Get More Out of Your Risk Assessment

Austin Chapter of the IIA
Speakers

Alyssa G. Martin, CPA
Dallas Executive Partner, Advisory Services

25 years of public accounting experience, with a practice emphasis in risk management, internal audit, and business process improvement

Daniel Graves, CPA
Senior Manager Advisory Services

9 years of public accounting experience, with a practice emphasis risk assessment, internal audit, and business process improvement
Agenda

• Moving to a New Approach for Internal Audit Planning
• The Partnership
• ERM Basics
• Risk Response Plan and Internal Audit
A NEW APPROACH

Transitioning Internal Audit Planning from the “Old Way” to the “New Way”
Traditional Audit Plan

Traditional audits were planned based on:

- Process-level risk-rated universe
- Typical financial and operational risk considerations
- Processes significant for financial reporting, compliance and regulatory risks
- Limited operational or strategic consideration
- Idea of “time to audit” the process again
Proportional internal audit plans are typically focused on activities identified as “high risk” by internal audit and compliance procedures.

60% • List of processes based on internal audit’s risk rating & the last date audited

40% • Compliance obligations (SOX, FDICIA, PCI, HIPAA, etc.)
  • New areas or changes that need to be audited
How many of you audit a process area because you have not audited it in 2, 3, 4 years?
Enterprise risk focused internal audit plan that is based on:

• Critical risks that impact the achievement of organizational strategic objectives
• Operational risks based on business unit feedback
• Key Performance and Risk Indicators (KPIs and KRIIs) that validate business unit performance and risk management
• Supporting assurance, compliance, and fraud prevention requirements
Mapping Critical Enterprise-wide Risks

Identify organization’s strategic objectives and major initiatives

- Determine critical success factors for each objective
- Understand which KPIs managers are monitoring to meet business results and strategic objectives
- Perform root analysis to identify risk influencers (KRI s) that affect KPIs
Many organizations currently monitor Key Performance Indicators (KPIs) in order to stay up-to-date on potential events. According to COSO, KPIs may not provide enough advance notice. Often, KPIs alert management to risk events that have already impacted the organization.

Key Risk Indicators (KRI) are metrics developed by management to identify potential future shifts in risk conditions. Using KRI allows for more timely, strategic, and proactive development of risk mitigation approaches.
Profile: A company derives most of its earnings from manufacturing outdoor recreational products for younger adults.

**Enterprise Risk Area:**
- Demographic Risk

**Enterprise Risk Event:**
- Significant change in the target demographic

**Significant Processes:**
- Marketing
- Customer Awareness
- Research and Development

**Key Risk Indicator:**
- Increase in the age of the target demographic
Profile: A company derives most of its earnings from manufacturing outdoor recreational products for younger adults.

Market Data:
- Census data indicates a average age
- Trend analysis indicates a steady historical increase.

Analysis:
- Market for existing product line is shrinking
- Likelihood of impact to company is high
- Effects may not be immediately felt

Response:
- Company launches R&D initiative for new products
- Internal audit would consider auditing R&D based on:
  - Significance of risk factor
  - Impact on the company’s objectives
Risk Realignment

How do you effectively realign risk?

• Determine which risks are most consequential to objectives and initiatives.
• Identify how key risks influence processes in ordinary course of business.
• Establish Internal Audit Plan based on criticality of risk.
• Prioritize resources based on most relevant activities.
Risk Realignment

Determine consequential risks

- Determine which risks directly impact the organization’s objectives and initiatives

Identify how risks influence financial/operational processes

- Determine whether risks affect auditable functions
- Audit risk management through significant activities of the organization

Establish the Internal Audit Plan based on criticality of risks

- Prioritize IA efforts based on risk while maintaining required financial and compliance coverage
- Using the Risk Response Plan, the Internal Audit Plan should address:
  - Risks critical to meeting strategic initiatives
  - Risks that directly impact critical success factors and KPIs
  - Support for assurance, compliance, fraud, financial and operational risks
- Prioritize resources
  - Identify audit methods to gain greatest coverage of financial, compliance requirements
  - Identify skills, expertise needed to augment the existing team
THE PARTNERSHIP

Internal Audit and Risk Management Function
Establish and operate the enterprise risk management framework on behalf of the board.

Incorporate the Internal Audit function and their monitoring activities into the risk management effort.

