>
<td>• Recalculating a bank reconciliation, tracing back to bank statements, and general ledger balance</td>
</tr>
</tbody>
</table>
### Documenting Findings: The 5 C’s

<table>
<thead>
<tr>
<th>Condition</th>
<th>Statement of the issue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion</td>
<td>Description of what should be</td>
</tr>
<tr>
<td>Consequence</td>
<td>Explanation of the significance or impact</td>
</tr>
<tr>
<td>Cause</td>
<td>Explanation of what allowed the condition to occur</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>Description of action necessary to correct the condition</td>
</tr>
</tbody>
</table>
## Example Issue Write-Up Statement

<table>
<thead>
<tr>
<th>Condition</th>
<th>15% of the development team has “write” access to the production environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criterion</td>
<td>The corporate IT security policy dictates that access should be granted according to “least privilege” and developers should not have “write” access to the production environment.</td>
</tr>
<tr>
<td>Consequence</td>
<td>Unauthorized developer activity may introduce unstable and/or malicious changes to the production environment.</td>
</tr>
<tr>
<td>Cause</td>
<td>Developer production access was not reviewed and eliminated when the IT security policy was implemented.</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>The system security administrators will review and disable all developer “write” access in production, and the VP of IT will conduct monthly access reviews to verify no developers have improperly obtained “write” access to production.</td>
</tr>
</tbody>
</table>
Key Field Work Documents / Outputs

• Risk & control matrices (RCMs)
• Testing memoranda / lead sheets
• Workpapers / testing documentation:
  – Data analyses (e.g., spreadsheets)
  – Narratives / procedures
  – Process maps
  – System output (e.g., reports, log files)
• Issue tracker / testing summary
• Completed work program
Reporting

Objective

Summarize and present issues, observations and value-added recommendations based upon fieldwork, sound analysis and business judgment.

Approach

- Determine which issues to Report
- Link Issues to Objectives
- Develop and Present Recommendations

Value

High quality reporting is responsive to specific client needs and is well supported by analysis and test procedure results. Internal audit reports provide companies with a powerful mechanism for making decisions to improve their ability to achieve business objectives.
Compelling Recommendations

• Actionable
• Supported with sufficient evidence
• Focused on the root cause
• Appropriate level of management is involved in issue identification early on
• In line with client priorities and objectives
• Are items the client is ready or able to make changes
• Based on objective and accurate information
• May offer near-term and long-term solutions

**Goal of our audit report:**

To report facts in a manner that puts management in a position to reach informed conclusions on their own.
Adding Value with Recommendations

- How can the process measurements and controls be modified or enhanced?
- What are other companies doing (e.g., benchmarks, standards)?
- Are you missing out on some best practices?
- Where is this process going?
- Can it scale as the company grows?
- Will current controls be adequate in the future?
- What planned or future changes need to be considered?
Knowledge Leader (KL)
Activity – KnowledgeLeader Research

• Objective:
  • Give you the opportunity to perform advance research on the accounts payable process on KnowledgeLeader.

• Deliverables:
  • Examples of planning and process documents that you can utilize from KnowledgeLeader.
<table>
<thead>
<tr>
<th>Tasks</th>
<th>Who/How</th>
<th>Approx. Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Go to the KnowledgeLeader website, knowledgeleader.com.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 2. Identify six documents a consultant could use to prepare for an Accounts Payable review. Two of the six documents should be for the:  
  • planning stage (information gathering)  
  • process documentation stage (risk and control analysis and process flowcharts/ narratives) | Table Group      | 10 minutes   |
| 3. Each table should create a listing of documents they found and indicate what stage the documents could be used. |                  |              |
| Debrief Meeting                                                       | Class Group      | 5 minutes    |
Thank you!