Report Writing and Communicating to the Audit Committee

*Presented to the Topeka IIA*

December 4, 2018
AGENDA

03 Part 1 – Internal Audit Reports
   Executive Summary
   Issue Write Up
   The Recommendation
   Overall Audit Rating

37 Part 2 – Communicating to the Audit Committee
   Dashboard Samples
   Risk Assessment Results
   Internal Audit Calendar and Plan
   Activity Summary
   Issue Follow Up Status
   SOX Program Overview and Results
PART 1 – INTERNAL AUDIT REPORTS
Internal Audit (IA) reporting may be the biggest challenge in the audit process.

An audit report presents results of an examination or review within the organization and is considered to be the core deliverable of audit services.

Each organization has unique reporting practices and expectations that affect the format, frequency and depth of their communications.

**Key Considerations:**

- Poorly communicated results may completely detract from what may be critical information for senior management and the board.
- The audit report is often the main, routine vehicle through which senior management understands the value that internal audit delivers.
- Well-organized and clearly communicated results are a key indicator of competency and professionalism.
- Despite this, the reporting phase is typically under-budgeted and reporting templates are stale.
AUDIT REPORTING ISSUES

Some typical reporting issues are:

- Ineffective communication of results
- Delays in writing draft report
- Management does not accept findings
- Quality control during editing process
- Delays in receiving management responses
AUDIT REPORTING CHALLENGES

Lengthy cycle times

Reports must be factually correct and issued timely

Constant complaint – audits take too long

**Consequences of Lengthy Audit Cycles**

- Audit results are not timely
- Stakeholders dissatisfaction
- Inefficient use of internal audit’s time
APPLICABLE IIA STANDARDS

**Reporting to Senior Management and the Board**

The chief audit executive must report periodically to senior management and the board on the internal audit activity’s purpose, authority, responsibility, and performance relative to its plan. Reporting must also include significant risk exposures and control issues, including fraud risks, governance issues, and other matters needed or requested by senior management and the board.

**Criteria for Communicating**

Communications must include the engagement’s objectives and scope as well as applicable conclusions, recommendations, and actions plans.

**Quality of Communications**

Communications must be accurate, objective, clear, concise, constructive, complete, and timely.

**Disseminating Results**

The chief audit executive must communicate results to the appropriate parties.

**Overall Opinions**

When an overall opinion is issued, it must take into account the expectations of senior management, the board, and other stakeholders and must be supported by sufficient, reliable, relevant, and useful information.
# TYPICAL ELEMENTS IN AN INTERNAL AUDIT REPORT

<table>
<thead>
<tr>
<th>1</th>
<th>Title Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Table of Contents</td>
</tr>
<tr>
<td>3</td>
<td>Executive Summary</td>
</tr>
<tr>
<td></td>
<td>• Report rating</td>
</tr>
<tr>
<td></td>
<td>• Audit issues</td>
</tr>
<tr>
<td></td>
<td>• Status of management remediation planning</td>
</tr>
<tr>
<td>4</td>
<td>Audit Objectives and Scope</td>
</tr>
<tr>
<td>5</td>
<td>Business Context</td>
</tr>
<tr>
<td>6</td>
<td>Audit Issues</td>
</tr>
<tr>
<td></td>
<td>• Issue owner</td>
</tr>
<tr>
<td></td>
<td>• Issue severity</td>
</tr>
<tr>
<td></td>
<td>• Issue &amp; root cause</td>
</tr>
<tr>
<td></td>
<td>• Risk</td>
</tr>
<tr>
<td></td>
<td>• Supporting observations</td>
</tr>
<tr>
<td></td>
<td>• Recommendation</td>
</tr>
<tr>
<td></td>
<td>• Management agreement and Due Date</td>
</tr>
<tr>
<td>7</td>
<td>Appendices</td>
</tr>
</tbody>
</table>
DEVELOPING CONTENT OF AN AUDIT REPORT

- Begin consideration for the audit report early on in the audit process. Consider things like data elements, risk coverage, and the importance and craft the messages during the planning phase.

- Create a tracking log at the beginning of an engagement to note potential findings identified during fieldwork.