Include Internal Audit’s input of the effectiveness of internal controls to evaluate residual risk.
Internal Audit’s Role

Create tools and techniques used by internal audit to analyze risks and controls available to the RM function.

Share knowledge, expertise, and methods for analyzing risks and controls with the RM function.

Act as the central point for coordinating, monitoring and reporting on effectiveness of internal controls. IA should participate in identifying and evaluating risk but not own the risk management responsibility.

Support managers as they work to identify the best way to mitigate a risk. Provide consultation services that helps management develop the controls to mitigate risk.
Internal Audit’s core role with regard to ERM is to provide objective assurance to the board on the effectiveness of risk management.

• Does your organization have risk management function, separate and apart from Internal Audit?
• How well do the Internal Audit and Risk Management functions coordinate?
ERM BASICS

Defining ERM and Evaluating the ERM Function
Defining ERM

Enterprise Risk Management (ERM) is a process:

• Effected by people
• Applied in strategy setting
• Applied across the enterprise
• Designed to identify potential events (both positive and negative)
• Designed to manage risk within risk appetite
• Designed to provides “reasonable assurance”
• Designed to support the achievement of key objectives
Enterprise Risk Management incorporates a broad spectrum of considerations:

- Financial and nonfinancial indicators
- Intangible assets, like your “brand”
- Enhancing business strategy
- External influences
- Operational management
- Opportunities in addition to risks
Establish objectives for the ERM function that link people, process, capital, and risk appetite.

**Risk Appetite**: Level of risk the organization is willing to accept in pursuit of value creation

- Reflects risk management philosophy
- Influences risk culture
- A guidepost in strategy-setting
- Related to business model

**Risk Tolerance**: The acceptable level of variation in achievement of objectives, typically measured in same units as related objectives; how much exposure to accept success or failure

- Can be measured as key risk and performance indicators
The ERM approach begins with risk identification and assessment, then incorporates risk mitigation and monitoring activities.

**Risk Identification**
- Identification of relevant risk factors

**Risk Assessment**
- Entity level risk assessment.
- Process level risk assessment.

**Risk Response and Mitigation**
- Development and confirmation of control activities
- Control rationalization and process documentation
- Imbedding risk and control consciousness throughout the organization
- Internal audit over high risk operational, financial, and regulatory activities

**Monitoring**
- Periodic re-evaluation of risk factors and risk assessment
- Risk and control registers
- Continuous monitoring of critical risks and controls
Three Phases of ERM

- Conduct enterprise-wide risk assessments
- Involve all departments in the assessment to foster ownership in the process and increase risk awareness
- Use knowledge gained about significant organizational risks to develop a response plan that focuses on most critical risks
Build an interdisciplinary committee to brainstorm and discuss the relevant risk events that may influence activities, processes, and the achievement of strategic goals.
Types of Risk

Typical categories of risks often considered in creating a risk universe:

- **Inherent Risk**: The natural risk within a specific area of process, and the tendency for occurrence, when internal controls are weak or altogether absent.
- **Financial Reporting Risk**: The risk arising from errors in the financial reporting process, such as specific errors in reporting financial results.
- **Fraud Risk**: The risk resulting from any illegal acts characterized by deceit, concealment or violation of trust.
- **Information Technology Risk**: The risk that information systems will fail to ensure confidentiality, integrity, and availability of the storage and processing of the organization’s data.
- **Governance Risk**: The risk that governance processes will fail to provide adequate oversight.
- **Reputational Risk**: The risk that the organizational will suffer damage to its reputation if negative media attention occurs due to failure to prevent or detect misconduct within the organization.
- **Environmental Risk**: The risk that environmental catastrophes could interrupt normal business operations.
- **Strategic Risk**: The risk associated with an organization’s chosen business strategy, which includes entering new markets, developing new products, and expanding through mergers and acquisitions.

