OP AUDIT PROCESS
Audit Process

1. Identifying Risks
2. Define Audit Objectives (Risk-Based)
3. Define Scope
4. Knowledge Gathering
5. Authoritative Research
6. Interview Management
7. Understand / Document Process
8. Work Program
9. Recommendations / Report Writing
Risk-based Performance Audits

• Start with an organization’s objectives and associated performance measures
• Focus on an evaluation of performance risks and controls related to those objectives
• Help the organization achieve the desirable goals and protect it from bad or undesirable things happening
• Help reduce the chance of missed opportunities
• Provide suggestions for improvement in controls designed to mitigate the risks associated with meeting performance objectives
What is Risk

• Risks are things that could prevent an organization from meeting its objectives

• IIA definition - **Risk** is the possibility of an event occurring that will have an impact on the achievement of objectives
  – Risk is measured in terms of impact and likelihood
Risk Responses

- Examples of Risk Response options:
  - Acceptance
  - Avoidance
  - Transfer
  - Mitigation
Assess Inherent Risk – What is IR?

Inherent Risk: The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls)

• Start with inherent (gross risk)
• Identify controls in place that mitigate that risk
• Inherent risk minus controls equals net (residual risk)
• Determine if residual risk is within management’s risk tolerance
• If not, need additional controls / management action items to further reduce net risk
Defining Objectives
Define 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
Business Objectives Cascade

- Mission/Vision
  - Strategic Objectives
    - Objective 1
      - Sub-Objective
      - Sub-Objective
      - Sub-Objective
    - Objective 2
      - Sub-Objective
      - Sub-Objective
      - Sub-Objective
    - Objective 3
      - Sub-Objective
      - Sub-Objective
      - Sub-Objective
### Aligning Audit Plan to 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>Lack of compliance with Anti-corruption / FCPA regulations results in</td>
<td>Anti-corruption / FCPA Audits</td>
</tr>
<tr>
<td></td>
<td>criminal or civil sanctions as well as damage to the Company’s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>reputation.</td>
<td></td>
</tr>
<tr>
<td>Maintain an effective Supply Chain function that adequately</td>
<td>Loss of key supplier disrupts Operations</td>
<td>Procurement Audit</td>
</tr>
<tr>
<td>supports Operations at xxxx production levels.</td>
<td>and impacts Sales/Revenue goals.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inadequate DR/BC plan allows an external event to disrupt or eliminate</td>
<td>DR/BC Readiness Assessment</td>
</tr>
<tr>
<td></td>
<td>critical activities.</td>
<td></td>
</tr>
</tbody>
</table>
Business Objectives Cascade

• Strategies of the business
• Key business objectives
• Related objectives that cascade down the organization from key business objectives
• Assignment of responsibilities to organizational elements and leaders (linkage)
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?
Key Processes

• Discussion with Business (what are their key business objectives?)
• What are the key processes to achieve these business objectives?
• If process is not performed or a control failed, the business objective would not be achieved.
• What could go wrong (key risks)?
• Is there a control that addresses the key risks? (if not, there is a control gap)
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

(C) 2017 GoldCal LLC
Key Processes

• Discussion with Business (what are their key business objectives?)
• What are the key processes to achieve these business objectives?
• If process is not performed or a control failed, the business objective would not be achieved.
• What could go wrong (key risks)?
• Is there a control that addresses the key risks? (if not, there is a control gap)
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
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
What are some good 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 / Document Process
Walkthroughs

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
Process Documentation

• 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.
  – Indicate any **systems** used in the process.
  – Identify inputs and outputs of process (e.g. reports and supporting documents).
3.1 Employee Masterfile Setups - Terminations

**Employee**

- Start
- Submit resignation letter to HR

**Employee Manager/Department Head**

- Start
- Request employee termination

**HR Benefits Manager/HR Generalist**

- Obtain letter from employee
- HR maintains a termination checklist with all related action items for each department for the employee termination. Once terminated in Workday, an email is sent out notifying appropriate parties (e.g., benefits, IS, Payroll, etc.) of the termination. Benefits terminations are communicated to administrator(s) via file feed after final payroll is processed.

