Internal Audit and SOX Best Practices

ERIC LISTER

RISK ADVISORY SERVICES

whitleypenn

Agenda

Internal Audit Procedures and Examples

SOX 404 Procedures and Examples

Questions and Discussion

Overview of IA Best Practices

- Planning
- Fieldwork
- Reporting
- Post Audit

whitleypenn

IA Dallas

Audit Timelines and Procedures

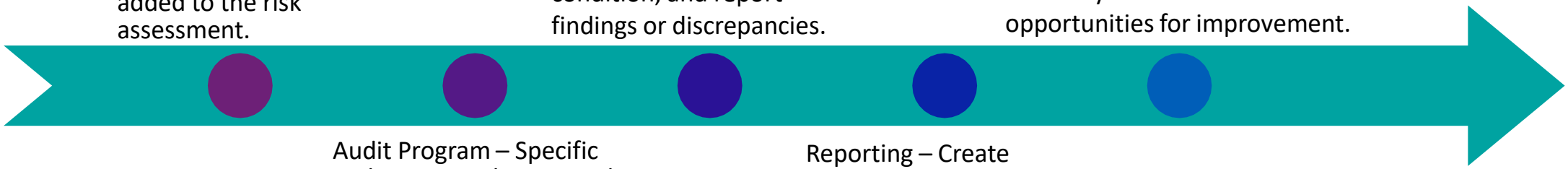
Planning – Audit Assignment and objectives are established here in depth after being added to the risk assessment.

Audit Program – Specific audit steps and personnel involved are established here, which leads to more efficient testing of procedures and samples.

Fieldwork – Create flowcharts, select and test samples, compare to ideal condition, and report findings or discrepancies.

Reporting – Create recommendations and remediation plans for any issues found with a timeline for correction.

Post Audit – Follow-up on remediation actions are reviewed and quality surveys are sent to process owners to obtain an idea of the value added by internal audit and opportunities for improvement.



Risk Assessment and Audit Plan

Establish Annual Audit Plan:

- Done by the CAE and senior management.

- Risk-based approach based on auditable items in the company.

- External and internal risks are considered: Environmental, regulations, turnover, segregation of duties.

- Best use of audit teams time is considered.

- Various types of audits should be introduced.

- Should be approved by the board of directors.

- Should present to process owners to provide reasonable amount of time to prepare.

Planning

Establish Audit Assignment and Objective:

- Does the objective meet the organization's goals?

- Will the testing procedures reach the most effective conclusion on performance?

- Do we have adequate knowledge and resources?

- Gather and review policies and procedures related to the specific activity.

- Send engagement memo.

- Send preliminary survey and questionnaires for background information.

- Develop audit program

October 22, 2018

Joe Smith
IIA Conference Attendee
Dallas Institute of Internal Auditors
P.O. Box 261747
Plano, TX 75026

Dear Joe:

Subject: Dallas IIA Conference Audit

The Generic Audit Group will soon be ready to begin the 2018 audit of the IIA Dallas Super conference registration process. The proposed objective and scope for this review are attached for your consideration.

Eric Lister will lead the audit and John Doe will assist. At this time, we anticipate that on-site fieldwork will take place October 22, 2018. If necessary, the audit team will make a 1 day trip to Dallas prior to the commencement of fieldwork to perform the audit planning. We will work with you to determine the availability of the key IIA resources and tailor our planning and audit schedule around that timeframe.

Prepared By:	
Date:	

XXX Audit
SUMMARY OF INTERVIEW WITH XXX

Purpose: To ensure that the appropriate interviews are performed to obtain an initial understanding and adequately complete the Audit Planning Guide to enable a properly focused audit.

