Leveraging IT risk assessment to add value.

Leading Practice IT Risk Assessment

ISACA San Francisco Chapter Luncheon
January 24, 2008
Leading Practice IT Risk Assessment

The Fine Print

This publication contains general information only and Deloitte & Touche LLP is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte & Touche LLP, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this publication.
Today’s discussion

• **Overview:** Leading Practice IT Risk Assessment

• **Performing Risk Assessments for IT**
  – Identifying and Evaluating IT Risks
  – Using IT Risk Frameworks including CobiT
  – Linking IT Risks to Organizational Objectives

• **Creating a Risk Response**

• **Common and Emerging IT Risks**
Leading Practice IT Risk Assessment

- Organizations are focusing on increasing the cost efficiency of their compliance programs while improving the effectiveness of their governance, risk management and compliance programs.

- In this high pressure business environment, how can IT internal auditors perform risk assessments to ensure that internal audit activities link to business objectives and organizational value drivers?
The Role of Internal Audit

• “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 processes.”

Source: The International Standards for the Professional Practice of Internal Auditing (Standards)  
The Institute of Internal Auditors
Typical Company Risk Assessment Activities

Enterprise Risk Management
- Enterprise Risk Assessment

Compliance
- Regulatory Risk Assessments

Internal Audit Risk Assessment
- Business Risks
- IT Risks
- Project Risks
- Vendor Risks
- Location Risks
- Etc.

SOX
- Financial Reporting Risk Assessments
- Control Assessment

Business Continuity
- Business Impact Assessment
The need to improve Governance, Risk Management and Compliance is clear

CURRENT STATE
In some organizations, the current state of governance, risk and compliance processes is disorganized, unnecessarily complex and fragmented.

Adapted from the GRC illustration that appeared in Compliance Week, sponsored by Deloitte Consulting, SAP, and OCEG.
The opportunity exists to simultaneously improve GRC efficiency and effectiveness

**FUTURE STATE**

As with any enterprise process, it is possible to realize a future state where GRC processes are organized, streamlined and efficient. Organizations that accomplish this will unlock hidden value and help drive toward their enterprise objectives.

**Critical Success Factors**

- **Team**
  Leadership alignment and the right mix of skills to see and analyze the entire situation
- **Openness**
  Willingness to listen, face the facts, don’t shoot messengers
- **Enterprise Perspective**
  Get out of siloed thinking to see the big picture
- **Fact-Driven Analysis**
  Accurate, relevant information that reflects reality; use both quantitative and qualitative evidence
- **Clear & Compelling Story**
  Numbers will not speak for themselves – the numeric case must be supported by a narrative case
Evaluating Risk Intelligence

Integrated Enterprise Risk Management Capability

Stakeholder Value

Tribal & Heroic
- Ad-hoc/chaotic
- Depends primarily on individual heroics, capabilities, and verbal wisdom

Specialist Silos
- Independent risk management activities
- Limited focus on the linkage between risks
- Limited alignment of risk to strategies
- Disparate monitoring and reporting functions

Top Down
- Common framework, program statement, policy
- Routine risk assessments
- Communication of top strategic risks to the Board
- Executive/Steering Committee
- Knowledge sharing across risk functions
- Awareness activities
- Formal risk consulting
- Dedicated team

Systemic Risk Management
- Coordinated risk mgmt. activities across silos
- Risk appetite is fully defined
- Enterprise-wide risk monitoring, measuring, and reporting
- Technology implementation
- Contingency plans and escalation procedures
- Risk management training

Risk Intelligent
- Embedded in strategic planning, capital allocation, product development, etc.
- Early warning risk indicators
- Linkage to performance measurement/incentives
- Risk modeling/scenarios
- Industry benchmarking
The Level of Internal Audit’s Effort is Dependent of the Company’s Risk Intelligence Capability

Integrated Enterprise Risk Management Capability

Stakeholder Value

Tribal & Heroic  Specialist Silos  Top Down  Systemic Risk Management  Risk Intelligent