*This is where we want to move the focus.*
# Executive Perspectives: Top Risks for 2014

<table>
<thead>
<tr>
<th>Rank</th>
<th>Risk Issue</th>
<th>Risk Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Regulatory changes</strong> and heightened <strong>regulatory scrutiny</strong> may affect the manner in which our products or services will be produced or delivered.</td>
<td>Strategic Risk</td>
</tr>
<tr>
<td>2</td>
<td><strong>Economic conditions</strong> in markets we currently serve will significantly restrict <strong>growth opportunities</strong> for our organization.</td>
<td>Economic Risk</td>
</tr>
<tr>
<td>3</td>
<td>Uncertainty surrounding <strong>political leadership</strong> in national and international markets will limit growth opportunities.</td>
<td>Economic Risk</td>
</tr>
<tr>
<td>4</td>
<td><strong>Succession challenges</strong> and the ability to <strong>attract and retain top talent</strong> may limit our ability to achieve operational targets.</td>
<td>Operational Risk</td>
</tr>
<tr>
<td>5</td>
<td><strong>Organic growth</strong> through customer acquisition and/or enhancement presents a significant challenge.</td>
<td>Strategic Risk</td>
</tr>
<tr>
<td>6</td>
<td><strong>Cyber threats</strong> have the potential to significantly <strong>disrupt core operations</strong> for our organization.</td>
<td>Economic Risk</td>
</tr>
<tr>
<td>7</td>
<td><strong>Resistance to change</strong> will restrict our organization from making necessary <strong>adjustments to the business model</strong> and core operations.</td>
<td>Operational Risk</td>
</tr>
<tr>
<td>8</td>
<td>Ensuring <strong>privacy/identity management</strong> and <strong>information security/system protection</strong> will <strong>require significant resources</strong> for us.</td>
<td>Operational Risk</td>
</tr>
<tr>
<td>9</td>
<td>Anticipated <strong>volatility in global financial markets</strong> and currencies will create challenging issues for our organization to address.</td>
<td>Economic Risk</td>
</tr>
<tr>
<td>10</td>
<td>Uncertainty surrounding <strong>costs of complying with health care reform legislation</strong> will limit growth opportunities for our organization.</td>
<td>Economic Risk</td>
</tr>
</tbody>
</table>
## Risk Identification

### Brainstorming

<table>
<thead>
<tr>
<th>Risk Event</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>External Risks</strong> - Risks that are outside the control of the Entity, yet if not managed may inhibit or prevent the achievement of strategic objectives. Considers the cultural, social, political, legal, economic, and competitive environment of providing goods and services.</td>
<td></td>
</tr>
<tr>
<td>Demographic - The risk of socio-economic, cultural, and population changes in the organization's business environment, including the stratification of member needs and relevance to all member classes and generations. Consider population projections and changes, cultural and generational differences, etc.</td>
<td></td>
</tr>
<tr>
<td>aging workforce</td>
<td>retiree volume increase vs. workforce size</td>
</tr>
<tr>
<td>smaller government</td>
<td>fewer members, fewer active employees</td>
</tr>
<tr>
<td>generational differences</td>
<td>communication requirements, priorities, loyalty</td>
</tr>
<tr>
<td>workforce mobility</td>
<td>Long term organizational loyalty</td>
</tr>
<tr>
<td>multi-cultural employee base</td>
<td>shifting / increasing, expectations</td>
</tr>
<tr>
<td>healthcare cost based on location</td>
<td>population increases and changes, lifestyle</td>
</tr>
</tbody>
</table>
Determine the significance of identified risk categories and events to the achievement of the entity’s strategic goals.

- Consider both external and internal risk events
- Consider the concept of velocity. Is the event something that is currently impacting the entity, or is the event more forward-looking? How quickly could the risk become significant?
Use surveys, interviews, and forum meetings to develop an assessment of risk significance for each risk category and event.

The resulting risk profile provides insight for risk managers and internal audit professionals regarding the nature and extent of specific risk categories to the entity.

### Resulting Risk Profile

<table>
<thead>
<tr>
<th>RISK CATEGORIES AND EVENTS</th>
<th>ASSESSED RISK SIGNIFICANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HUMAN CAPITAL RISK</strong></td>
<td></td>
</tr>
<tr>
<td>Inadequate employee recruiting and retention</td>
<td>2.55</td>
</tr>
<tr>
<td>Poor team cohesion and interdepartmental relations create a lack of supportive culture.</td>
<td>2.84</td>
</tr>
<tr>
<td>Low employee morale</td>
<td>2.83</td>
</tr>
<tr>
<td>Inadequate management leadership, skills, and competence</td>
<td>2.63</td>
</tr>
<tr>
<td>Inadequate employee skills and competence</td>
<td>2.41</td>
</tr>
<tr>
<td>Inadequate measurement of employee performance</td>
<td>2.35</td>
</tr>
<tr>
<td>Inadequate investment in human capital</td>
<td>2.24</td>
</tr>
</tbody>
</table>