Interviewees (Title, Department/Region):	
Date of Interview:	
Individuals conducting interview:	

Topics/Questions to Cover:

Interview Notes (examples: major process steps, departments involved in the process, reports used / reviewed, manual & system control points, internal control weaknesses, etc.):

Follow Up Items:

Conclusion (risks identified, out of scope areas, etc.):

Objective: To aide Internal Audit in appropriately planning the audit resources and testing strategies we would like to request the following information to assist our understanding of the IIA Super conference registration process and activities as well as your area of management.
Audit Name: Dallas Super Conference Registration Process
Date: October 22, 2018
Interviewee(s): Joe Smith
Interviewer(s): Eric Lister
1. Provide brief details of the following:
a. Roles / Responsibilities:
i. Personnel involved in the process
ii. Key Reporting Relationships

Audit Program

Establish Audit Testing Procedures:

- Restate the audit objective to ensure clarity and focus

- Establish the time period of the audit

- Populate initial risks to address based on preliminary surveys, interviews, and risk assessments.

- Document controls in place and how they should be operating.

- Describe the tests that will be performed to validate the operating effectiveness.

- Fraud Considerations

- Testing Reference to identify location of testing phase documents.

Audit Program Example

Dallas IIA Super Conference Registration				
Time Period of Audit: October 22, 2018				
Objective: To audit registration process of the Super Conference and to ensure proper accounting procedures were followed.				
Risk Ranking	**Risks**	**Controls**	**Testing Procedures**	**Workpaper Reference**
High	**Missing Registration Funds**	System Access Controls and balances	Review for approval on refund requests.	

Fieldwork

Testing and Documentation Stage:

- Evidence is created from tests or questions with process owners.

- Request evidence and compare to established criteria obtained during planning.

- Support conclusions (pass/fail) reached.

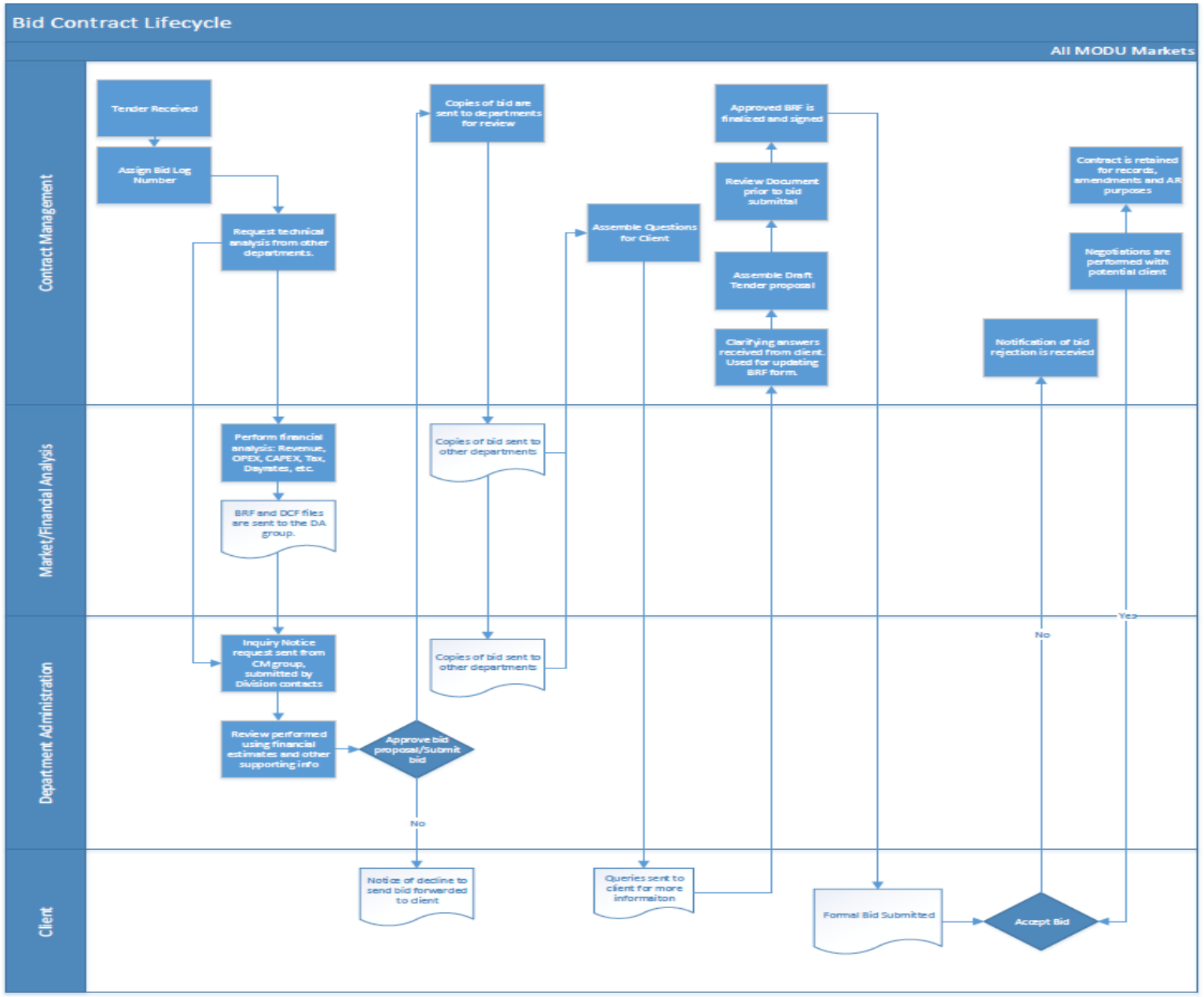
- Create flowcharts, conduct interviews, meetings, etc.