- Develop a tentative conclusion based on data reviewed/tested.

- Review potential findings with process owners as they’re identified during fieldwork and fresh in the auditor/auditee’s mind – do not wait until the audit closing to validate findings.

- Review the final list of findings with management prior to the closing meeting.

- Audit report communicates to managers of the audited entity (for them to act) and to upper level management (for them to be informed) of audit conclusions.
FINAL REPORT VALIDATION

The process for Final Report Validation is as follows:

**Proofread and spell check draft report**

- The draft should go through 1-2 levels of internal review before it is sent to the auditees.

**Send the draft report to the auditees**

- Allow sufficient time for the draft report to be reviewed by the auditees prior to the closing meeting.

**Obtain validation from managers**

- Comments about observations and recommendations
- Specify for each recommendation’s deadline, person responsible for setting up and delivering action plan.

**Final report**

- Agree on final wording
- Issue and distribute (make sure distribution list is adequate)

This process is critical. This is usually when delays occur.
EXECUTIVE SUMMARY
EXECUTIVE SUMMARY

A strong executive summary will assist the reader by answering the following questions.

- What were the scope and objectives of the audit?
- Why was the audit relevant?
- What were the significant findings?
- What is being done to remediate any significant findings?

Consider using Appendices for anything else.
1. Executive Summary

Background

ABC Co’s generic program was setup to drive sales across product types and to address discounted pricing from competitors. Approximately X% of customers (approximately XX% of all customers) received generics in 2014, with the majority issued on either an annual or quarterly basis in the form of a credit memo. Generics are typically awarded based on contracted volume/product order matrices.

The value of generics increased X% between December 31, 2013 ($Xm) and December 31, 2014 ($Xm). This increase was primarily driven by the fact that 2014 was the first year that the ABC contract was in place for the entire year.

There are two types of generics on customer sales:

1. Administration Fees, and
2. Direct Generic Agreements with direct customers or ABC members.

Sales Operations manually calculates Administration Fees paid to XX different ABCs by pulling sales information from ERP and performing calculations via spreadsheets. Accounting manually calculates Direct Generic generics by querying an Access database of customer sales figures and performing calculations in separate spreadsheets for each generic type.

Scope and Objectives

The scope of the review will include a review of processes and controls that are in place within the generic process. The objectives of the review are:

- Objective 1
- Objective 2
- Objective 3

Summary of Findings

The table below includes a summary of key findings.

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Findings</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>The generic calculation process is primarily manual, increasing the risk of errors as the program expands.</td>
<td>Medium</td>
</tr>
<tr>
<td>P2</td>
<td>Direct generic spreadsheet and sales database can be modified without detection, impacting generic calculations.</td>
<td>Medium</td>
</tr>
<tr>
<td>P3</td>
<td>Generic calculation process is not adequately documented, which limits the ability to transition key activities to other personnel.</td>
<td>Medium</td>
</tr>
<tr>
<td>P4</td>
<td>Changes to certain fields in ERP, which may impact generic calculations, are not monitored.</td>
<td>Medium</td>
</tr>
<tr>
<td>P5</td>
<td>Generic credits remain unclaimed for extended periods of time, and have no expiration dates.</td>
<td>Low</td>
</tr>
<tr>
<td>P6</td>
<td>Management reporting on generics is ad-hoc and informal.</td>
<td>Improvement</td>
</tr>
</tbody>
</table>

Positive Aspects of Internal Control

The following positive aspects of internal control were identified during the review:

- **Pricing**: Negotiated customer pricing and generic terms that vary from the predetermined ABC Co customer contract template must be reviewed by a Pricing Administration Committee, made up of Sales Operations and Finance personnel.
- **ABC Renewals**: During the renegotiation process with ABCs, the VP of Sales Operations and Customer Service coordinates with executive management to align the contract negotiation with company goals.
EXECUTIVE SUMMARY – SAMPLE 1 (CONT.)

1. Executive Summary

Process Maturity Assessment
The chart below shows the current process maturity for each element of infrastructure from 1 (Ad-hoc) to 5 (Optimized) and the maturity after the implementation of the management actions identified in this report.