**Example**
Determine the significance of high risk categories and events on individual processes and activities.

- Include the major processes and activities from all divisions and functions of the organization.
- Focus on inherent risk for the initial assessment.
## Process-level Risk Assessment

**Entity Level Risks to be assessed for each process**

### Significant Processes and Activities

<table>
<thead>
<tr>
<th>Process Level Risk Assessment</th>
<th>Sub-Process Considerations</th>
<th>Economic</th>
<th>Political</th>
<th>Financial Stability</th>
<th>Human Capital</th>
<th>Regulatory</th>
<th>Information Technology</th>
<th>Investment</th>
</tr>
</thead>
</table>

**Human Resources**

- Hiring and Retention
  - Hiring, Retention, and Termination Policies
  - Employee Compensation and Benefits Administration
  - Employee Performance Management & Disciplinary Practices
  - ERS Employee Relations
  - Succession Planning

**Information Technology**

- Information Security
  - Logical Security
  - Data Security
  - Physical Security
  - Penetration Testing

- Database Administration

- ERP Systems
  - Application Development
  - Application Implementation
  - Enterprise Systems

**Probability and impact to be completed by risk assessment forum team(s)**

- Significant processes and activities to be risk rated.
Process-level Risk Assessment

Legend: Points with Multiple References:
(A) 14, 15; (B) 18, 20; (C) 17, 21.
Refocusing on the “Right Risks”

ERM aids the organization in:

• Identifying and assessing the criticality of risk events facing the entity
• Enhances risk awareness and ownership across the entity
• Refocusing the internal audit plan and scoping procedures on the “right risks”
• What are the “right risks”?
• How do you focus an Internal Audit Plan on the “right risks”?
RISK RESPONSE PLAN AND INTERNAL AUDIT

Developing an Internal Audit Plan with Strategic Focus
Q: How does internal audit use the enterprise risk assessment? What is the next step?

A: Use the Risk Response Plan. But... what does that look like?

<table>
<thead>
<tr>
<th>Traditional Risk Response Plan</th>
<th>ERM Risk Response Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Based on the overall risk rating each activity received at the process level</td>
<td>• Based on the results of entity and process specific risk assessments</td>
</tr>
<tr>
<td>• Considers prior audit history and results</td>
<td>• Considers the related risk events</td>
</tr>
<tr>
<td>• Audit decision</td>
<td>• Identifies KPI’s and KRI’s</td>
</tr>
<tr>
<td></td>
<td>• Identifies recent operational changes in the process</td>
</tr>
<tr>
<td></td>
<td>• Considers prior audit results and other existing monitoring activities</td>
</tr>
<tr>
<td></td>
<td>• Determination of residual risk</td>
</tr>
<tr>
<td></td>
<td>• Audit decision</td>
</tr>
</tbody>
</table>
### Traditional Risk Response Plan