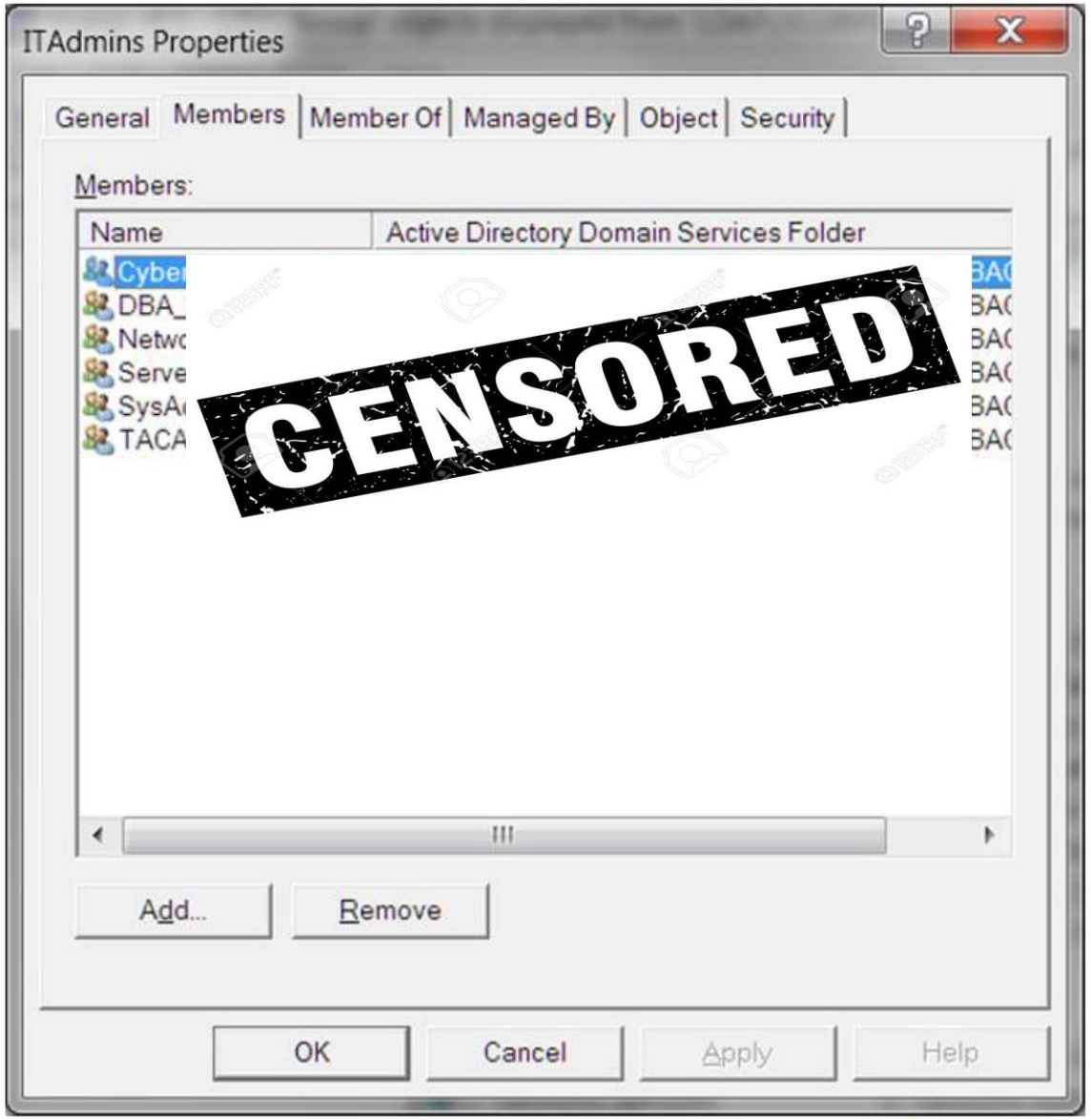
- Document method of selecting samples (judgmental or random)