Typical Implications for Internal Audit

**Tribal & Heroic**
- Risk identification and assessment typically initiated and led by IA
- Heavier involvement in risk analysis
- Heavier involvement in formulation of recommendation for risk mitigation and control

**Specialist Silos**
- Leveraged risk identification / assessment
- Better coordination with risk owners on risk mitigation efforts and controls

**Top Down**
- Linkage of IA Risk Based audit plan to ERM
- Risk Owners Formulate Mitigation
- Internal Audit evaluates and monitors

**Systemic Risk Mgmt.**
- Linkage of IA Risk Based audit plan to ERM
- Risk Owners Formulate Mitigation
- Internal Audit evaluates and monitors

**Risk Intelligent**
Introduction: Overview of the IT risk assessment methodology

- The Information Technology Internal Audit Risk Assessment Methodology adopts the broader concepts of Enterprise Risk Assessment with the overall objective of developing a risk-based internal audit plan.
- Likewise, the methodology creates a meaningful linkage to value-creation, achieving both assurance and consulting objectives of an Internal Audit activity.

Phases of the IT IA Risk Assessment Methodology:

1. Phase 1: Understand the Business and IT
2. Phase 2: Develop the IT Risk Model
3. Phase 3: Prioritize IT Risks
4. Phase 4: Develop Risk-Based IT Internal Audit Plan
5. Phase 5: Schedule the Audits & Plan resources
Phase One: Understand the Client’s Business

Key Activities

• Gather information:
  – Business and IT objectives and strategies
  – Organizational structure and changes
  – Key business processes and locations
  – Key information systems
  – Company’s disclosed risks (10-K)
  – Key industry risks and issues

• Organize information on the company’s structure (processes, locations, and systems)

Key Deliverables

• Client Profile
  – Business and IT Objectives/Strategies
  – Organizational structure
  – Business Process, Locations and systems

• Preliminary risk information
  – 10-K disclosed risks
  – Other company risk information
  – Key industry issues
Understand IT objectives, goals, strategy and processes

- IT & Business Strategic Plans
- Annual IT Plan & Budget
- Annual Business Plan
- Key IT Performance Metrics
  - E.g., projects, change requests, service requests, contracts, SLAs, etc.
- IT Project List
- IT Project Charters and Project Plans
- Entity Level Control Environment
- IT Policies & Procedures
- IT Risk and Control Matrices
- Attest Reports (IT)
- Management’s IT SOX Results
- Previous IT Internal Audit Reports

- IT organization chart; company org chart
- Business locations
- Data Center and other IT locations
- IT processes & process owners
- Inventory of systems and key interfaces
  - Applications
  - Databases
  - Operating systems
  - Tools
  - Hardware
- Network and other diagrams
Business Processes Linked to Information Systems and Locations

Illustrative

Corporate; Europe
A/P & Cash Disbursement
SAP

Asia
Inventory Management
RMS

Corporate; Europe
Fixed Assets
SAP
RMS

Asia
Wholesale Revenue, A/R
SAP
RMS

Asia
Retail Revenue, A/R
RMS

Corporate; Europe
Financial Reporting
SAP

Asia
Store Operations
POS

Oracle 11i

UNIX-Solaris 7
UNIX-Solaris 8
Windows 2003 sp2

Windows 2000 Network Management System: Cisco Equipment
Example - Key Processes, Systems, and Locations

**Key Locations**
- Corporate - Japan
- Service Centre - Atlanta
- USA
- Asia
- Europe

**Key Process/Divisions**
- Revenues (A)
- Corporate Legal & Compliance (B)
- Payroll & Personnel (C)
- Fixed Assets (D)
- Corporate Finance (E)
- Expenditures (F)