Create a **Risk Response Plan and Align it with the Internal Audit Plan**

<table>
<thead>
<tr>
<th>Significant Activity</th>
<th>Sub-Process</th>
<th>Impact</th>
<th>Probability</th>
<th>Composite</th>
<th>Risk Map Quadrant</th>
<th>Risk Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery / Business Continuity Plan</td>
<td>Information Technology</td>
<td>3.81</td>
<td>3.07</td>
<td>3.44</td>
<td>4</td>
<td>DR / BCP testing is planned for March 2014</td>
</tr>
<tr>
<td>Environmental Reporting &amp; Compliance</td>
<td>Facilities</td>
<td>3.53</td>
<td>3.11</td>
<td>3.32</td>
<td>4</td>
<td>Compliance Audit over for Phase I and II Environmental is planned for November 2014</td>
</tr>
<tr>
<td>Training and Competencies</td>
<td>Human Resources</td>
<td>2.83</td>
<td>2.53</td>
<td>2.68</td>
<td>4</td>
<td>Monitoring of training compliance is performed quarterly by HR. Employee competencies are part of the Annual Employee Evaluation</td>
</tr>
<tr>
<td>Emergency Response Plans</td>
<td>Security</td>
<td>3.18</td>
<td>2.68</td>
<td>3.07</td>
<td>4</td>
<td>Included in the 2014 Internal Audit Plan</td>
</tr>
<tr>
<td>Physical Security</td>
<td>Security</td>
<td>2.3</td>
<td>2.48</td>
<td>2.66</td>
<td>3</td>
<td>Included in the 2014 Internal Audit Plan</td>
</tr>
<tr>
<td>Incident Reporting and Investigation</td>
<td>Human Resources</td>
<td>2.80</td>
<td>2.48</td>
<td>2.64</td>
<td>3</td>
<td>Included in the 2014 Internal Audit Plan</td>
</tr>
<tr>
<td>Network Security (Encryption, Logical Access, Virus, Internal or External)</td>
<td>Information Technology</td>
<td>3.71</td>
<td>2.85</td>
<td>3.28</td>
<td>4</td>
<td>Network security will be added to the 2014 internal audit plan. Application access is addressed through SOX Compliance procedures. 2014 Internal Audit Plan</td>
</tr>
<tr>
<td>Critical Application Access and Controls</td>
<td>Information Technology</td>
<td>3.06</td>
<td>2.63</td>
<td>2.85</td>
<td>4</td>
<td>Included in the 2013 Internal Audit Plan</td>
</tr>
<tr>
<td>Debt Covenant Compliance</td>
<td>Debt and Equity</td>
<td>3.32</td>
<td>3.09</td>
<td>3.21</td>
<td>4</td>
<td>Included in the 2014 Internal Audit Plan</td>
</tr>
<tr>
<td>Monitoring Collateral Provisions and Contingencies</td>
<td>Debt and Equity</td>
<td>3.00</td>
<td>1.67</td>
<td>2.33</td>
<td>3</td>
<td>Included in the 2013 Internal Audit Plan</td>
</tr>
</tbody>
</table>
Inherent vs. Residual Risk

**Inherent Risk:**
The natural state of risk in an uncontrolled activity.

**Residual Risk:**
The risk of the processes with consideration of controls and other risk mitigation steps.

- Risk Response Plan
- Monitoring Activities

and

Internal Audit’s efforts to ensure the desired residual risk is met
<table>
<thead>
<tr>
<th>Audit Coverage</th>
<th>Initial Risk Rating</th>
<th>Initial Audit Date</th>
<th>2nd Audit/ Follow Up Date</th>
<th>Audit Rating</th>
<th>Recommendation Count</th>
<th>Other Monitoring Activities</th>
<th>Recent Operational Changes</th>
<th>Residual Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Credit Cards</td>
<td>High</td>
<td>2/20/2008</td>
<td>8/15/2013</td>
<td>Needs Improvement- Design &amp; Effectiveness</td>
<td>10</td>
<td></td>
<td>MCC code restriction</td>
<td>High</td>
</tr>
<tr>
<td>Payroll Processing</td>
<td>High</td>
<td>11/24/2008</td>
<td></td>
<td>Needs Improvement- Design &amp; Effectiveness</td>
<td>16</td>
<td></td>
<td>New credit card vendor</td>
<td>High</td>
</tr>
<tr>
<td>Cash Receipts Audit</td>
<td>Moderate</td>
<td>7/7/2009</td>
<td>8/15/2012</td>
<td>Satisfactory</td>
<td>9</td>
<td></td>
<td>30% turnover in department</td>
<td>Moderate</td>
</tr>
<tr>
<td>Vendor Acceptance Review</td>
<td>High</td>
<td>9/1/2009</td>
<td>5/16/2012</td>
<td>Needs Improvement- Design &amp; Effectiveness</td>
<td>15</td>
<td></td>
<td>New purchasing manager</td>
<td>High</td>
</tr>
<tr>
<td>Employee Benefits</td>
<td>Moderate</td>
<td>5/21/2010</td>
<td></td>
<td>Needs Improvement- Effectiveness</td>
<td>11</td>
<td></td>
<td>DOL Reporting</td>
<td>Low</td>
</tr>
<tr>
<td>Purchase to Pay</td>
<td>High</td>
<td>6/2/2010</td>
<td>4/26/2013</td>
<td>Satisfactory</td>
<td>7</td>
<td></td>
<td>New purchasing manager</td>
<td>Moderate</td>
</tr>
<tr>
<td>IT General Computer Controls</td>
<td>High</td>
<td>6/18/2009</td>
<td>1/15/2012</td>
<td>Satisfactory</td>
<td>7</td>
<td></td>
<td>SOC Reports for DR Site</td>
<td>Moderate</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Moderate</td>
<td>6/22/2012</td>
<td></td>
<td>Satisfactory</td>
<td>5</td>
<td></td>
<td>New healthcare legislation</td>
<td>Low</td>
</tr>
<tr>
<td>Marketing and External</td>
<td>Moderate</td>
<td>7/10/2012</td>
<td></td>
<td>Needs Improvement- Design &amp; Effectiveness</td>
<td>13</td>
<td></td>
<td>Outsourced Marketing Consulting</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