<table>
<thead>
<tr>
<th>Infrastructure Element</th>
<th>Current State</th>
<th>Related Actions</th>
<th>Future State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Policies</td>
<td>3. Defined</td>
<td>N/A</td>
<td>3. Defined</td>
</tr>
<tr>
<td>Business Processes</td>
<td>2. Repeatable</td>
<td>A3.1, A3.2</td>
<td>3. Defined</td>
</tr>
<tr>
<td>People &amp; Organization</td>
<td>2. Repeatable</td>
<td>A3.1, A3.2</td>
<td>3. Defined</td>
</tr>
<tr>
<td>Management Reports</td>
<td>1. Ad-hoc</td>
<td>A4.1, A5.1</td>
<td>3. Defined</td>
</tr>
<tr>
<td>Methodologies</td>
<td>2. Repeatable</td>
<td>A1.1, A5.1, A5.2</td>
<td>3. Defined</td>
</tr>
<tr>
<td>Systems &amp; Data</td>
<td>1. Ad-hoc</td>
<td>A2.1</td>
<td>2. Repeatable</td>
</tr>
</tbody>
</table>

Action Plan Analysis
Future state process maturity will be achieved upon the completion of the related management actions as per the table below.

Summary of Actions
<table>
<thead>
<tr>
<th>Ref</th>
<th>Action Plan</th>
<th>Owner, Title</th>
<th>Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1.1</td>
<td>Streamline the generic plans offered to direct customers</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A2.1</td>
<td>Restrict access to the Access database and calculation spreadsheets</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A3.1</td>
<td>Document the direct generic calculation process</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A3.2</td>
<td>Document the administration fee calculation process</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A4.1</td>
<td>Review changes to customer data that affect generics in ERP</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A5.1</td>
<td>Where there are no legal restrictions, incorporate a generic credit expiration date into future contract negotiations</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A5.2</td>
<td>Implement alternative credit repayment methods</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
<tr>
<td>A6.1</td>
<td>Develop key metrics to evaluate ABC Co's generic program</td>
<td>Name, Title</td>
<td>TBD</td>
</tr>
</tbody>
</table>

Refer to Appendix C for a detailed processes maturity assessment and Appendix D for details of the Capability Maturity Model against which the process has been assessed.
Executive Summary

In August 20XX, XYZ moved from PayChex to ADP as the primary provider of outsourced applications that support the Payroll and HR processes. This review assessed pre- and post-implementation activities, including process and controls points that are in operation today. Key objectives of the audit included: assessing the process to define and test the implementation of business requirements, assessing application security, and evaluating post go-live support processes.

The conversion to ADP was managed by the HR/Payroll department and did not involve IT resources from a management, tactical, or consultative perspective. HR/Payroll contracted Project Management experience and relied heavily on ADP’s methodology to complete the conversion. Primarily because IT personnel were not involved, adherence to XYZ IT policies and processes did not occur, resulting in issues related to SOX compliance and overall good practice for a conversion of this size and scope. While many of the processes used to manage the conversion effort appeared to have been appropriate and well executed, sufficient documentation was not always available to verify key control practices were utilized. Also, it should be noted that significant turnover in key HR/Payroll personnel was incurred at key points of the project, further highlighting the need for a well-documented and organized set of project documentation for future reference. Despite significant turnover and an aggressive timeline, HR/Payroll personnel performed many key activities diligently to help ensure critical functionality was in place to support important processes such as Payroll.

Eight observations noted from the ADP Post-Implementation Audit are summarized below. Recommendations and management action plans are detailed in the Control Improvement Action Plan section of this report starting on Page 4.