**HR Director/HR Manager**

- Review termination request with Employee Manager
- Approved?
  - Approved
    - Inform employee
  - N
- Collect company material
- Conduct exit interview
- Only performed for voluntary terminations if agreed upon by the employee

**Workday**
Example Walkthru Documentation

Processing and Authorization of Wire Transfers:
The banks maintain an updated list of authorized signers for business checking accounts as well as individuals approved to administer wire transactions. Only authorized employees can transact on bank accounts. In order to administer wire transactions, the individuals must be personnel authorized to initiate or approve wire transfers and the wire transfer initiator and approver must be two different individuals. Per inquiry of Angel, Yvette, Rich and herself are responsible for maintaining this updated list of authorized signers with the bank. This list is sent, in excel format, from Bank of America for all entity accounts. Per inquiry of Angel, changes to the authorized signers list maintained for the Bank of America accounts are required to be submitted through either a Banking Resolution or Authorized Signor form and are required to be approved in writing by two of the following individuals:
Example Walkthru Documentation

Control Point OSI.AP.C11: Oracle is configured to route new vendor setups/changes for approval based on the workflow established in the system.

New Vendor Requests:

Vendor – XXXX
Date of test: XXXX
Approver: XXXX

1. Obtain the configuration screenshots in Oracle for new vendor setups and changes.
2. Select a vendor or create a test vendor (used “Test – Do Not Use” vendor #50217 in 2017).
3. Observe the Accounts Payable Administrator change the vendor information.
4. Observe the Sr. Director Accounting and Consolidations approve a new/changed vendor in the queue and obtain a screenshot and verify the “inactive date” is removed after their approval.

NOTE: Config workflow is the same for new and changed vendors.
Building an Effective Workprogram
Steps for building and Audit 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
Steps for building and Audit 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
Assertions

1. Occurrence
2. Accuracy/Valuation
3. Completeness
4. Timeliness
5. Classification
Now Let’s Exercise
Group Exercise – Key Risks

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 key Risks? What are key audit objectives that should be included in our workprogram?
Group Exercise – Key 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 – Key Audit Objectives

1. Assess effectiveness of talent acquisition process.
3. Assess effectiveness of compensation process.
5. Assess effectiveness of succession planning process.
Group Exercise – 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
Group Exercise – Control Tests

• Select a sample of xx new hires and verify that the following were performed:
  – There is a job description for the position and evidence Hiring Manager reviewed/approved.
  – 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.
Group Exercise – Other Considerations

• 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?
Group Exercise – Other Considerations

1. Governance
2. Authorization / Approval
3. Management Monitoring
4. Performance Measurement
5. Reporting
Sample 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!
Now Let’s Exercise
Data Analytics - Example

• What type of Exception reports could be generated from a T&E system for a T&E Audit?
Data Analytics - Example

• 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 – Performance Auditing

- 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
## T&E – Data Analytics Reports

### U.S. Meals $ Over Guideline

<table>
<thead>
<tr>
<th>Meal</th>
<th>(A) Total</th>
<th>(B) Spend Under</th>
<th>(C) Spend Over</th>
<th>(C/B) % Over</th>
<th>(C/A) Over % Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakfast</td>
<td>$50,488</td>
<td>$38,379</td>
<td>$14,898</td>
<td>39%</td>
<td>30%</td>
</tr>
<tr>
<td>Lunch</td>
<td>$80,755</td>
<td>$57,850</td>
<td>$23,257</td>
<td>40%</td>
<td>29%</td>
</tr>
<tr>
<td>Dinner</td>
<td>$108,456</td>
<td>$85,022</td>
<td>$27,020</td>
<td>32%</td>
<td>25%</td>
</tr>
<tr>
<td>Total</td>
<td>$239,699</td>
<td>$181,251</td>
<td>$65,175</td>
<td>36%</td>
<td>27%</td>
</tr>
</tbody>
</table>