- Document the test procedure, area of work paper reviewed, and identifying information.

- Establish recommendation and remediation needed in order to correct any issues.

- Discuss issues with management in order for them to accept or address the risk identified.


Bid Contract Lifecycle
All MODU Markets
Contract Management
Market/Financial Analysis
Department Administration
Client
Tender Received
Assign Bid Log Number
Request technical analysis from other departments.
Copies of bid are sent to departments for review
Assemble Questions for Client
Approved BRF is finalized and signed
Review Document prior to bid submittal
Assemble Draft Tender proposal
Clarifying answers received from client. Used for updating BRF form.
Contract is retained for records, amendments and AR purposes
Negotiations are performed with potential client
Notification of bid rejection is recevied
Perform financial analysis: Revenue, OPEX, CAPEX, Tax, Daystes, etc.
BRF and DCF files are sent to the DA group.
Copies of bid sent to other departments
Copies of bid sent to other departments
Inquiry Notice request sent from CM group, submitted by Division contacts
Review performed using financial estimates and other supporting info
Approve bid proposal/Submit bid
No
Yes
No
Notice of decline to send bid forwarded to client
Queries sent to client for more informaiton
Formal Bid Submitted
Accept Bid


ITAdmins Properties
General
Members
Member Of
Managed By
Object
Security
Members:
Name
Active Directory Domain Services Folder
CENSORED
Add...
Remove
OK
Cancel
Apply
Help

2018 Expenses - Message (HTML)

FILE | MESSAGE

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | IM | More | Presentations | Team Email | Reply & Delete | To Manager | Done | Create New | Move | Rules | Actions | Mark Unread | Categorize | Follow Up | Translate | Find | Related | Select | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

Tue 10/9/2018 4:34 PM

Eric Lister

2018 Expenses

To Eric Lister

Retention Policy Firm Policy (1 year) Expires 10/9/2019

Bing Maps + Get more apps

I approve.

Eric Lister, MBA, CFE
Risk Advisory – Senior Manager

Eric.Lister@Whitleypenn.com
713-386-1179 Direct
615-828-8905 Cell

DATE	TRANSACTION	AMOUNT
01-11	DIGITAL DEPOSIT	17,466.68
01-18	DIGITAL DEPOSIT	828.97
01-18	DIGITAL DEPOSIT	1,218.01
01-18	DIGITAL DEPOSIT	1,549.23
01-18	DIGITAL DEPOSIT	21,923.12
01-18	DIGITAL DEPOSIT	358,460.35
01-22	DIGITAL DEPOSIT	141,217.49
01-25	DIGITAL DEPOSIT	8,297.05
01-25	DIGITAL DEPOSIT	212,559.95
01-30	DIGITAL DEPOSIT	511,810.02
01-31	DIGITAL DEPOSIT	229.91
01-31	DIGI	
01-31	DIGI	
01-31	DIGITAL DEPOSIT	26,675.15

Rev.CP3: Attribute B: Sample 30

Audit:	Dallas Superconference Registration Audit
Objective:	To determine whether processes were followed correctly.
Procedures:	How did you do it?
Testwork Performed:	What did you do?
Results:	Were there any issues?