**Process Owners/Head**
- Corporate - Japan
- Service Centre - Atlanta
- USA
- Asia
- Europe

<table>
<thead>
<tr>
<th>Key Application Systems</th>
<th>Key Databases</th>
<th>Key Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Financials</td>
<td>Oracle Database</td>
<td>Unix</td>
</tr>
<tr>
<td>Siebel CRM</td>
<td>Oracle Database</td>
<td>Unix</td>
</tr>
<tr>
<td>Corp Legal &amp; Compliance Apps</td>
<td>Microsoft Access</td>
<td>Windows</td>
</tr>
<tr>
<td>PeopleSoft HR</td>
<td>Oracle Database</td>
<td>Unix</td>
</tr>
<tr>
<td>ADP Payroll</td>
<td>ADP (Outsourced Service Provider)</td>
<td>ADP (Outsourced Service Provider)</td>
</tr>
<tr>
<td>Hyperion</td>
<td>Oracle Database</td>
<td>Windows</td>
</tr>
</tbody>
</table>
# Example – Map of Business Processes to Systems

**Company Name:** ABC

<table>
<thead>
<tr>
<th>Key Applications / Module</th>
<th>Business Critical Process</th>
<th>Application vendor</th>
<th>Key Interfaces</th>
<th>Operating System</th>
<th>Database</th>
<th>Business</th>
<th>IT Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Oracle</td>
<td>Financial system</td>
<td>Oracle</td>
<td>Avantis, ADP, Toptech</td>
<td>IBM AIX</td>
<td>Oracle</td>
<td>Owner</td>
</tr>
<tr>
<td>B</td>
<td>Avantis</td>
<td>Project/ Maintenance Mgmt</td>
<td>Vendor - Ivensys</td>
<td>Excel</td>
<td>MS Win 2003</td>
<td>MS SQL</td>
<td>Owner</td>
</tr>
<tr>
<td>C</td>
<td>ADP</td>
<td>Payroll</td>
<td>Outsourced - ADP (SAS70)</td>
<td>N/A</td>
<td>N/A</td>
<td>Owner</td>
<td>App Mgr</td>
</tr>
<tr>
<td>D</td>
<td>Toptech</td>
<td>Marketing terminal, all daily liftings</td>
<td>Outsourced - Toptech</td>
<td>FAS</td>
<td>Proprietary QNX</td>
<td>Proprietary</td>
<td>Owner</td>
</tr>
<tr>
<td>E</td>
<td>FAS (Fixed Asset)</td>
<td>Fixed Assets</td>
<td>Sage Software (formerly Best Software)</td>
<td>Excel</td>
<td>MS Win 2000</td>
<td>Sybase</td>
<td>Owner</td>
</tr>
</tbody>
</table>
Phase Two: Develop Risk Model

Key Activities

- Develop the IT risk framework:
  - Risk categories framework
  - IT Risk listing with definitions
  - Risk rating criteria factors
    (Impact and Vulnerability)
- Validate the risk framework with key stakeholders

Key Deliverables

- Risk Categories Framework
  - Governance
  - Strategy
  - Operations
  - Infrastructure
  - External
- Business Risk Listing with risk definitions
- Risk rating criteria:
  - Impact
  - Vulnerability
Develop the IT risk model

Control Objectives for Information and related Technology (COBIT®)

• An IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.

• Provides good practices across a domain and process framework

Control Objectives for Information and related Technology (COBIT®)

### IT Governance
- Mission
- IT and Business Alignment
- Portfolio Management
- IT Risk Management
- Policy

### IT Strategy & Planning
- IT Planning
- Strategic Sourcing
- IT Organization
- Human Resources
- Asset Management
- Budgets, Metrics & Controls