### U.S. Policy Guidelines:
- Breakfast $14
- Lunch $25.50
- Dinner $35.50

### U.S. Meal Count Over Guideline

<table>
<thead>
<tr>
<th>Meal</th>
<th>Meal Count</th>
<th>Meals Over Guideline</th>
<th>% Meal Count Over</th>
</tr>
</thead>
<tbody>
<tr>
<td>Breakfast</td>
<td>4,044</td>
<td>941</td>
<td>23%</td>
</tr>
<tr>
<td>Lunch</td>
<td>4,140</td>
<td>997</td>
<td>24%</td>
</tr>
<tr>
<td>Dinner</td>
<td>3,307</td>
<td>1,174</td>
<td>36%</td>
</tr>
<tr>
<td>Total</td>
<td>11,491</td>
<td>3,112</td>
<td>27%</td>
</tr>
<tr>
<td>Inherent Risks</td>
<td>Observations</td>
<td>IA Recommendation</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Travel arrangements not made through Concur or expenses not paid with Corporate Card limit company’s ability to obtain global view of travel spend in Concur,</td>
<td>Europe: Evaluate business case to book all travel directly through Concur to consolidate travel spend visibility to better leverage Company’s purchasing power.</td>
<td>Implement a step in the new hire/onboarding process and in Concur new account set up to remind managers to request corporate credit cards if appropriate and regularly identify travelers submitting expenses but not issued a card and issue them one.</td>
<td></td>
</tr>
<tr>
<td>Cash/non-Corporate Card expense represented 11% of 2016 global Concur spend, limiting spend visibility and rebate opportunity,</td>
<td></td>
<td>US: Determine if it is worthwhile to negotiate contracts with Delta, #2 airline and Enterprise/National, top rental car company.</td>
<td></td>
</tr>
<tr>
<td>Failure to leverage the company’s purchasing power may result in missed opportunities to lower costs,</td>
<td>Orthofix has negotiated rates with American Airlines and several Lewisville area hotels.</td>
<td>Update travel policy guidance to Amex Travel identifying travel arrangers authorized to use dedicated agent to book travel.</td>
<td></td>
</tr>
</tbody>
</table>
**Useful Recommendations**

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>Observations</th>
<th>IA Recommendation</th>
</tr>
</thead>
</table>
| Lack of expense transparency or supporting documentation may limit the company’s ability to prevent or detect fraud and abuse. | All expense reports are reviewed by the Finance personnel. In the US, the review focuses on:  
- HCP Meals documentation  
- Cash reimbursements  
- DOA of approving manager  
- Recipients populated for gifts  
- Attendees populated for Business Meals | Enforce Policy requirements on non-reimbursable expenses, paid only with written approval of CFO. Develop and follow specific audit guidelines for Finance review to support.  
Provide sufficient training to Finance Personnel responsible for Concur to permit them to fully leverage available application controls and reporting.  
Leverage available Amex Travel and Concur Reporting to provide regular management reports to highlight policy non-compliance or abuse. At a minimum, include the following:  
- Arrangements booked/not booked through Concur by employee  
- T&E Expense charged/not charged to Corporate Card by employee  
- First/Business Class Booking policy non-compliance  
- Advance purchase guideline non-compliance  
- Non-compliance to meal spend guideline by employee  
The U.S. T&E team is currently working to define such reports for distribution. |
Quantify Value
## Quantify Value

<table>
<thead>
<tr>
<th>#</th>
<th>Order #</th>
<th>Transaction Date</th>
<th>Category</th>
<th>Account Name</th>
<th>List Price ≠ Contract Price</th>
<th>Contract Price ≠ Selling Price</th>
<th>Net Discount %</th>
<th>Net Total Value of Discount</th>
<th>Evidence of Required Approval?</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>998338</td>
<td>5/16/2018</td>
<td>Delay in uploading prices</td>
<td>SIM (Argentina)</td>
<td>26 of 32 Products</td>
<td>22 of 32 Products</td>
<td>32%</td>
<td>$16,101</td>
<td>N/A</td>
</tr>
<tr>
<td>2</td>
<td>950281</td>
<td>1/18/2018</td>
<td>Human error</td>
<td>MBA Incorporado (Spain)</td>
<td>N/A</td>
<td>1 of 1 Products</td>
<td>17%</td>
<td>$12</td>
<td>No</td>
</tr>
<tr>
<td>3</td>
<td>985011</td>
<td>4/13/2018</td>
<td>Human error</td>
<td>SIM (Argentina)</td>
<td>1 of 9 Products*</td>
<td>9 of 9 Products</td>
<td>20%</td>
<td>$2,121</td>
<td>No</td>
</tr>
<tr>
<td>4</td>
<td>968319</td>
<td>3/2/2018</td>
<td>Human error</td>
<td>SIM (Argentina)</td>
<td>1 of 1 Products*</td>
<td>1 of 1 Products</td>
<td>22%</td>
<td>$1,280</td>
<td>No</td>
</tr>
<tr>
<td>5</td>
<td>961048</td>
<td>2/13/2018</td>
<td>Required approvals not obtained</td>
<td>Orthobone (Puerto Rico)</td>
<td>N/A</td>
<td>2 of 2 Products</td>
<td>84%</td>
<td>$3,556</td>
<td>No</td>
</tr>
<tr>
<td>6</td>
<td>949921</td>
<td>1/16/2018</td>
<td>Required approvals not obtained</td>
<td>SIM (Argentina)</td>
<td>1 of 18 Products*</td>
<td>18 of 18 Products</td>
<td>32%</td>
<td>$6,991</td>
<td>No</td>
</tr>
<tr>
<td>7</td>
<td>947697</td>
<td>1/10/2018</td>
<td>Required approvals not obtained</td>
<td>HTO (Italy)</td>
<td>2 of 2 Products*</td>
<td>2 of 2 Products</td>
<td>11%</td>
<td>$48</td>
<td>No</td>
</tr>
<tr>
<td>8</td>
<td>891764</td>
<td>4/5/2018</td>
<td>Required approvals not obtained</td>
<td>SIM (Argentina)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>9</td>
<td>959048</td>
<td>2/8/2018</td>
<td>Required approvals not obtained</td>
<td>MBA Incorporado (Spain)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>10</td>
<td>983926</td>
<td>4/11/2018</td>
<td>Price above contract</td>
<td>Implamed (US)</td>
<td>N/A</td>
<td>1 of 1 Products</td>
<td>-714%</td>
<td>$(11,985)</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Risk Assessments / Audit Programs
## Example: Risk Assessments

