Effective Audit Planning: From Engagement Risk Assessments To Building Work Programs

Linh Truong
Director Internal Audit, Orthofix
Linh Truong, CPA, CIA, CISA

- Currently CAE at Orthofix
- Former CAE – Kosmos Energy
- Former CAE – Alon USA
- Former Director of Business Process Compliance – Affiliated Computer Services (now a division of Xerox)
- Founder of Energy CAE Shareforum
- Speaking experience:
  - IIA’s CAE Spotlight
  - IIA’s Superconference
  - IIA/ISACA’s GRC conference
  - MISTI’s Auditworld
  - Women’s Energy Network
  - Energy CAE Shareforum
Orthofix is a global medical device company with four Business Units:
- Biostim
- Biologics
- Spine Fixation
- External Fixation

- $400M in annual revenues
- Founded in 1980 in Verona, Italy
- Products sold in over 50 countries
- 900 employees worldwide with offices in:
  - Italy
  - Germany
  - France
  - UK
  - Brazil
  - Australia
  - Puerto Rico

(C) 2017 GoldCal LLC
QUOTES ON PLANNING

- “Everyone has a plan - until they get punched in the face.”
  — Mike Tyson, Boxer.

- “People often complain about lack of time when the lack of direction is the real problem.”
  — Zig Ziglar
QUOTES ON PLANNING

- “Have a plan. Follow the plan, and you'll be surprised how successful you can be. Most people don't have a plan. That's why it's easy to beat most folks.”
  — Paul "Bear" Bryant, football coach, University of Alabama's Crimson Tide.”

“Those who plan do better than those who do not plan even though they rarely stick to their plan.”
Winston Churchill, British Prime Minister
THE INTERNAL AUDIT PROCESS

1. Audit Assigned for Audit Plan (through Risk Assessment Process)
2. Preliminary Work
3. Development of Audit Program
4. Conducting Fieldwork
5. Documenting Results and Observations
2200 – Engagement Planning

Internal auditors must develop and document a plan for each engagement, including the engagement’s objectives, scope, timing, and resource allocations.

2201 – Planning Considerations

In planning the engagement, internal auditors must consider:

- The objectives of the activity being reviewed and the means by which the activity controls its performance
- The significant risks to the activity, its objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level
- The adequacy and effectiveness of the activity’s risk management and control processes compared to a relevant control framework or model
- The opportunities for making significant improvements to the activity’s risk management and control processes

(C) 2017 GoldCal LLC
2210 – Engagement Objectives

Objectives must be established for each engagement

- **2210.A1** – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment.

- **2210.A2** – Internal auditors **MUST** consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives.

- **2210.A3** – Adequate criteria are needed to evaluate controls. Internal auditors must ascertain the extent to which management has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must work with management to develop appropriate evaluation criteria.
IIA STANDARDS – ENGAGEMENT SCOPE

- **2220 – Engagement Scope**
  - The established scope must be sufficient to satisfy the objectives of the engagement

- **2220.A1** – The scope of the engagement must include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties

- **2220.A2** – If significant consulting opportunities arise during an assurance engagement, a specific written understanding as to the objectives, scope, respective responsibilities, and other expectations should be reached and the results of the consulting engagement communicated in accordance with consulting standards
ELEMENTS OF PRELIMINARY WORK

1. Define Audit Objectives (Risk-Based)
2. Define Scope
3. Knowledge Gathering
4. Authoritative Research
5. Interview Management
6. Understand / Document Process
7. Work Program
Defining Audit Objectives
DEFINE AUDIT OBJECTIVES

- Understanding the goals and objectives of an audit
  - Why is this audit being performed?
  - Why was it identified as a risk?
  - Why was it deemed important enough to appear in the audit plan?

- The above questions can be answered with the statements (which are really saying the same thing):
  - Because it addresses a risk that could negatively impact the company’s ability to achieve strategic goals/objectives
  - The audit is a part of an audit plan that is aligned with the company’s strategic goals/objectives
WHAT ARE SOME STRATEGIC OBJECTIVES?