---

#### IT Processes

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Project Management</th>
<th>Applications &amp; Databases</th>
<th>Operations</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Technology Planning</td>
<td>• Project Management Lifecycle (PMLC)</td>
<td>• Change Management (Applications, Databases &amp; Infrastructure)</td>
<td>• Data Processing</td>
<td>• Problem Management</td>
</tr>
<tr>
<td>• Emerging Technologies</td>
<td>• Initiating</td>
<td>• Change Prioritization</td>
<td>– Batch Scheduling</td>
<td>– Help Desk</td>
</tr>
<tr>
<td>• Standards</td>
<td>• Planning</td>
<td>• Documentation, Approval, and Tracking</td>
<td>– Online Processing</td>
<td>– Incident Response</td>
</tr>
<tr>
<td>• Architecture Design &amp; Management</td>
<td>• Executing</td>
<td>• Acquire / Build</td>
<td>• Application / Database Management</td>
<td>– Root Cause Analysis</td>
</tr>
<tr>
<td>– Software</td>
<td>• Controlling</td>
<td>• Test &amp; QA</td>
<td>– Capacity</td>
<td>• Service Level Management</td>
</tr>
<tr>
<td>– Infrastructure</td>
<td>• Closing</td>
<td>• User Acceptance</td>
<td>– Availability</td>
<td>• Vendor / Third-Party Management</td>
</tr>
<tr>
<td>– Security</td>
<td>• Systems Development (SDLC)</td>
<td>• Approval to Transfer to Production</td>
<td>– Performance</td>
<td>• End-User Computing</td>
</tr>
<tr>
<td>• Vendor / Product Selection</td>
<td>• Design</td>
<td>• Emergency Changes</td>
<td>• Facilities Management</td>
<td>• Software Licensing</td>
</tr>
<tr>
<td>• Integration &amp; Consolidation</td>
<td>• Acquire / Build</td>
<td>• Patch Management</td>
<td>• Data Retention / Backup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Test &amp; QA</td>
<td>• Configurable Controls</td>
<td>– Scheduling</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data Conversion</td>
<td>• Data Quality &amp; Integrity</td>
<td>– Processing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Implement / Deploy</td>
<td>• Interface Validation &amp; Integrity</td>
<td>• Offsite Storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Support / Maintain</td>
<td></td>
<td>• Retrieval &amp; Restoration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Project Risk (Pre-Imp) Review</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Post Implementation Review</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Enterprise Security
- • Threat & Vulnerability Management
- – Intrusion Detection / Response
- – Intrusion Prevention
- – Security Penetration & Vulnerability Testing
- – Virus Prevention / Detection

### Disaster Recovery
- • Business Impact Assessment
- • Disaster Recovery Planning
- • Communications / Crisis Management Plans
- • Disaster Recovery Testing
- • Ongoing Maintenance / Updates

### Infrastructure
- • Operating Systems
- • Database Structures
- • Networks (Internal & Perimeter)
- • Hardware
- • Locations
- • Tools (E-mail, EDI, Messaging, etc.)
Phase Three: Prioritize Risks

Key Activities

• Conduct interviews or workshops to gather risk ratings by designated key client participants:
  - C-Suite
  - Second tier management respondents (Vulnerability risk rating)
• Based on the executive risk assessment inputs, develop the Risk Heat Map

Key Deliverables

• Risk Heat Map
  - Risks prioritized based on Impact and Vulnerability risk ratings
  - A summary of risk assessment
  - Interview notes
Prioritize IT risks

• Define the risk factors to be used as a basis for risk ranking:
  – Impact
  – Vulnerability

• Impact and Vulnerability can be assessed in terms of High, Medium and Low or using numerical ratings (e.g., 1 to 5 or 1 to 100)

• Risk Factors are used to assess the relative risk of each identified IT risk
Prioritize IT risks

• Impact and Vulnerability criteria MUST be defined explicitly and agreed with the Risk Assessment sponsor in advance of the interviews, workshops, surveys and risk ranking. This will enable the following:
  – Standard criteria ensures consistency
  – Agreeing the criteria in advance helps build a foundation for consensus of risk assessment results
Impact

• Impact is an estimate of the severity of adverse effects, the magnitude of a loss, or the potential opportunity cost should a risk be realized.
  – Impact can be thought of as gross inherent risk.