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>KRank</th>
<th>Potential Control Gaps</th>
<th>IA Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The company lacks a governance structure that allows for an effective and independent compliance organization.</td>
<td><img src="green" alt="" /></td>
<td>None</td>
<td>There are various compliance functions within the organization (Compliance, Legal, Quality Assurance, Regulatory, IT Security, Accounting/Finance, HR and Internal Audit). It is recommended that a regular forum be established for these compliance functions to share information and ensure there is neither duplication of effort nor gaps in compliance efforts.</td>
</tr>
<tr>
<td>The organization’s performance measurement and compensation structure does not incorporate compliance objectives.</td>
<td><img src="yellow" alt="" /></td>
<td>None</td>
<td>The company currently links completion of compliance-related training to compensation (e.g. bonuses and/or commissions could be withheld if training is not completed timely). Compliance should be involved in the process of developing / revising compensation plans for employees, in particular, sales employees / representatives. The company could consider other initiatives to engage the Sales organization in and encourage a level of accountability for the compliance process.</td>
</tr>
</tbody>
</table>
### Example: Risk Assessments

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>Risk Rank</th>
<th>Potential Control Gaps</th>
<th>IA Recommendation</th>
</tr>
</thead>
</table>
| Related policies are not in place, not centrally located and accessible, and/or not reviewed on an annual basis. | 3         | The company’s Procure-to-Pay policy has not been issued and currently does not reference the potential need for Compliance due diligence for high-risk vendors, contracts / suppliers.  
The FCPA-related Sales Representative Compensation policy has not been updated since 2012.                                                                                                                     | The Procure-to-Pay policy should:  
- include reference to Compliance policies and related processes  
- include requirements for obtaining multiple bids and/or market prices  
- be communicated / implemented  
The company’s Policy Committee should ensure that all needed policies are in place, communicated to responsible parties and reviewed, at a minimum, on an annual basis.                                                                                     |
| Related policies are not effectively communicated, consistently implemented or training is not provided to target individuals. | 4         | US employees and Contingent Workers are currently included in Global Anti-corruption training via a static list that was developed in 2015 and has not yet been updated.  
HR’s Recruitment policy (which requires criminal background checks) is only applicable in the US.  
It is difficult to obtain a complete population of all contingent workers as they are not all entered into Workday.                                                                                                           | Identify all high-risk employees and Contingent Workers (executives, international business development, M&A, Tax, Accounting & Finance, Procurement) who, based on their job function, could potentially interact with government officials, and, therefore, would require Anti-corruption training.  
Implement formal hiring policy consistent with US standard for international locations.  
In addition to compliance training, other touchpoints could enhance compliance awareness.                                                                                                           |
# Example: Risk Assessments

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>Risk Rank</th>
<th>Potential Control Gaps</th>
<th>IA Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are insufficient controls for ensuring that expenses are recorded</td>
<td></td>
<td>AP currently reviews invoices only for proper Delegation of Authority approval prior to</td>
<td>Establish a centralized control in Accounting for reviewing proper coding from business owners of invoices.</td>
</tr>
<tr>
<td>accurately in the company’s books/records.</td>
<td></td>
<td>payment. AP does not review for proper coding.</td>
<td>Add the following management reports for the Compliance organization’s regular review:</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>- General Ledger account activity for high risk accounts, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Charitable Contributions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- TPECS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Grants</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Expediting Fees</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Customs Fees</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Concur T&amp;E exception reports (see recommendations at T&amp;E section of the report)</td>
</tr>
<tr>
<td>There are insufficient feedback mechanisms in place to detect breaches in</td>
<td></td>
<td>There is a risk assessment process in place that determines which Distributor Audits are</td>
<td>Include high risk vendors / suppliers in the TPI in the risk assessment and, potentially, audit scope.</td>
</tr>
<tr>
<td>compliance to related policies.</td>
<td></td>
<td>are conducted each year. However, no other Third Party Intermediaries are currently</td>
<td>Conduct Compliance interviews onsite or phone (in addition to Due Diligence questionnaires) with prospective Distributors prior to engaging them (more proactive than conducting a post facto Distributor Audit).</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>audited.</td>
<td></td>
</tr>
</tbody>
</table>
How does the Risk Assessment tell us we should do in our Audit Program?
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 Process