- Recruiting/Retaining top talent
- Growth (Organic / Inorganic)
  - Maintaining an effective Supply Chain function:
    - Inventory
    - Procurement
  - Regulatory Compliance:
    - FCPA
    - SOX
    - FDA

(C) 2017 GoldCal LLC
## Aligning Audit Plan to Company Strategic Objectives

<table>
<thead>
<tr>
<th>Strategic Business Goal</th>
<th>ERM Risks</th>
<th>Internal Audit Engagement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee engagement / development</td>
<td>Loss of key employees</td>
<td>HR Audit:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Talent Acquisition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Succession Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Training/Development</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>Lack of compliance with SEC causes a restatement or penalties.</td>
<td>SOX Compliance Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Anti-corruption / FCPA Audits</td>
</tr>
<tr>
<td>Maintain an effective Supply Chain function that adequately supports Operations at xxxx production levels.</td>
<td>Lack of compliance with Anti-corruption / FCPA regulations results in criminal or civil sanctions as well as damage to the Company’s reputation.</td>
<td>Procurement Audit</td>
</tr>
<tr>
<td></td>
<td>Loss of key supplier disrupts Operations and impacts Sales/Revenue goals.</td>
<td>DR/BC Readiness Assessment</td>
</tr>
<tr>
<td></td>
<td>Inadequate DR/BC plan allows an external event to disrupt or eliminate critical activities.</td>
<td></td>
</tr>
</tbody>
</table>
Question:

What about the Company’s “growth” initiatives? How can Internal Audit help with this strategic objective?
ALIGNING AUDIT PLAN TO COMPANY STRATEGIC OBJECTIVES

Answer:

- **Assess HR function for scalability** - are HR people, processes and tools (systems) capable of
  - Supporting a significant increase in number of employees due to an future acquisition?
  - Processing a significant number of relocations or severance packages
- **Provide due diligence support** – help M&A team assess target company.
- **Post-acquisition integration assessment**

(C) 2017 GoldCal LLC
WHAT TYPE OF ENGAGEMENT SHOULD THIS BE?

Some questions to ask to determine what the right audit engagement should be:

- How mature is this function/process?
- Are there any policies/procedures?
- How long has this function been in place?
- Has this function/process ever been assessed?
- How manual/automated is this process?
- Are there any management monitoring controls or feedback mechanism?
- How sophisticated is leadership regarding controls or control environment?
TYPES OF ENGAGEMENTS

- Consulting Projects / Management Requested Special Project
- Gap Assessments / Risk Assessments
- Audits
  - Financial Audit
  - IT Audit
  - Integrated Audit
  - Compliance Audit
  - Operational Audit

(C) 2017 GoldCal LLC
INTEGRATED AUDITS - EXAMPLE

- HR Audit - processes included in scope:
  - Talent Acquisition
  - Performance Evaluation
  - Termination Process
  - Compensation
  - Contractor Governance
  - Employee Data Privacy

How would an Integrated Audit benefit this HR Audit?
### Integrated Audits - Example

- **Termination Process**
  - Is process to terminate access for (terminated employees) to all company systems effective/timely

- **Compensation**
  - Are interfaces effective between equity compensation administration system and Accounting system?

- **Contractor Governance**
  - Is there a module to track contractors or are contractors being tracked on excel spreadsheets?

- **Employee Data Privacy**
  - Are logical access / data security controls effective to prevent data privacy breaches?

(C) 2017 GoldCal LLC
WHAT IF?

…the organization does not have an ERA / ERM in place?
Now Let’s Exercise!
The Company has had very high turnover and VP of HR would like to know if HR’s processes are effective in supporting the strategic objective of “Acquiring/Retaining the best talent for organization”.

What processes should be in scope for our review/audit?
GROUP EXERCISE – WHAT ARE THE RISKS?

What are the risks?
GROUP EXERCISE – WHAT ARE THE RISKS?

1. Company hires employees that are not competent to perform required job duties.
2. New employees are not properly trained to effectively perform job duties.
3. Company does not attract/retain candidates/employees effectively due to less than market compensation.
4. Company does not have an effective performance measurement process.
5. Company does not have an effective succession planning process.
GROUP EXERCISE – WHAT ARE THE AUDIT OBJECTIVES?

1. Assess effectiveness of talent acquisition process.
3. Assess effectiveness of compensation process.
5. Assess effectiveness of succession planning process.
Defining Scope
DEFINING SCOPE

- What are the key processes included in scope?
- What is the timeline for the engagement?
- Will the review include both US and International processes?
- What is the period that will be tested?
- Which physical locations will be impacted?
- Which depts will be impacted?
RESOURCE ALLOCATION

- Roles / Responsibilities
  - Lead Auditor
  - Audit Staff
  - SME (as needed)

- Other things to consider:
  - If SME is needed, source externally or internally?
  - Travel required? If international travel is required, obtain necessary travel visas, immunization shots, etc.
  - Are SME costs / travel costs within budget?
Knowledge Gathering
Knowledge Gathering

- Narratives
- Policies & Procedures
- Organizational Chart
- Previous Audit Reports
- SOX Flowcharts, Controls, Deficiencies
- BoD and BoD Committee presentations
- Management Reports, Performance Metrics
What If?

...the function or process being assessed does not have any policies or procedures?