Observations

1. Service Level Agreements not defined and incorporated into ADP contract
2. Business case and project charter not formally documented
3. Business requirements definitions for reporting not consistently communicated to ADP
4. In-house understanding of ADP security structure does not appear to be adequate
5. Shared user accounts exist in the ADP system with Supervisor access
6. Read-only access not administered properly
7. Lack of monitoring around accounts with Supervisor access
8. Testing approach and test plan not defined and formally documented

Priority Risk Map

- Observations in the top right quadrant are given high priority.
- Observations in the bottom left quadrant are given low priority.
- Observations in the top left and bottom right quadrants are given medium priority.
EXECUTIVE SUMMARY – EXAMPLE 3

CLOUD SECURITY

Distribution: Employee A, Employee B, Employee C, Employee D, Employee E, Employee F, Law Department, Regulatory, Compliance, External Service Auditor

TYPE OF REVIEW: AUDIT

BACKGROUND & KEY METRICS

Cloud computing is the practice of using a network of remote servers and related technologies hosted on the Internet to store, process or manage data, rather than on local servers or computer hardware. Variations of cloud computing, commonly known as Software as Infrastructure-as-a-Service (SaaS, IaaS and PaaS) enable companies to reduce information technology (IT) infrastructure expenditures while focusing on core business needs and privileged.

Company ABC has recognized the benefit of offering cloud service solutions to client-facing teams managed by the Company's Cloud Solution (CCS) for projects operating sensitive and non-sensitive cloud computing environments, such as the Company's ABC Share Solution. Company ABC has also realized the financial benefits of cloud solutions for internal IT operations managed by the Enterprise Operations Team (EOT) by implementing cloud solutions for Office 365 (email), Workday and Concur to support basic company operations and sustainability.

To ensure properly implemented controls over cloud governance, Internal Audit (IA) first conducted a Cloud Computing audit in 2014. As deployment of cloud technologies was in its early stages, the prior audit included a high finding related to the need to implement overall governance for cloud environments. Management addressed the high finding through enhancements to the company's Acceptable Use Policy (AUP) and Computing Environment Policy (CEP). The company's use of cloud technology, both internally and for client-facing environments, has expanded significantly since 2014. Our current audit, conducted from May 2016 to September 2016, focused on the completion of internal and client-facing cloud instances with the new policies, as well as compliance with risk mitigation activities brought forward from the ERM program.

RISK HIGHLIGHTS

- **Linkage to ERM: Cloud Security as a Tier 1 Cyber and Security Risk.**
- **Significant challenges exist with cloud solutions which require implementation of governance and technology need to be effectively implemented to ensure the safety of Company ABC and client systems and data managed by cloud service providers.**

OBJECTIVES

- **Validated and ERM Cyber and Security cloud-related risk mitigation activities.**
- **Assessed internal and client-facing cloud environment samples for compliance with policies:**
  - Computing Environment Policy (CEP)
  - Acceptable Use Policy (AUP)

RESULTS OVERVIEW

Details of all audit findings including recommendations, management responses and actions are in Appendix A.

**Key Strengths** - Noted several strengths related to Company ABC's cloud security governance model, including:

- The company’s recent upgrade to Amazon Web Services (AWS) Cloud Edge;
- Implementation of AWS Virtual Private Cloud (VPC) Security;
- Implementation of OpenID Portal, an automation, orchestration, and business platform; and
- Snapshot IT via Sky High reporting on cloud service provider usage

**High Finding**

- **Cloud Environment Security - Use of cloud computing resources is not fully compliant with the Computing Environment Policy (CEP) and IT Acceptable Use Policies, including Client lab environments within the cloud that have not been properly registered, as well as frequent usage of prohibited cloud services by individual employees. In addition, a governance process has not been consistently and formally deployed to employees who violate the policies with respect to cloud environments.**
FINDINGS AND OBSERVATIONS
KEY COMPONENTS OF A DETAILED FINDING

- **Issue Owner**: Identify the process owner overseeing the area at risk that is responsible for addressing the issue.

- **Issue Severity**: Measure of issue’s impact to the business.

- **Issue & Root Cause**: The observed problem with the system of internal control and root cause.

- **Risk**: Details of risk and potential or actual consequence. Describe the impact of the business risks.

- **Supporting Observations**: Key relevant details to understand the issue and demonstrate the issue is based on observed facts (i.e. breach in corporate standards, audit evidence, compensating control to support the issue severity).

- **Recommendations**: A checklist of measurable recommendations to close the issue identified.