• Example Impact Criteria:
  – Strategic
  – Financial
  – Reputation
  – Legal and Regulatory
  – Operational
  – Stakeholders
Vulnerability

• Vulnerability is the extent to which the functional area may be exposed or unprotected in relation to various risk factors after existing controls have been taken into account.
  – Vulnerability can be thought of as net residual risk.

  **NOTE:** Vulnerability differs from likelihood because likelihood only considers the probability of an event occurring, whereas vulnerability considers other aspects such as control effectiveness and preparedness.

• Example Vulnerability Criteria:
  – Complexity
  – Control Effectiveness
  – Prior Risk Experience
  – Rate of Change
Define Impact and Vulnerability Criteria

- Impact
  - Strategic
  - Financial
  - Reputation
  - Legal and Regulatory
  - Operational
  - Stakeholders
  - Competitor

- Vulnerability
  - Complexity
  - Control Effectiveness
  - Prior Risk Experience
  - Rate of Change
  - Preparedness

Define the Impact and Vulnerability criteria which will be applied to each identified IT risk to determine the relative risk rankings:
### Sample Impact Criteria

#### RISK ASSESSMENT - IMPACT CRITERIA

**NOTE:** The percentages and dollar values used in this example are subject to change upon the company’s actual materiality levels and risk factors, based on the judgment made together with management.

<table>
<thead>
<tr>
<th></th>
<th>Financial</th>
<th>Reputation</th>
<th>Legal/ Regulatory</th>
<th>Customer Satisfaction</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating Margin</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>$41-$80M</td>
<td>National and International coverage Wall Street Journal</td>
<td>Any Federal or State action</td>
<td>Significantly impact achievement of sales and service satisfaction goals/metrics</td>
</tr>
<tr>
<td>Medium</td>
<td>$26-$40M</td>
<td>Escalating community activism, Regional Press Coverage</td>
<td>Any Federal or State scrutiny or Local action</td>
<td>Moderately impact achievement of sales and service satisfaction goals/metrics</td>
</tr>
<tr>
<td>Low</td>
<td>$0-25M</td>
<td>Local Press Coverage</td>
<td>Any Local scrutiny</td>
<td>Very low to No impact on the achievement of sales and service satisfaction goals/metrics</td>
</tr>
</tbody>
</table>

**NOTE:** When evaluating the potential impact of a risk, select the highest (worst case) impact threshold exceeded and assign the corresponding impact level. (example: if a risk has a MEDIUM potential financial impact but has a HIGH reputation or regulatory
## Sample Vulnerability Criteria

### RISK ASSESSMENT - VULNERABILITY CRITERIA

<table>
<thead>
<tr>
<th>Control effectiveness &amp; efficiency</th>
<th>Previous risk experience</th>
<th>Complexity</th>
<th>Capability</th>
<th>Rate of change</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criteria</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>High</strong></td>
<td>Controls are not working or do not exist</td>
<td>History of risk happening or knowledge of occurrence (through IA opinion, external auditor comments, legal cases, etc)</td>
<td>People</td>
<td>Process</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td>Controls are detective but not preventative and there may or may not be effective reporting</td>
<td>MEDIUM recent previous adverse experience</td>
<td>Risk affects a MEDIUM # of transactions OR a MEDIUM # of processes and/or systems</td>
<td>A limited # of staff or staff has moderate competency</td>
</tr>
<tr>
<td><strong>Low</strong></td>
<td>Controls are appropriately preventive and detective and there is effective reporting</td>
<td>LOW recent previous adverse experience</td>
<td>Risk affects a LOW # of transactions OR a LOW # of processes and/or systems</td>
<td>Most staff has high competency</td>
</tr>
</tbody>
</table>
Prioritize IT risks

