Applying & Utilizing Risk Assessments to Establish Work Plans & Audit Objectives

IIA – San Diego Chapter’s Government Seminar
March 9, 2016

Lee Parravano, CPA, CIA, CGMA
Internal Auditor at SDCERS
Discussion Topics

- Standard 2010 Risk Based Audit Plans
- Standard 2201 Engagement Planning
- Standard 2210 Engagement Objectives
Standard 2010

The Internal Auditor must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organization’s goals.
Mission Statement

SDCERS’ Mission
To deliver accurate and timely benefits to participants and ensure the Trust Fund’s safety, integrity and growth
## Risk Assessment

<table>
<thead>
<tr>
<th>Ln#</th>
<th>Division</th>
<th>Key Work Activity</th>
<th>Complexity</th>
<th>Change</th>
<th>Materiality</th>
<th>Strategic</th>
<th>Reputation</th>
<th>Weighted Score</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Finance</td>
<td>Investment Accounting/Reconciliation</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>1</td>
<td>357</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>Legal</td>
<td>Draft, Review, and Assist Negotiate Contracts</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>2</td>
<td>355</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>Benefits Admin.</td>
<td>Plan Sponsor Contribution &amp; Reporting</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>339</td>
<td>9</td>
</tr>
<tr>
<td>4</td>
<td>Benefits Admin.</td>
<td>Member Salary Data Posting</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>339</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Legal</td>
<td>Oversee and Monitor Other Compliance Issues</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>339</td>
<td>9</td>
</tr>
<tr>
<td>6</td>
<td>Information Tech.</td>
<td>Intergency/Intelligence Data Transmission Management</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>265</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>Member Services</td>
<td>Retiree Health Insurance Reimbursements / Enrollment</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>265</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>Finance</td>
<td>Health Insurance Accounting/Payments</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>264</td>
<td>8</td>
</tr>
<tr>
<td>9</td>
<td>Investments</td>
<td>Monitoring / Rebalancing of Portfolio</td>
<td>3</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>264</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>Benefits Admin.</td>
<td>Required Minimum Distribution Processing</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>262</td>
<td>7</td>
</tr>
</tbody>
</table>
Standard 2201

Internal auditors must consider:

- Significant risks to the activity, its objectives, resources and operations and the means by which the potential impact is kept to an acceptable level.
- The adequacy and effectiveness of the activity’s risk management and control systems compared to a relevant framework.
- The opportunities for making significant improvements to the activity’s risk management and control processes.
Standard 2210

Internal auditors must conduct a preliminary assessment of risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.
Preliminary Assessment

- Interviewing:
  - Management
  - Chief Compliance Officer
  - General Counsel
  - Staff
Publications & Resources

APPFA Publications

- Statements of Key Investment Risks and Common Practices to Address Those Risks
- Operational Risks of Defined Benefit and Related Plans and Controls to Mitigate Those Risks
- Model Audit Committee Charter
- Model Internal Audit Department Charter
- Model Code of Conduct and Ethics Policy

Internet Resources
Preliminary Assessment

You are here: Home > Resources > Abstracts

Abstracts

Submit an Abstract
Please sign in and use this form to post your audit report abstracts. Submissions may be posted in the following categories:

- Finance
- Housing & Social Services / Community Development
- Human Resources
- Information Technology
- Parks, Recreation & Library
- Performance & Risk Management / Service Accomplishments
- Procurement & Contract Compliance
- Public Safety & Court Operations
- Public Works & Capital Facilities
- Public Utilities & Environmental
- Transportation / Fleet
- Miscellaneous
- View All
Other Considerations

- Engagement Duration
- Engagement Staffing
- Extent of Documentation
- Managements Self Assessments
- Prior External or Internal Audit Findings
- Engagement Audience
Plan Sponsor Risks and Controls

- **Risks**
  - Incorrect Compensation is reported
  - Contributions wrong because of contribution rates or calculations
  - Pensionable salary includes ineligible earnings (OT, per diem)
  - Contributions on ineligible earnings
  - Retroactive payments not handled correctly
  - Incorrect service credit

- **Controls to Mitigate**
  - Suggest Internal Audit conduct audits
  - Provide training
  - Conduct reviews on eligible wages
  - Independently recalculate contributions
  - Automatic computerized checks on transmittal information
  - Perform variance analysis on pensionable salary or other info
## Risks & Control Matrix

### Plan Sponsor Audit

#### Risks and Controls Assessment Matrix

<table>
<thead>
<tr>
<th>Risk #</th>
<th>Risk Description/Issue</th>
<th>Fraud Risk (Y/N)</th>
<th>Inherent Risk</th>
<th>Control #</th>
<th>Controls</th>
<th>Internal Control Rating</th>
<th>Actual (A) or Potential (P) Control?</th>
<th>Vulnerability Assessment</th>
<th>Audit Program (AP) Testing Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The Plan Sponsor may incorrectly report compensation to SDCERS</td>
<td>Y</td>
<td>Moderate</td>
<td>1.1</td>
<td>Payroll Reports automatically generate transmittal file that is sent to SDCERS based on payroll configuration.</td>
<td>Adequate</td>
<td>A</td>
<td>Moderate to High</td>
<td>AP #4b - Review payroll records and compensation reported to SDCERS for 25 members and determine if they reconcile to employees personnel file (personnel records to payroll register).</td>
</tr>
<tr>
<td>2</td>
<td>The Plan Sponsor may not enroll all eligible employees into SDCERS membership.</td>
<td>Y</td>
<td>Moderate</td>
<td>2.1</td>
<td>Each plan sponsor has detailed membership criteria. Any change in status requires a Personnel Action Form or its equivalent. A Personnel Action Form alerts the payroll/HR to make changes as necessary. The change made by payroll/HR would automatically enroll/not enroll a Member.</td>
<td>Weak</td>
<td>A</td>
<td>Low to Moderate</td>
<td>AP #5 - Haphazardly select 25 employees being paid on 2 pay registers and determine if the employees were correctly classified as Members or not. Additionally determine if Plan Sponsor complied with Sections 7522.56 and 7522.57 for employment after 1/1/13 for PEPRA members.</td>
</tr>
</tbody>
</table>
Risk Assessment on Activity

Good work, but I think we might need just a little more detail right here.
Questions?