What do you audit against?
Authoritative Research
AUTHORITATIVE RESEARCH

- Audit Director’s Roundtable
- Knowledgeleader.com
- www.aicpa.org
- www.auditnet.org
- www.theiia.org
- www.isaca.org
- www.acuia.org
- www.sec.org
- Peer Groups
- Big 4 Whitepapers, industry best practices
- Benchmarking data
Interview Management

(C) 2017 GoldCal LLC
WHO SHOULD YOU INTERVIEW

- Executives
- Functional Management
- Process Owners of the audited area
- “Customers” of the audited area
  - Process Owners who receive deliverables / services from the audited area
  - Process Owners who provide data, information into the audited area
GOOD INTERVIEW HABITS

- Have an agenda - Do not conduct an interview or meeting WITHOUT an agenda
- Send questions in advance
- Organize multiple topic areas
- Introduce multiple interviewers/participants
- Helps keep all parties on track
- Next steps / Summarize action items
MORE GOOD INTERVIEW HABITS

- What this Interview is Not!
  - An Interrogation
  - A Fraud Interview
  - A Structured Interview

Who knows more about their business than they do!
Interview Protocol

- Never be Late
- Stay within the Allotted Time
- Stick to Relevant Questions
- Move from Simple to Complex
- Establish Rapport
  - Professionalism
  - Commonalities
  - Familiarity
Interview Questions
10 Useful Interview Questions

- Is there a **current** policy/procedure in place?
- Is the policies/procedures in place reviewed/updated at least annually?
- How are the policies/procedures communicated?
- Have there been any system **changes**?
- Have there been any process **changes**?
- Have there been any people **changes**?
- Which processes/procedures are critical to achieving objectives?
- What are some pain points in the process?
- What management reports are reviewed?
- What keeps you up at night?
Understand and Document Process
Walkthroughs trace the transaction step-by-step through the process from its inception to the final disposition/recording

Objectives:

- Verify control design effectiveness
- Identifies any interfaces
- Identifies reports used in
- Identifies reports generated by the process
Best Practices in Process Narrative Development:

- Documentation should include *Who*, *What*, *Where*, *When* & *How*: Indicate *who* is performing *what* action *where* (systems) and *how* the action occurs.
- Indicate whether each action is *automated* or *manual*.
- Indicate the *frequency* of action where appropriate. Avoid vague terms such as periodically, often, sometimes, or occasionally.
- Indicate any *systems* used in the process.
- Identify *reports and supporting documents* within the step description.
Document the *current state only*

- Avoid ideal, future, or past state. If a process is in the middle of a change, please consult jointly with the Lead Auditor / your Manager to identify how best to document that process. If it is a new process, indicate the date the process was put into effect and document only the new process.
- Use complete *job titles* to indicate who is performing the action. Avoid using a person’s name or using only a Department or Business Unit name.
Building an Effective Workprogram
WORKPROGRAM

- The Workprogram addresses:
  - What is to be done
  - When it is to be done
  - How it is to be done
  - Who will do it
The Workprogram should document:

- Source for population
- Verification of completeness/accuracy of population
- How many samples were selected
- Reference to actual workpapers
- Results of test
Steps for Building an Work Program

1. Identify Specific Audit Risks (previously discussed)
2. Define Expected Controls
3. Document Actual Controls (or lack thereof)
4. Define Overall Steps to Testing Objectives
5. Define Specific Work Sub-Steps for Each Overall Step
TRANSACTION ASSERTIONS

1. Occurrence
2. Accuracy/Valuation
3. Completeness
4. Timeliness
5. Classification
OTHER CONSIDERATIONS

1. Governance
2. Authorization / Approval
3. Management Monitoring
4. Performance Measurement
5. Reporting
# Sample Work Program

<table>
<thead>
<tr>
<th>Risks</th>
<th>Activities / Processes / Controls</th>
<th>Control Test</th>
<th>Detail Control Test</th>
<th>Link to Testing</th>
<th>Results of Testing</th>
<th>Tested by</th>
<th>Date</th>
<th>Reviewed by</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The Policy is periodically and timely communicated to company personnel.</td>
<td>Obtain evidence of periodic communication of the policy and/or timely communication of policy changes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Policy is reviewed by the CCO on an annual basis.</td>
<td>Obtain evidence of annual review of related policies.</td>
<td>In the event, modifications were made to the FCPA policy during the review period, training materials were updated to reflect changes in the Policy.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BoD communication includes compliance activities.</td>
<td>Obtain evidence of BoD agendas and minutes of meetings.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance objectives/goals are incorporated into performance management and/or compensation initiatives.</td>
<td>Understand and obtain evidence of how compliance objectives are incorporated into performance management or compensation structure.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Let’s Exercise!
## Workprogram Exercise

<table>
<thead>
<tr>
<th>Risks</th>
<th>Expected Controls</th>
<th>Activities / Processes / Controls</th>
<th>Control Test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Expected Controls**

- **Risk:** Company hires employees that are not competent to perform required job duties.