			Audit Tests					
Sample Number	Sample Name	Descriptive Information	Audit Test	Audit Test	Audit Test	Result	Tickmark	Workpaper Reference

Tickmark Legend (Note Exception or No Exception)	
[a]	Explain the issue noted.
✓	No exceptions noted in performance of test.

Reporting

Communicate the findings of the audit:

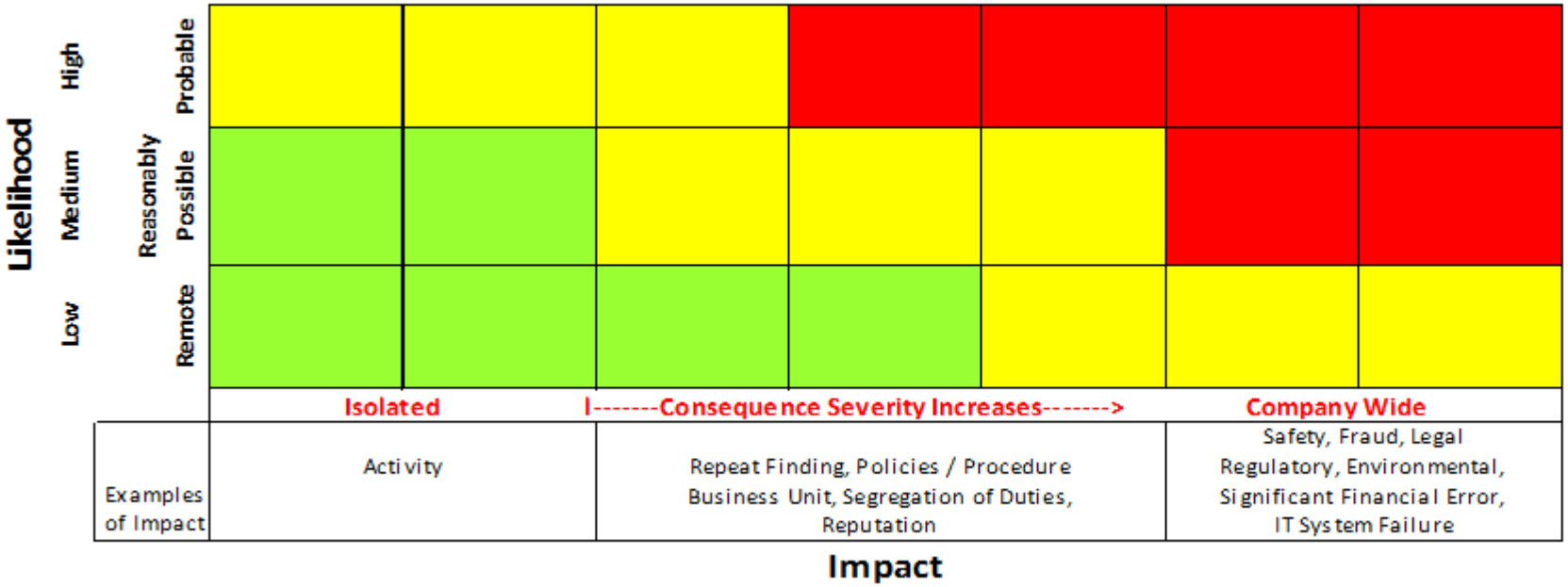
- Provide documented communication to process owners.

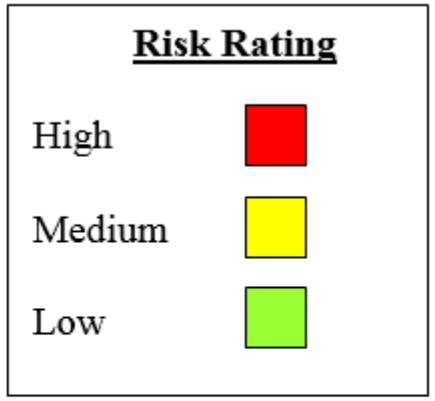
- Provide operating management with assessments and/or expected corrective action.

