Audit Risk Assessment
Art or Science?

Sanjay Singh
VP, Audit Services
Evolution of Audit Planning

Changing Characteristics of Audit Planning

Alignment with Enterprise Risk Exposure

Strategy
- Cyclical audits with a fixed refresh
- Risk-driven cycles ordered by materiality
- Risk-driven plan with a business unit/functionally defined audit universe
- Risk-driven plan with a geographically defined audit universe
- Risk-driven plan with an audit universe defined by process
- Risk-driven plan based on a risk universe
- Risk-driven plan based on risk universe and risk assessment activities

Operational

Financial

Attributes

Risk-based Audit Planning
- Set number and type of audits performed each year
- No risk assessment performed
- Cyclical plan with a fixed refresh process

Defining Characteristics
- Does not recognize change in the organization
- Fails to provide reasonable evaluation and risk coverage

Phase II
- Audit universe defined by geography, function, or process
- Internal Audit-owned risk assessment incorporating qualitative and quantitative data from multiple sources
- Annual audit plan focusing on highest risk areas

Phase II
- Audit universe equals the risk universe
- Heavy reliance on risk information from management and risk management groups/activities
- Quarterly rolling audit plan focusing on highest risk areas

Phase II
- Relies on Internal Audit’s judgement to assess the level of risk in each entity
- Does not evaluate the overall risk profile of the company

Phase II
- Relies on management’s understanding of the risks the organization faces
- Enables Internal Audit to maximize risk coverage in the audit plan

Source: Corporate Executive Board
Top Down or Bottom-up Risk Assessment?

- Key risks or risk universe?
- Objective/numerical or subjective?
- How much of risk bureaucracy do you need/can afford?
- Do you consider inherent risk, control environment and residual risk?

See page 4

See page 5

Risk-based projects

PwC, ADR, & 10-K Risks

Audit Risk Assessment (Emerging Risks)

SOX 404 Key Controls – Risk Ranked Based on Materiality

Coverage by Business, Function, Process, Geography, or Cyclical

Management and ACC Request

Quarterly Close / DC / Monthly Close Meetings; Internal Communications

ERM

Corruption / Fraud Risks

Compliance Risk

IT Risk

International Risk
## Risk Assessment for Emerging Risks

Defining risk in simple terms

### What are your business objectives? What are the biggest constraints to those objectives? What keeps you up at night?

<table>
<thead>
<tr>
<th>What is New?</th>
<th>What is Large?</th>
<th>Not a Core Competency</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g., On-demand, maintenance, disruptive business models/technologies</td>
<td>e.g., Revenue</td>
<td>e.g., New product development, disruptive business models/technologies, change management</td>
</tr>
</tbody>
</table>

### Changes

- Responsibilities
- Organizational Structure
- Systems/Technology
- Processes/Controls
- Accounting

### Strategic Expansions

- Acquisitions
- New Products
- New Businesses
- New Geographies
- New Brands
- New Channels

### Unfamiliar Landscape
- Management Bandwidth
- Non-core Capabilities
Assessing Technology Risks

Internal Risk Inputs

• Management Discussions & Feedback
• Ryder IT Project Listing
• Ryder ERM Program
• Strategic Initiatives/Projects

External Risk Inputs

• AICPA - Top Technology Initiatives
• Audit Leadership Council
• Protiviti Top Risks Survey
• ISACA IT Audit Benchmarking Survey
• Big 4 Risk guidance/publications

Internal Audit Plan
Assessing System Development Risks

A. System Implementation - Control Self Assessment

To provide guidance on key governance deliverables that may be reviewed by external or internal Audit for significant system implementations, especially those with financial statement impact. This list may be scaled back, depending on the size and complexity of the project (i.e., a larger type implementation will have each element but for a smaller implementation, some of these items may not be applicable).