- **Expected Controls:**
  - Company has job descriptions for all positions.
  - Recruiting process requires minimum of 3 candidates.
  - Interview process requires 3 different interviewers.
  - Recruiting process requires background checks on candidates prior to extending offer.
  - Recruiting process requires 3 business references.

- **Control Test:** Select a sample of xx new hires
Select a sample of xx new hires and verify that the following were performed:

- There is a job description for the position.
- At least 3 candidates were interviewed.
- There were at least 3 different interviewers who interviewed the candidate and feedback was obtained from all interviewers.
- A criminal background check was completed prior to the offer being extended.
- At least 3 business references were obtained.
WHAT ELSE SHOULD YOU REVIEW TO ASSESS THE EFFECTIVENESS OF COMPANY’S TALENT ACQUISITION:

- What is the turnover rate and how does it compare to industry standards?
- For voluntary terminations, what are common themes from exit interviews?
- For involuntary terminations, what are common themes (competency? culture fit? communication?)
- Does performance evaluation process solicit upward feedback for managers?
- What areas does the company score low on engagement survey?
**Sampling Size**

- Identify your population first
- Base sample size on risk
- Consider transaction frequency
- Establish a sampling technique/process/policy
- Consider the number of exceptions you expect to find (more exceptions = more samples) – set your error rate
- Ask your external auditor
  
  or

- Test entire population (using Data Analytics)
TYPES OF AUDIT TESTS

- Design only (no control testing)
- Interviews only (for Risk / Gap Assessments)
- IT testing (analyze files, screen prints, procedures, logs, and audit trails)
- Tests of control effectiveness
- Substantive tests
- CAATs / Data Analytics
Data Analytics

Data Analytics is the process of accessing, normalizing and modeling data with the intent of discovering useful information.

Software/Tools:
- Excel
- Access
- Excel Add-ins (TeamMate Analytics, ACL, et.)
- ACL
- IDEA
- IBM/Watson Analytics
- Tableau
DATA ANALYTICS

- Why we don’t use data analytics:
  - It takes a lot of TIME!!!
  - Perceived difficulty
  - Entities don’t have the information needed

- If you don’t have the tools or expertise:
  - Outsource it
  - Use Excel
  - Get trained and get started!
Let’s Exercise!
What type of Exception reports could be generated from a T&E system?
What type of Exception reports could be generated from a T&E system?

- Meals > predefined threshold per attendee
- Top spenders overall
- Top spenders in “high risk” categories:
  - Miscellaneous
  - Incidentals
  - Gifts / Charitable Contributions
- Duplicate meals (e.g. Dinners) on same day
- T&E expenses not paid by Corporate Card
Value Add

- How does this audit add value?
  - Identify potential fraud and abuse
  - Identify lost opportunities:
    • Preferred vendor utilization (volume discounts)
    • Advance ticket purchases vs late bookings
    • Optimize rebates
    • Minimize late fees
  - Provide input into T&E Policy
  - Provide input into automated controls
  - Provide input into recurring Management Reports
EVIDENCE REQUIREMENTS

- **Sufficient** – Measure of quantity of the evidence; should be collected and evaluated sufficient information so that the reasonably informed unbiased person agreed with the auditor’s conclusions.

- **Reliable** – Comprises the measure of reliability and adequacy of the source of evidence and the method of seeking thereof; generally, information received from a third party that is independent is more reliable; the evidence is reliable where it is gained via direct physical examination, observations and inspection and where it is received in the documentary form, rather than verbally. Degree of information reliability increases where it is received from several sources;

- **Adequate** – Measure of adequacy of the evidence. Audit evidence may be physical, testimonial, documentary and analytical.
Final Thoughts
COMMUNICATION PLAN

- Have a touchpoints throughout audit
- Ask What Frequency is Best
- Do it in Person
- Transparent throughout the audit process (build buy-in)

No Surprises!
AUDIT ENGAGEMENT MONITORING

- Benchmarks/Milestones
- Vetting Observations
- Progress Reports
- Timely Workpaper Reviews
- Update Meetings

Did the audit achieve it’s objectives?
SUMMARY

- Effective planning is the key to an effective audit
- Company’s Strategic Plan should be your guide
- Gauge Initial Risk Assessment and Update Throughout
- Goal – effective planning will allow staff with minimum experience and supervision to complete fieldwork
Questions?
Linh Truong’s contact info:

linhtruong@orthofix.com

- Office Phone: 214-937-2509
- Cell Phone: 469-971-4037