- Provides Internal Audit Activity a way to demonstrate their value to entity.

- Provides auditor and management with follow-up actions if needed and a timeline for expected remediation.

Reporting


Likelihood
High
Medium
Low
Reasonably Possible
Probable
Remote
Isolated
I-------Consequence Severity Increases------->
Company Wide
Examples of Impact
Activity
Repeat Finding, Policies / Procedure Business Unit, Segregation of Duties, Reputation
Safety, Fraud, Legal Regulatory, Environmental, Significant Financial Error, IT System Failure
Impact


Risk Rating
High
Medium
Low

Reporting

Summary of Audit Results:

<Title of Observation>

- XXX

Management Action Plan: XXX
Risk Rating: XXX Management Corrective Action Expected Completion Date: XX/XX/20XX

Post-Audit

Communicate the findings of the audit:

- Follow up on the corrective action needed to be taken by management outlined in the report.

- Complete Audit Checklist to ensure all procedures outlined previously have been completed and documented.

- Finalize presentations to BOD members.

- Send survey to managers and process owners to gain an understanding of the value and effectiveness of the internal audit activity.

Post-Audit

whitleypenn

INTERNAL AUDIT CUSTOMER SURVEY

Please provide some information regarding our previous audit over the Dallas IIA registration process to ensure continuous improvement of our internal audit function and provide future auditees with a better service.

Audit Name: Dallas IIA Registration Audit	**Date: 10/22/2018**
Lead Auditor: Eric Lister	**Report Date: 10/22/2018**

PROFESSSIONAL PROFICIENCY	**Excellent - Poor**
Technical skills, competency, and knowledge of auditor(s)	5 4 3 2 1
Professionalism and courtesy of auditor(s)	5 4 3 2 1
Degree to which audit staff provided a clear indication of the planned procedures, objectives and scope of the audit	5 4 3 2 1
Emphasis on minimal disruption to operations and reasonableness of requests for information	5 4 3 2 1

Overview of SOX Best Practices

- Population
- Sampling
- Testing
- Reporting

whitleypenn

IIA Dallas

What Are Internal Controls?

- Any action taken by management, the board, and other parties to manage risk and increase likelihood that established objectives and goals will be achieved.

- Related to financial reporting and corporate governance

- The control wording should list the “ideal state” of the process being tested.

- Identify roles and responsibility of the people in the process.

What Are Internal Controls?

Who Is Responsible?

- Internal Auditors are not responsible for establishing or maintaining internal controls.

- Must examine the adequacy and effectiveness of the internal controls.

- Board, management, employees

- Make Recommendations where improvements to design or application are needed.

- Contribute to the effectiveness of the control environment.

What Is The Difference?

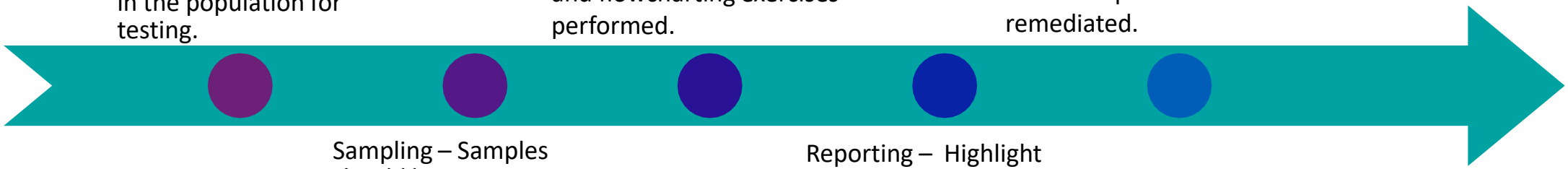
Audit

- Less frequent, more formalized
- Larger scale, scope, and sample
- System or program based
- Structured and allows for further investigation and analysis
- Risk-based

Compliance

- Frequent, repeating
- Scope and scale oftentimes do not change
- Large number of inspectors per year
- More rigid and checklist based

SOX Timelines and Procedures



Population – based on the company or entity's fiscal year. The entire 12 months should be considered in the population for testing.