<table>
<thead>
<tr>
<th>Description</th>
<th>Key Financial System</th>
<th>Priority</th>
<th>Timing</th>
<th>Responsible Party</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Authorization</td>
<td>H</td>
<td></td>
<td></td>
<td>PMO</td>
<td>Planned and Approved</td>
</tr>
<tr>
<td>Business Requirements</td>
<td>M</td>
<td></td>
<td></td>
<td>IT</td>
<td>Reviewed and Approved</td>
</tr>
<tr>
<td>Technical Requirements</td>
<td>M</td>
<td></td>
<td></td>
<td>BUS</td>
<td>Communicate to appropriate stakeholders</td>
</tr>
<tr>
<td>Architecture/Design Documentation</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>Kept up to date</td>
</tr>
<tr>
<td>Interface Design (Including Subsystems)</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>Filed and Archived</td>
</tr>
<tr>
<td>Information Design/Requirements</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>Subsystem included</td>
</tr>
<tr>
<td>System and Data Security</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>Privacy considered</td>
</tr>
<tr>
<td>Segregation of Duties Considerations</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>Subsystem included</td>
</tr>
<tr>
<td>System Access</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>Subsystem included</td>
</tr>
<tr>
<td>Change Management Process (Business Requirements)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>Business provided key reports</td>
</tr>
<tr>
<td>Change Management Process (Key Financial Report Generation)</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>All stakeholders considered</td>
</tr>
<tr>
<td>Quality Assurance Protocols</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>Issues linked to requirements</td>
</tr>
<tr>
<td>Issue and Risk Management (During System Implementation)</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>Issues linked to requirements</td>
</tr>
<tr>
<td>Communication Strategy</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>refreshed</td>
</tr>
<tr>
<td>Business Processes Narratives</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>refreshed</td>
</tr>
<tr>
<td>General Application Controls Mapping (As Is vs. To Be)</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>refreshed</td>
</tr>
<tr>
<td>Financial Reporting Controls Mapping (As Is vs. To Be)</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>refreshed</td>
</tr>
<tr>
<td>Change Management for Chart of Account</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Data Conversion Process</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Roll Forward Process and Opening Balances Confirmation</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Sign Off on Chart of Account (Include Hierarchies, Consolidations, Entity Roll Ups)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Application Configuration Clean Up</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Testing Tie Out to Requirements</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Technical Requirements Testing (ie. Unit Testing)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Parallel Testing (If Applicable)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>User Acceptance Testing</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Testing for Key Financial Statement Report Generation</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Cut Over Plan/Strategy</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Dress Rehearsal</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Go/No Go Decision Process</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Post Go-Live Support</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Knowledge Transfer from Contingent Workers to Partners</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Training Plan (End Users, Super Users, Other Markets)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Revoke Super User/Administrator Access Post Implementation</td>
<td>H</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>New and Changed Controls Operate Effectively</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Monitor System Speed (In conjunction with Expanded Hierarchies)</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Patch Support</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
<tr>
<td>Data Backup</td>
<td>M</td>
<td></td>
<td></td>
<td></td>
<td>conforme</td>
</tr>
</tbody>
</table>

Notes:
- Pink bold means formal approval is expected.

1. Do these elements exist on the plan?
2. Does a timeline exist?
3. Are timelines reasonable?
4. How is progress against timelines?
Identifying Auditable Risks

1. Strategic Management (e.g., Competitive Threats)
2. Emerging Priorities/Risks (e.g., Channel Development and Emerging Brands)
3. External Factors (Ignore) (e.g., Economic Conditions)
4. Corporate Governance & Hygiene (e.g., SOX)

<table>
<thead>
<tr>
<th>Need for Structural/Strategic Response</th>
<th>Need for Process Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
</tbody>
</table>

Focus in strategically dynamic environments
Focus in strategically stable environments
Considering Strategic Risks?

Consider what not to audit

- Auditing risk vs. uncertainty?
- Auditing creative processes?
- Question of credibility – Is Audit a subject matter expert in strategy?
- Is Audit viewed as a process, risk and control resource?
- Auditing model assumptions?
- Auditing whether process is documented and auditable?
- Post audits on strategic projects?
- Auditing strategy navigation vs. formulation?
- Second guessing strategy?
(305) 500-3258
Sanjay_Singh@ryder.com