Define the IT Risk Assessment Participation Approach

• One-on-one interviews
  – Determine if a top-down or bottom-up approach is preferred
    • Tier 1 = Executive Management
    • Tier 2 = Senior Management
    • Tier 3 = Line Management

• Surveys
  – An effective way to expand the level of participation beyond interviews
  – Can be used to solicit anonymous input

• Facilitated Workshops
  – May facilitate management buy-in to the risk assessment process
  – Cross-functional workshops may enhance risk assessment comprehensiveness and quality
  – Can be used to expand the level of participation beyond interviews
## Illustrative IT Risk Assessment Summary

<table>
<thead>
<tr>
<th>IT RISK</th>
<th>Risk Definition</th>
<th>Impact (I)</th>
<th>Overall Impact Commentary</th>
<th>Vulnerability (V)</th>
<th>Overall Vulnerability Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Management and Governance</td>
<td>Ensure transparency and understanding of costs, benefits, strategy, policies and service levels. Ensure proper use, controls, and performance of the applications and technology solutions. Ensure IT compliance with laws and regulations.</td>
<td>75</td>
<td>IT Control Environment considerations; high IT spend</td>
<td>50</td>
<td>Management focus on improving capability and maturity</td>
</tr>
<tr>
<td>Information Security / Asset Protection</td>
<td>Ensure critical and confidential information is withheld from those who should not have access to it. Ensure automated business transactions and information exchanges can be trusted. Maintain the integrity of information and processing infrastructure. Account for and protect all IT assets. Ensure IT services can properly resist and recovery from failures due to error, deliberate attack or disaster.</td>
<td>90</td>
<td>Data protection and data confidentiality are fundamental to business model and organizational success</td>
<td>75</td>
<td>Prior risk experience indicates a relatively high level of vulnerability</td>
</tr>
<tr>
<td>System Development</td>
<td>Define how business functional and control requirements are translated into effective and efficient automated solutions. Acquire and/or develop integrated and standardized application systems.</td>
<td>20</td>
<td>Minimal systems development activities performed</td>
<td>20</td>
<td>Proven track record of success</td>
</tr>
<tr>
<td>Change / Problem Management</td>
<td>Maintain integrated and standardized application systems. Ensure minimal impact to business operations.</td>
<td>40</td>
<td>Change control activities affect multiple processes and systems</td>
<td>20</td>
<td>Proven track record of success</td>
</tr>
<tr>
<td>Relationships with outsourced vendors</td>
<td>Ensure mutual satisfaction of 3rd party relationships. Ensure satisfaction of end-users with service offerings and service levels.</td>
<td>30</td>
<td>Limited to non-core functions</td>
<td>20</td>
<td>Positive control structure</td>
</tr>
</tbody>
</table>

### Impact Levels
- **Low (10)**
- **Medium (50)**
- **High (100)**
Based on management’s assessment of the key IT risks, the Company’s IT risk profile was developed as follows:

Note: The IT Risk Heat Map is a point-in-time depiction of management’s assessment of the Company's key IT risks and should be periodically updated.
Phase Four: Develop the Risk-Based Internal Audit Plan

Key Activities

- Validate risk assessment results with management
- Map the key risks to business processes and locations (Phase 1)
- Identify risks for Internal Audit focus (to be included in the IA Plan)
- Determine the high level audit approach for risks in the IA Plan

Key Deliverables

- Risks mapped to business processes, locations and key systems
- Risks for Internal Audit focus and IA Plan development
- Risk-based Internal Audit Plan
Develop risk-based IT internal audit plan

- Identify IT risks for internal audit focus
- Map the key risks to IT processes (IT audit universe)
- Map IT processes to locations and systems to be audited
- Determine the audit approach
- Develop the risk based audit plan

IT risks that do not get selected for IT IA focus and will not be part of the IT IA plan should be addressed by management through a variety of other control activities
## Key IT Risks Mapped to the IT Processes