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

Did the audit achieve its objectives?
Learning from Project Challenges

• It ensures everyone is aware of the challenges encountered and what was done to resolve them.

• If something is learned from a mistake or failed endeavor, then the effort put into the task is not entirely wasted.

• Participants can apply these lessons to future projects and be more successful.

• Lessons learned should be documented and included with final project documentation.

• Complete a post-mortem after every audit
Close Out Meetings

• **No surprises**
• Discuss Recommendations
• Ensure objectives have been achieved
• Timeline for management action items
• Next steps / follow up meeting?
• How else can Internal Audit help?
Post Audit Interviews

- Conduct after report issuance
- Not just a survey
- Discuss of what went right/wrong & what can be done better
- Share post-mortem with clients (to an extent)
Observations

• Draft Recommendations collaboratively with audit clients.
• Who Owns the Recommendation? Action Plan?
• Has the observation been vetted at all levels?
• Avoid “So What?” observations
• Workpapers should document all testing and testing exceptions to support all observations
Examples of Operational Audit Observations and Recommendations
Contract Pricing / Discount Exercise
Observations

• IA observed that there was not a Contract Pricing / Discount Policy in place
  – Outlining process for establishing / changing pricing on products
  – Requiring approval for discounts exceeding predefined tolerable threshold

• IA observed that system access to Pricing tables was not restricted (e.g. Sales employees has ability to change pricing)

• No management monitoring control to identify variances between original approved pricing versus actual pricing in system or invoiced
Recommendations

- IA recommended Policy be established and communicated to all stakeholders
  - Outlining process for establishing / changing pricing on products
  - Requiring approval for discounts exceeding predefined tolerable threshold
- IA recommended that access to system be restricted (sales personnel no longer had access)
- IA generated report of all variances between approved contract price and actual price
  - Variances that were not acceptable were changed
  - Variances that were acceptable required amendment to contract
  - All future changes to contract pricing had to be approved
Value Add

• Benefits include:
  – More economical sales transactions (governance over discounts and prices ensured profitable sales)
  – Less exceptions (between contract price and invoice price to research / resolve resulting in more efficient process)
  – IA recommended management exception report to identify future variances which resulted in effective achievement of dept. objectives
AR Credit / Collections Exercise
Observations

• IA observed that there was not a Credit Collections Policy in place; however:
  – Sales personnel were making side negotiations with customers without pre-approval
  – AR personnel finds out about changed terms (credit limits, payment terms, etc.) when they start to collect on receivables

• Amended terms were not communicated to AR function or required pre-approval
• Management monitoring control is a manual process and very time intensive
Recommendations

- IA recommended Policy be revised to require pre-approval if credit or payment terms are revised
- IA recommended that management monitoring control be automated (exception report generated from system on a recurring basis)
Value Add

- Benefits include:
  - Less write-offs / delinquent payments economical
  - Less more efficient process for identifying exceptions (automated vs manual)
  - Pre-approval of changes in terms reduced number of deviations from standard terms resulting in less research / resolution and more effective collection of receivables
7 C’s of Communication

1. Completeness
2. Conciseness
3. Consideration
4. Clarity
5. Concreteness
6. Courtesy
7. Correctness
Completeness

• Information communicated should convey all facts required by the audience.

• Examples, include:
  • 100 exceptions identified during audit versus
  • 100 exceptions (from a population of 1,000,000) identified during audit
Conciseness

• Conciseness means communicating in least possible words without compromising the other Cs.