Sampling – Samples should be representative of the population and are determined based on daily, weekly, monthly, annual action.

Testing – Test based on the criteria established in walkthroughs, narratives, and flowcharting exercises performed.

Reporting – Highlight any issues of noncompliance and report to process owners for remediation.

Testing – Test second half of population and document the remediation actions taken by process owners and determine if noncompliance has been remediated.

Population and Sampling

- Ensure population is accurate and complete. Provided by entity versus pulled by Internal Audit?

- Sampling should be representative of the process being audited.

- Coordinate with external auditors on sampling to reduce burden on the process owners.

Reperformance Sample Sizes					The proposed sampling distribution across entities and quarters, subject to modification.			
Frequency of Control	Assumed Population of Control Occurrences	Min. No. of Items to Test*			Phase I Interim (July - Sept)		Phase II Rollforward (Oct - Nov)	Phase IV Annual / YE (Jan'16 - Feb'16)
		Low	Mod	High	Q1	Q2	Q3	Q4
Annual	1	1						1
Semi-Annual	2	1						1
Quarterly	4	2			1			1
Monthly	12	2	3	5	1 / 1 / 3		0 / 1 / 1	1 / 1 / 1
Weekly	52	5	10	15	2 / 5 / 9		1 / 4 / 3	1 / 1 / 2
Daily	250	20	30	40	9 / 20 / 25		8 / 7 / 10	3 / 3 / 5
Multiple times per day	Over 250	25	45	60	11 / 30 / 40		9 / 10 / 10	5 / 5 / 10

Testing

Testing and Documentation Stage:

- Evidence is created from documents obtained by systems or provided by process owners.

- Verify accuracy and authenticity when receiving documents second-hand.

- Support conclusions (pass/fail) reached.

- Provide remediation action if controls are to fail.

- During the initial testing phase, allow enough time for process owners to remediate during a second testing window.

Reporting

Communicate the findings of the testing:

- Provide documented communication to process owners, CEO, CFO, and board of directors.

- Identify whether issues and/or control failures are control deficiencies, significant deficiencies, or material weaknesses.

- Coordinate with external auditors on issues, risk rating, and impact to the organization.

- Issue final memo documenting control failures, remediated items, open issues, risk level, and plan of action.