**Risk Monitoring Activities**
## Risk Response Plan

<table>
<thead>
<tr>
<th>Ranking</th>
<th>PROCESS AREA</th>
<th>FUNCTIONAL AREA</th>
<th>HIGHEST RISK CATEGORY</th>
<th>2ND HIGHEST RISK CATEGORY</th>
<th>3RD HIGHEST RISK CATEGORY</th>
<th>OVERALL AVERAGE</th>
<th>RISK RESPONSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information Security</td>
<td>Operational</td>
<td>Information Technology</td>
<td>Regulatory and Compliance</td>
<td>Reputational</td>
<td>5.00</td>
<td>Dedicated Information Security Officer responsible for monitoring security. The last IT assessment was performed in FY2011. The Organization restricts physical access to the IT area in a 3-Part Physical Access scheme. The College participates in the Greater Austin Area Telecommunications Network (GAATN). The College also has a redundant recovery site. Include in 2015 Audit Plan</td>
</tr>
<tr>
<td>2</td>
<td>Payroll</td>
<td>Financial</td>
<td>Information Technology</td>
<td>Financial and Fraud</td>
<td>Operations and Complexity</td>
<td>4.85</td>
<td>Risks are partially addressed by the annual financial statement audit. Include in 2015 Audit Plan</td>
</tr>
<tr>
<td>3</td>
<td>Human Resource Administration</td>
<td>Operational</td>
<td>Information Technology</td>
<td>Regulatory and Compliance</td>
<td>Reputational</td>
<td>4.67</td>
<td>Human Resources Audit completed in 2014</td>
</tr>
<tr>
<td>5</td>
<td>Database Administration / ERP</td>
<td>Operational</td>
<td>Information Technology</td>
<td>Financial and Fraud</td>
<td>Operations and Complexity</td>
<td>4.50</td>
<td>Monitored by routine external reviews of software licensing and ERP functionality and utilization study, last performed in 2013.</td>
</tr>
<tr>
<td>6</td>
<td>Budget and Planning</td>
<td>Financial</td>
<td>Financial and Fraud</td>
<td>Operations and Complexity</td>
<td>Reputational</td>
<td>4.44</td>
<td>Monitored by the Board and the annual approval of the budget</td>
</tr>
<tr>
<td>7</td>
<td>Purchasing</td>
<td>Financial</td>
<td>Reputational</td>
<td>Financial and Fraud</td>
<td>Operations and Complexity</td>
<td>3.79</td>
<td>Risks are partially addressed by the formalization of Board Policy 2100-Purchasing, recurring grant audits, and the 2012 Procurements Internal Audit. Include in 2017 Audit Plan</td>
</tr>
<tr>
<td>8</td>
<td>Accounts Receivable</td>
<td>Financial</td>
<td>Information Technology</td>
<td>Reputational</td>
<td>Financial and Fraud</td>
<td>1.77</td>
<td>Risks are partially addressed by the annual financial statement audit. The College relies on outsourced collection agencies.</td>
</tr>
</tbody>
</table>
Prioritize audit activities to ensure that strategically impactful risks and activities are reviewed.