• Examples, include:
  • Using powerpoint and bullets, graphs, etc. versus
  • Word document narratives, paragraphs
Conciseness - Example

Executive Summary

<table>
<thead>
<tr>
<th>Strengths</th>
</tr>
</thead>
<tbody>
<tr>
<td>• There are Emergency Response Plans in place (US and OUS)</td>
</tr>
<tr>
<td>• There are several IT Policies related to Disaster Recovery (US) as well as related IT Disaster Recovery / Resumption procedures in place (US and SrL).</td>
</tr>
<tr>
<td>• Several financial applications (including Workday, Xactly, Equity Edge CashPro) are cloud based and, therefore, would be easily accessible in the event of a disaster.</td>
</tr>
<tr>
<td>• The Company has business interruption insurance coverage ($96M for lost revenue and expenses / $40M contingent coverage on MTF)</td>
</tr>
</tbody>
</table>

| Challenges |
Consideration

- Consideration is communication that considers the audience’s viewpoints, background, etc.
- Examples, include:
  - Leader over audited area has recently assumed position versus a legacy leader
  - Audited area is newly created function versus mature function
Clarity

- Clarity in communication has following attributes:
  - Easy to understand
  - Clear message making use of appropriate words, terms

- Example:
  - “Control is ineffective” versus
  - “Control was not designed to ensure that all high payments, as defined by Policy” were routed to Compliance for further review”
Concreteness

• Concrete communication is specific and clear rather than fuzzy and general.
  • Supported by facts and figures
  • Concrete messages minimize potential for misinterpretation

• Example:
  • The number of exceptions identified during the audit represent 1% of the # of transactions in population and a total of $1,000 or 3% of the total Accounts Payable balance for 2017 globally.
Courtesy

• Courtesy in communication exhibits empathy and respect for the receiver.
  • Positive messaging
  • Unbiased and considers all viewpoints

• Example:
  • “The number of exceptions identified during the audit represent 1% of the # of transactions in population. This represent a decrease from 5% compared to prior year’s audit results.”
Correctness

- Correctness in communication ensures precision and accuracy of facts/figures

- Example:
  - “The number of exceptions identified during the audit represent 1% * of the # of transactions in population.
  - Validate all exceptions/observations at all levels.

* See Internal Audit workpapers for Accounts Payable 2017 Audit, test procedure AP1.20
Let’s Exercise
## 2017 SOX Interim Test Results

<table>
<thead>
<tr>
<th>Location</th>
<th>Key Controls</th>
<th>Ineffective</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (Business Process)</td>
<td>126</td>
<td>5</td>
<td>96%</td>
</tr>
<tr>
<td>US (ITGC)</td>
<td>19</td>
<td>2</td>
<td>89%</td>
</tr>
<tr>
<td>Italy</td>
<td>52</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>Brazil*</td>
<td>28</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>225</strong></td>
<td><strong>7</strong></td>
<td><strong>96%</strong></td>
</tr>
</tbody>
</table>

**What could make this information more meaningful (using 7 Cs)?**
### 2017 SOX Interim Test Results

<table>
<thead>
<tr>
<th>Location</th>
<th>2016 Key Controls</th>
<th>Ineffective</th>
<th>Effectiveness</th>
<th>Key Controls</th>
<th>Ineffective</th>
<th>Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>US (Business Process)</td>
<td>130</td>
<td>3</td>
<td>98%</td>
<td>126</td>
<td>5</td>
<td>96%</td>
</tr>
<tr>
<td>US (ITGC)</td>
<td>23</td>
<td>2</td>
<td>91%</td>
<td>19</td>
<td>2</td>
<td>89%</td>
</tr>
<tr>
<td>Italy</td>
<td>52</td>
<td>0</td>
<td>100%</td>
<td>52</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>Brazil*</td>
<td>42</td>
<td>2</td>
<td>95%</td>
<td>28</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>247</strong></td>
<td><strong>7</strong></td>
<td><strong>96%</strong></td>
<td><strong>225</strong></td>
<td><strong>7</strong></td>
<td><strong>96%</strong></td>
</tr>
</tbody>
</table>

*Brazil testing kicked off on 11/21/17.

** represents net of management remediation efforts (11 gross number of ineffective controls less 4 remediated)

- **Interim Testing Results**
  - No SDs or MWs to date
  - On track for deliverables for EY
Audit Reports

• Scope, Objectives, Coverage Period
• As a general rule: Audit Reports should be completed in the following quarter
• SME?

• Executive Summary
  – Strengths
  – Challenges
  – Trends
  – Insight
Emotional Words

- We/I/You
- Ambiguous Terms (Reasonable, Generally)
- Condescending Descriptive (Apparent, Obviously)
- Should
- Finding
- Adequate/Inadequate
- Fail
- Ensure
- Magical Terms (Appears, Found, Discovered)
- Fraud
- Opinion
Follow-Up

• What
• When
• What Level of Testing?