whitleypenn

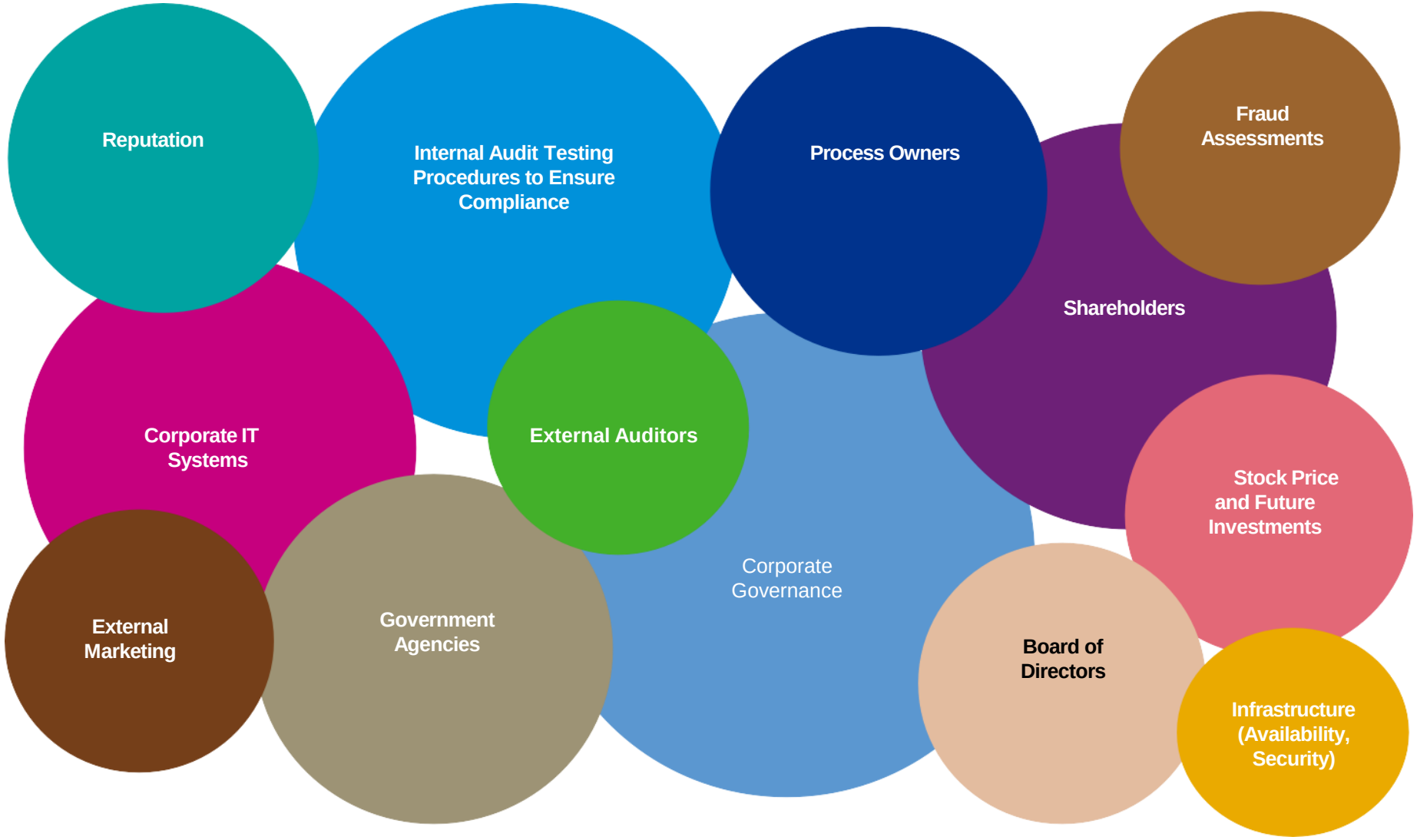
SOX Best Practices

Area	Best Practice
Planning and Orientation	Interviews with management and internal process experts should see SOX testers gain an understanding of the business practices, policies and procedures, and departmental processes.
Governance Assessment	Senior management and BOD members should be interviewed to gain an understanding of their commitment to ethics, anti-fraud policies, their management philosophy, and corporate tone.
Documentation	Narratives and flowcharts should be established documenting key processes with high complexity. Narratives provide a written description of people and systems involved and can identify weak areas.
Control Matrix	A complete matrix of internal controls should be maintained to identify changes, areas tested, process owners, document requests, and any noncompliance.
Remediation	For control issues, a remediation plan of action should be established quickly in order for the organization and process owners to have a chance to conform effectively.

SOX Best Practices

Area	Best Practice
Test Procedures	Procedures and types of tests should be established prior to performance to ensure full understanding of all involved. Tests should also be complete and test all areas of the control.
Retesting Remediation	Select a second sample of items to be tested for any control that did not operate effectively in the initial testing phase. After agreeing with process owners, the new samples are tested similarly to the originals.

whitleypenn



SOX Takeaways: Convincing Doubters

What is the Return on Investment?	— Know your customers and their requirements — Coordinate with external auditors for reliance on controls to reduce burden — Maintains high assurance that controls and governance activities are operating effectively — Become an efficient and valuable part of the organization by incorporating SOX into audits.
Why do we need it?	— Know your compliance requirements and the types of regulations that run your business — Addresses risks beyond just a financial impact — Know when to “push back”
What does it involve?	— Communication, Communication, Communication — Define the scope of the system or process including infrastructure, software, people, procedures and data — Constant verification of changes — Cooperation between the entire entity to ensure effective controls and remediation of ineffective controls — Know when to “push back”

whitleypenn

Questions?