80%

- Prioritize resources on most significant risks in the Entity-wide and Process-level Risk Assessments
- Focus on Risk Response Plan activities will cover some compliance objectives

20%

- Compliance Obligations (SOX, FDICIA, PCI, HIPAA, etc.)
- New areas or changes that are outside of the Enterprise Risk Assessment
# ERM-based Audit Plan

**Planned Risk Based Internal Audits**

<table>
<thead>
<tr>
<th>Process</th>
<th>Key Risk Areas</th>
<th>Risk Rating</th>
<th>Summary Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advertising/Marketing</td>
<td>Reputation, Economic, Financial Stability</td>
<td>High</td>
<td>Internal Audit will include an evaluation of risks and internal controls in place related to the Organization's Advertising activities. Activities to be evaluated will include Market Analysis, Campaign Development, Quality Control Review, Publication Release, and Distribution.</td>
</tr>
<tr>
<td>Information Security</td>
<td>Information Technology, Business Environment</td>
<td>High</td>
<td>Internal Audit will include an evaluation of risks and internal controls in place related to the Organization's Information Security practices. Activities to be evaluated will include Internal and External Security, Logical Access, Physical Access, and Compliance with security and privacy requirements.</td>
</tr>
<tr>
<td>Disaster Recovery / Business Continuity Planning</td>
<td>Regulatory, Reputaion, Operational</td>
<td>Moderate</td>
<td>Internal audit will include an evaluation of the disaster recovery plan and procedures to restore Organizational data and operations in the event a disaster event occurs. Activities to be evaluated will include, Disaster Identification, Scenario Planning, Resumption Planning and Periodic Testing.</td>
</tr>
</tbody>
</table>

**Planned Internal Audit Follow-up**

<table>
<thead>
<tr>
<th>Process</th>
<th>Key Risk Areas</th>
<th>Risk Rating</th>
<th>Summary Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchasing</td>
<td>Financial Stability, Economic, Operational</td>
<td>Moderate</td>
<td>Internal Audit will perform follow-up procedures on prior Internal Audit findings to ensure corrective action has been taken.</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Human Capital, Demographic, Political</td>
<td>High</td>
<td>Internal Audit will perform follow-up procedures on prior Internal Audit findings to ensure corrective action has been taken.</td>
</tr>
<tr>
<td>Construction Management</td>
<td>Economic, Reputaion, Regulatory</td>
<td>High</td>
<td>Internal Audit will perform follow-up procedures on prior Internal Audit findings to ensure corrective action has been taken.</td>
</tr>
</tbody>
</table>

**Planned Compliance Internal Audits**

<table>
<thead>
<tr>
<th>Process</th>
<th>Key Risk Areas</th>
<th>Risk Rating</th>
<th>Summary Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Privacy</td>
<td>Regulatory, Information Technology, Business Environment</td>
<td>Moderate</td>
<td>Internal Audit will include an evaluation of the Organization's controls in place related to customer data privacy and compliance with privacy regulations. Activities to be evaluated will include, Data Collection, Data Entry, Data Storage (digital and manual), Data Security, and Data Transmission.</td>
</tr>
<tr>
<td>PCI Readiness</td>
<td>Regulatory, Information Technology, Reputaion</td>
<td>Moderate</td>
<td>Internal Audit will include an evaluation of the Organization's controls and processes in place related to compliance with PCI DSS standards. Activities to be evaluated will include Data Storage and Retention, Network Security, Vulnerability Management, Policies and Procedures, and Network Scanning.</td>
</tr>
</tbody>
</table>
Recap: Benefits of an ERM-based Focus

- ERM approach ensures that critical risks and processes are linked to strategic objectives to ensure coverage of the “right risks”.
- Drives the establishment and monitoring of KRI's to monitor the root causes of critical risks for more proactive risk management.
- Creates an awareness of risk across the entity that enhances collaboration between departments and cooperation with internal audit.
Recap: Benefits of an ERM-based Focus

• Provides a broader view of risk to avoid compartmentalized thinking and ensure a value-added approach.

• Assists in engagement scoping to ensure that audit procedures are focused on key risks and strategic initiatives.

• Enhances the perception of the internal audit function as a trusted advisor that adds value to the organization.
• Have you attempted an ERM based approach to developing an internal audit plan?

• What obstacles did you have to overcome?
QUESTIONS & ANSWERS

Alyssa G. Martin, CPA, MBA | Dallas Executive Partner, Advisory Services
512.609.1975 | alyssa.martin@weaver.com

Daniel Graves, CPA | Senior Manager, Advisory Services
512.609.1913 | daniel.graves@weaver.com