• Reporting results of Follow-Up
  – Quarterly to Audit Committee
  – Open/Past Due, Closed, Risk Accepted
# Follow-Up Matrix

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retest, Full Scope</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Walkthrough of New Process</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Inquiry/Observation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
EXAMPLES OF AUDIT REPORTS
Travel & Expenses Audit - Reporting
Cash/Non-Corp Card Reimbursements

Thousands

<table>
<thead>
<tr>
<th>Month</th>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Class of Service vs. Time Duration

First & Business Class
w/ 4 or more flights from Jul 17’ – Oct 17’

* 13 of 26 non-VP or Higher flew Business or Higher on <5 hr trips
Advance Travel Booking

2017

- 0-1 days
- 2-6 days
- 7-13 days
- 14-20 days
- >20 days

Jan Feb Mar Apr May Jun Jul Aug Sep Oct
Qtr1 Qtr2 Qtr3 Qtr4
**Spend by Expense Type**

Y-o-Y Top 80% of Spend Volume (by $)

### 2017 Top 15 Expense Submitters

<table>
<thead>
<tr>
<th>Card Holder</th>
<th>Q1 17’</th>
<th>Q2 17’</th>
<th>Q3 17’</th>
<th>Q4 17’</th>
<th>2017 Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>157,730</td>
<td>234,529</td>
<td>52,640</td>
<td>-</td>
<td>444,900</td>
</tr>
<tr>
<td></td>
<td>153,130</td>
<td>29,703</td>
<td>26,577</td>
<td>8,968</td>
<td>218,377</td>
</tr>
<tr>
<td></td>
<td>105,100</td>
<td>96,873</td>
<td>-</td>
<td>-</td>
<td>201,973</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>67,621</td>
<td>107,113</td>
<td>21,884</td>
<td>196,618</td>
</tr>
<tr>
<td></td>
<td>49,388</td>
<td>35,327</td>
<td>41,288</td>
<td>-</td>
<td>126,004</td>
</tr>
<tr>
<td></td>
<td>-</td>
<td>58,810</td>
<td>50,178</td>
<td>5,120</td>
<td>114,108</td>
</tr>
<tr>
<td></td>
<td>55,620</td>
<td>18,917</td>
<td>29,621</td>
<td>8,484</td>
<td>112,641</td>
</tr>
<tr>
<td></td>
<td>60,579</td>
<td>2,696</td>
<td>44,004</td>
<td>-</td>
<td>107,279</td>
</tr>
<tr>
<td></td>
<td>19,717</td>
<td>22,278</td>
<td>28,183</td>
<td>19,908</td>
<td>90,085</td>
</tr>
<tr>
<td></td>
<td>32,565</td>
<td>25,517</td>
<td>26,928</td>
<td>3,825</td>
<td>88,834</td>
</tr>
</tbody>
</table>
## BC/DR Readiness Assessment

### Detailed Observations – Governance

<table>
<thead>
<tr>
<th>Inherent Risks</th>
<th>Maturity Level</th>
<th>Potential Control Gaps</th>
<th>IA Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Company’s BC/DR initiative</td>
<td>There has not been an executive</td>
<td></td>
<td>It is recommended that an executive sponsor for the DR/BC initiative be identified. In</td>
</tr>
</tbody>
</table>
Follow Up Reporting

**Q4 2016 FCPA**
- Strengthen Distributor Monitoring
- Update FCPA Training
- Identify High Risk Vendors Q3
- Coding Controls Q3
- Contracts Policy/Database TBD

**Q1 2017 BC/DR**
- Committee Formed
- BC Policy Q4
- Crisis Mgmt. Plan Q1 2018
- Plan Testing Q3 2018
- Training Q: 2018
- BIA Q1 2018
- BCM/ITDR Plan Q2 2018

**Q1 2017 T&E**
- Receipts Required > $75
- Management Reporting
- Updated T&E Policy Q4
- Concur Controls Q4
- Concur Travel OUS TBD
- Eliminate Ghost Cards
- DOA Automation Q4

Complete
Open
Risk Accepted
HOW BEST CAN IA HELP AN ORGANIZATION ACHIEVE IT’S OBJECTIVES?
Why IA should be engaged in ERM

• By helping executive management address their risks:
  – IA remains relevant
  – IA is focused on the top risks
  – IA is addressing what keeps management up at night
  – IA’s efforts are aligned with organization’s strategic objectives
  – IA is adding value
Risk Assessments

• Enterprise Risk Assessment
  – Identify/prioritize risks that could impact an organization’s strategic objectives
  – Drives IA Plan

• Functional Risk Assessments
  – Identify/prioritize risks that could impact a function’s objectives (which support an organization’s objectives)
  – Drives audit program
ERM:

IDENTIFYING AND MANAGING ENTERPRISE-WIDE RISKS
How are We Assessing Risk?