- **Management Agreement**: Identifies management’s agreement/disagreement with the issue identified and the status of developing an action plan to close the issue (including a targeted remediation date).
QUALITY FINDINGS AND MANAGEMENT ACTIONS

An impactful report needs insightful findings.

- Findings are more than just the results of testing
- Discuss management actions with client before issuing draft report
- Organize the Findings (ex. Sub-process, type)
- Quantify the Impact
- Describe the Consequences
- Use a concise writing style
FINDINGS RANKING

Individual audit finding rankings require the use of significant professional judgement. It is important to have a clearly defined approach to audit ratings understood by the auditor and auditees.

• Provide management with a clearer picture of the significance of control deficiencies as an aid to prioritize corrective actions

• Reported to relevant process owners, project sponsors, and audit committee

• Individual audit findings should be assessed and rated based on their significance relative to the individual project, individual risks / risk categories, or organization as a whole

• Consider materiality and impact
One host (xyzcompany.com) is running an insecure and non-encrypted version of the Post Office Protocol (POP3) service. Data and connections to the service are transmitted in clear text.

**Risk**

Data transmitted without encryption could be intercepted by a malicious (unauthorized) user and used to try accessing other applications or systems.

**Recommendation**

*Short Term:* Determine if a valid business purpose exists for the POP3 service. If the service is not required, disable it. If it is required, change it to POP3S for encrypted SSL communication.
## FINDINGS SAMPLE – 2

<table>
<thead>
<tr>
<th></th>
<th>Issue</th>
<th>Risk(s)</th>
<th>Action Plan</th>
<th>Relates to Best Practice Recommendation</th>
<th>Implementer</th>
<th>Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Per policy, contracts should be reviewed by Legal and approved by Executive Management prior to execution. Unable to obtain requested contracts as they were not formally executed as contracts. Reviewed the supplier selection detail from the RFQs related to strapping and lubricants in place of a contract, but evidence of executive management approval was not maintained for the selection decision.</td>
<td>Legal exposure may exist due to inadequate/improper terms and conditions in PO or contract. Contract changes may not be documented, reviewed, approved and entered in the system (per policy and DOA). Contracts may no longer be competitive (price, performance, etc.) or in alignment with Corporate strategies, goals, and objectives.</td>
<td>Procurement will work with IT to determine the feasibility of implementing a system-based PO checklist that would ensure appropriate approvals are obtained and all PO requirements are included on POs prior to sending to suppliers.</td>
<td>R10</td>
<td>John Doe Q120XX</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>In the place of a formal contract with a supplier, POs should contain payment terms and applicable terms and conditions. Out of 20 POs sampled, 10 did not contain payment terms. 5 of the 10 POs also did not contain terms of delivery.</td>
<td>Legal exposure may exist due to inadequate/improper terms and conditions in PO or contract. Contract may not be current or valid (expiration date)</td>
<td>R14</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Observation #1 – Manual Process Steps Outside of SAP GRC

Observation:
Access management processes contain multiple manual activities that are managed outside of the scope of the SAP GRC application. Key observations include:

• SAP roles are manually mapped to XYZ Company positions and job roles – this mapping is stored in an offline database that has not been well-maintained since initial SAP go-live. Over time, the alignment of SAP roles to XYZ Company positions and job roles has become disconnected and resulted in manual procedures to determine appropriate access for end users. Significant time and effort has been put towards trying to determine a standardized alignment of roles and responsibilities across the enterprise to enable appropriate training and SAP access, but variability of what people actually do has created significant challenges to achieving a model that is sustainable.

• End users are required to complete SAP training modules before they are granted access to SAP production systems. This requirement significantly impacts users’ ability to get timely access to SAP, as multiple emails and follow ups are typically required to inform all appropriate personnel of training completion so access requests can be manually fulfilled.

• There currently is no process in place to update employees’ access when they change positions within the company. After discussions with IT and the business, it was noted the user’s manager is currently responsible to request the appropriate role removals, but this does not happen on a regular basis.

Root Cause:
The process design requires multiple manual steps that results in the delay of SAP access moves, adds, and changes.

Severity:
Critical
THE RECOMMENDATION
A well-developed recommendation demonstrates Internal Audit’s knowledge of the business context and adds value to the organization.