### Sample

<table>
<thead>
<tr>
<th>Client IT Processes</th>
<th>Primary Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT Governance</strong></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>X X</td>
</tr>
<tr>
<td>Strategy and Planning</td>
<td>X X X X X</td>
</tr>
<tr>
<td>IT Processes</td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td>X X X X X</td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
</tr>
<tr>
<td>– Project Management Lifecycle</td>
<td>X X</td>
</tr>
<tr>
<td>– Project Risk (Pre and Post Imp Review)</td>
<td>X</td>
</tr>
<tr>
<td>Applications and Databases</td>
<td>X X X X X X X X</td>
</tr>
<tr>
<td>– Change Management</td>
<td>X X X X X X X</td>
</tr>
<tr>
<td>– Patch and Configuration Management</td>
<td>X X X X X X X</td>
</tr>
<tr>
<td>– Data Quality and Interfaces</td>
<td>X</td>
</tr>
<tr>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>– Data Processing</td>
<td>X X</td>
</tr>
<tr>
<td>– Application Management</td>
<td>X X</td>
</tr>
<tr>
<td>– Database Management</td>
<td>X X X</td>
</tr>
<tr>
<td>– Storage Management</td>
<td>X X X X X</td>
</tr>
<tr>
<td>– Facilities Management</td>
<td>X X X X X X X</td>
</tr>
</tbody>
</table>
## Example #1 – Risks for IT internal audit focus

<table>
<thead>
<tr>
<th>Risks for IT IA Focus</th>
<th>IT Process(es)</th>
<th>Risk Ranking</th>
<th>General Audit Approach</th>
<th>Corporate Illinois</th>
<th>Texas</th>
<th>Canada</th>
<th>Mexico</th>
<th>Ireland</th>
<th>European Shared Service Center</th>
<th>Italy</th>
<th>France</th>
<th>China</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Strategy &amp; IT Compliance</td>
<td>Enterprise Security</td>
<td>H</td>
<td>Risk Mitigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy and Data Protection</td>
<td>Enterprise Security</td>
<td>H</td>
<td>Risk Mitigation</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Infrastructure Security &amp; Support</td>
<td>Enterprise Security Support</td>
<td>H</td>
<td>Risk Mitigation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Change Mgmt</td>
<td>Apps &amp; Databases</td>
<td>H</td>
<td>Risk Mitigation</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Retention Backup</td>
<td>Operations</td>
<td>M</td>
<td>Assurance</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>BCP/Disaster Recovery</td>
<td>Disaster Recovery</td>
<td>M</td>
<td>Assurance</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Regulatory Compliance &amp; SOX Support</td>
<td>IT Governance</td>
<td>M</td>
<td>Assurance</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Project Mgmt</td>
<td>Project Mgmt</td>
<td>M</td>
<td>Assurance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Sys Dev Lifecycle</td>
<td>Project Mgmt</td>
<td>L</td>
<td>Assurance</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Enterprise Security</td>
<td>L</td>
<td>Assurance</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
## Example #2 IT – Risks for IT internal audit focus