• How many are performing a formal annual risk assessment?
• How many are performing a formal engagement-level risk assessment?
• What is the process?
  – Numerical/Ratings?
  – Interviews?
  – Questionnaires?
  – Surveys?
How can we manage risks effectively?
An effective ERM process

• Ownership – It is owned by Senior Management

• Relevant – it is updated and is aligned with the organization’s strategic objectives

• Measurable – key indicators are used to measure effectiveness

• Monitored – there is a governance process to:
  – Evaluate results
  – Hold Risk Owners accountable
  – Identify and execute action items

• Evolving – it adapts with the organization as it changes
ERM Roles / Responsibilities

• Senior Management should own the ERM process.

• Risk Owners are responsible for addressing their risks and reporting their progress

• CEO should support process and receive ERM progress reports

• BoD should ensure risk appetite set by management is not too aggressive

• Employees should understand what their role is in contributing to ERM
Align ERM with Strategic Objectives

• Start with the Corporate level goals/objectives

• Identify the risks that could impede achieving those strategic goals/objectives

• Identify risk owners and action items to address those risks

• Establish target dates that align with timeline of the strategic goals/objectives

• Update ERM process
Measurable = Managed

• Establish target performance results with Key Performance Indicators (KPIs)

• Establish Key Risk Indicators (KRI) to allow for company to proactively gauge prior to experiencing undesirable results

• KPIs and KRI should align with organization’s risk appetite

• Monitor KPIs and KRI to determine if:
  – Management’s actions are effectively mitigating risk
  – Additional or different action need to be taken to better address risk
  – Risk environment is shifting (increasing or decreasing)
  – KPIs and/or KRI need to be adjusted
Monitored

- ERM Dashboards should be used to report status
- Risk Owners complete Dashboard for their risks
- Key indicators (KPIs, KRIs) should be monitored on a regular basis
- Assessment of progress against those key indicators should be reported to ERM Committee
- Accountability can be established for each Risk Owner to stay within acceptable KPI range
- ERM updates should be reported to BoD as part of governance
Evolving

• Keep it Simple! This is recommended for first year ERM implementation, for small companies and/or for senior management team with limited experience with ERM.

• The more complicated the business or more mature the organization, the more robust the ERM process and reporting can become.

• The more flat the organization, the less number of layers of management is needed in the ERM process and vice versa.

• Solicit feedback from participants in ERM process to determine what can be improved and how the process can be more effective (what is working and what is not working).

• Determine if company’s risk appetite should be adjusted.

• Benchmark company’s ERM process to other organizations (similar in size, industry, etc.).
Reporting

• **Strategic Plan:** Corporate goals and objectives to be achieved for the year

• **Risk:** Top risks identified that could impede achieving the corporate plan

• **Risk Owner:** Individual responsible for each risk (both primary and supporting key players)

• **Action Items:** Actions planned to be completed (within 1 year) to address/remediate risks

• **KPIs / Monitoring Controls:** Metrics or tools used for management to monitor and ensure risk stays within pre-defined acceptable thresholds

• **Status:** Based upon progress of achieving Action Items and KPIs, assess progress:
  - Green: on track in successfully completing action items according to plan
  - Yellow: not on track but there is a plan in place to resolve issues
  - Red: delay and challenges are significant, resolution of issues is critical and urgent
ERM and IA

- IA can use ERM results to better perform risk assessments.

- IA can provide assurance of ERM process for executive management.

- IA can independently/objectively assess progress of ERM action items.

- Likelihood / Impact used in ERM can be used in IA assessments of findings.

- IA’s involvement in ERM will allow IA to better understand business risks.

- IA results can help ERM identify emerging risk trends and vice versa.

- IA’s focus on Company’s ERM risks will make IA more relevant.
ERM – Success Factors

• Lack of executive support and/or lack of management ownership.

• Progress is not measurable.

• KPIs are “outcome” KPIs (lagging versus leading indicators).

• Data / information reported in ERM initiative is not accurate or timely.

• Using a “silo” mentality (risks do not exist in a vacuum, they interact with other risks).

• ERM is a separate project rather than embedded in business.

• ERM process, reporting tools, etc. is too complex and/or cumbersome.

• Emerging risks are not identified.
Summary
Questions?
Linh Truong’s contact info:

linhtruong@orthofix.com

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