<table>
<thead>
<tr>
<th>IT Risk Universe Area</th>
<th>Impact</th>
<th>Vulnerability</th>
<th>Risk Category</th>
<th>Rotation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Governance</td>
<td>H</td>
<td>H</td>
<td>Mitigate</td>
<td>Consult</td>
</tr>
<tr>
<td>Regulatory Compliance &amp; Sarbanes-Oxley Support</td>
<td>H</td>
<td>M</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>IT Strategy &amp; Planning</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Strategy &amp; Planning</td>
<td>M</td>
<td>M</td>
<td>Assurance</td>
<td>Every Two Years</td>
</tr>
<tr>
<td>Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture Design and Management</td>
<td>L</td>
<td>H</td>
<td>Cumulative Impact</td>
<td>Annual</td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Mgmt (PMLC)</td>
<td>H</td>
<td>M</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>Systems Development Lifecycle (SDLC)</td>
<td>H</td>
<td>M</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>Data Management &amp; Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data/Job Processing</td>
<td>H</td>
<td>L</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>App/DB Storage &amp; Availability Management</td>
<td>H</td>
<td>L</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>Facilities/Data Center Management</td>
<td>M</td>
<td>L</td>
<td>Review Resources</td>
<td>As Needed</td>
</tr>
<tr>
<td>Data Retention / Backup</td>
<td>L</td>
<td>M</td>
<td>Review Resources</td>
<td>As Needed</td>
</tr>
<tr>
<td>Applications &amp; Databases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change Management</td>
<td>H</td>
<td>H</td>
<td>Mitigate</td>
<td>Consult</td>
</tr>
<tr>
<td>Data Quality &amp; Integrity</td>
<td>M</td>
<td>H</td>
<td>Mitigate</td>
<td>Consult</td>
</tr>
<tr>
<td>Infrastructure Patch Management</td>
<td>M</td>
<td>H</td>
<td>Mitigate</td>
<td>Consult</td>
</tr>
<tr>
<td>Interface Validation &amp; Integrity</td>
<td>M</td>
<td>H</td>
<td>Mitigate</td>
<td>Consult</td>
</tr>
<tr>
<td>Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Management</td>
<td>H</td>
<td>L</td>
<td>Assurance</td>
<td>Annual</td>
</tr>
<tr>
<td>Service Level Management</td>
<td>L</td>
<td>M</td>
<td>Cumulative Impact</td>
<td>Every Two Years</td>
</tr>
</tbody>
</table>

Leading Practice IT Risk Assessment

Copyright © 2008 Deloitte Development LLC. All rights reserved.
Phase Five: Schedule the Audits and Plan Resources

Key Activities

• Work with the client (CAE) to determine the resource needs (skill sets, tools, competencies) given the risk information for the planned audits
• Allocate resources and schedule the audits

Key Deliverables

• Detailed risk-based internal audit plan showing:
  – linkage of IA projects to the risk assessment process and risk information
  – alignment of resource competencies to
  – risk focus of the project
  – audit timeline
Develop the risk response

• Internal audit can respond risks
  – Incorporate areas of risk into the risk-based internal audit plan and performing internal audits to provide assurance to management and the board on the design and operation of controls
    • Validate that reliance on existing controls is warranted
    • Recommend control improvements
  – For areas with higher vulnerability, internal audit can act in a consultative role
    • Advise management on control design
    • Monitor and report on management remediation activities

• Management has the primary responsibility for risk management
  – Perform risk assessment to identify areas of greatest risk
  – Identify and / or develop risk responses – investments, initiatives, strategy, etc.
  – Besides risk response (reactive), management should also define the overall risk management approach (proactive risk identification, classification and risk management)
Common and Emerging IT Risks

“Top 10” IT Risks

• Segregation of Duties
• Project Risk
• Application Configurable Controls
• Administrative Access
• Privacy
• Interfaces and Middleware
• High Availability
• Data Management
• User Provisioning
• Wireless

Source: Top IT Audit Issues, Deloitte presentation for The Institute of Internal Auditors, October 24, 2006.
Review of today’s discussion

• **Overview:** Leading Practice IT Risk Assessment

• **Performing Risk Assessments for IT**
  – Identifying and Evaluating IT Risks
  – Using IT Risk Frameworks including CobiT
  – Linking IT Risks to Organizational Objective

• **Creating a Risk Response**

• **Common and Emerging IT Risks**
Contact information

Melissa Bishop  
Enterprise Risk Services  
San Francisco, CA  
Tel: +1 415 783 6380  
Mobile: + 1 415 407 5818  
msbishop@deloitte.com  
www.deloitte.com

Carey Carpenter  
Enterprise Risk Services  
Honolulu, HI  
Tel: +1 808 543 0776  
Mobile: + 1 415 602 7605  
ccarpenter@deloitte.com  
www.deloitte.com