- Should be based on observations or conclusions
- Should be a call for action to correct existing conditions or improve operations
- May suggest approaches to correcting or enhancing performance as a guide for management in achieving desired results
- Are most effective when they are specific, measurable and actionable. They should also include ownership and timing
II. Detailed Observations

1.1 Insecure Internet Key Exchange (IKEv1) Configuration

Observation:
Two (2) instances of the IKE version 1 service were discovered that support "Aggressive Mode" with pre-shared key authentication.
* This vulnerability affects XYZ Company

Risk:
IKE Aggressive mode responds to a VPN client request to establish an IPSec Tunnel using an unencrypted authentication hash derived from the use of the pre-shared key (PSK). The design flaw in the IKEv1 protocol does not require an established IPSec Tunnel in order to capture the authentication hash from the gateway. Because this hash is not encrypted, all VPN connections that utilize pre-shared keys for authentication with aggressive mode enabled are at risk of divulging the unencrypted authentication hash. Note: Protiviti was able to obtain the authentication hash for both instances of this observation.

Recommendations:

Short Term:
- Disable Aggressive Mode if supported.
- Do not use Pre-Shared key authentication if possible. If using Pre-Shared key cannot be avoided, use strong keys.

Long Term:
- Ensure a process exists to configure all external devices not to use IKEv1 with Aggressive mode enabled.

Management Response:
Aggressive mode has been disabled.
### RECOMMENDATIONS SAMPLE – 2

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Related Observations</th>
<th>Benefits of Implementation</th>
<th>Challenges For Implementation</th>
<th>Time Impact</th>
<th>Cost Impact</th>
<th>People Impact</th>
</tr>
</thead>
</table>
| C. Adopt standard project management techniques into the ABC Co. project, including the development of project plans, status/issue reporting, and resource scheduling. | 1. No current project plan exists for the implementation. A high-level plan was developed initially, but was not maintained throughout the project.  
2. There is not a comprehensive list of issues and expected resolution dates currently maintained. Additionally, there is not a priority assigned to current issues.  
3. There is no formal detailed rollout plan to implement Application Z at the franchises. Sequencing the order of implementations at the franchise locations has not been formally developed and past implementations were decided on an ad hoc basis.  
4. Little effort or focus has been placed on the consideration of dependencies for the project. | - Increased visibility for management into the status of the implementation.  
- Increased focus on a successful implementation.  
- Increased ability to respond to issues and franchise requests.  
- Increased accountability for resources through the documentation of formalized tasks. | - Lack of experience with project management processes in the current IT organization.  
- Existing project resources may resist increased formalization and accountability. | Low | Low $ | Moderate ▲▲ |
| • This should primarily be the responsibility of the project manager that is identified in Recommendation B.  
• Regularly published status reports should be covered with Executive Management to help ensure resources are provided in a timely manner. | | | | | | |
RECOMMENDATIONS SAMPLE – 3

Ease of Implementation

Legend
- Wave 1
- Wave 2
- Wave 3

Recommendation

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
OVERALL AUDIT RATING
OVERALL AUDIT RATINGS

Audit ratings are a useful tool for management to gauge the performance of individual auditable units or areas against expectations.

- Can compare performance to previous audits
- Can describe how relevant section auditable/unit is performing
- Based on the number and rating of individual issues raised during the audit process
- Must take into account the expectations of senior management, the board, and other stakeholders
- Take care with wording, particularly around “waterlines” such as adequate or inadequate
<table>
<thead>
<tr>
<th>Rating</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong</td>
<td>Internal control systems are sufficiently comprehensive and appropriate to the size and complexity of the organization. Risks are effectively managed. Monetary risk associated with potential control failures is not material. A few exceptions to established policies and procedures were identified.</td>
</tr>
<tr>
<td>Satisfactory</td>
<td>While there may be some minor risk management weaknesses, these issues have been recognized and are being addressed. Risks are effectively managed. Internal control systems may display modest weaknesses or deficiencies, but they are correctable in the normal course of business.</td>
</tr>
<tr>
<td>Needs Improvement</td>
<td>Risk management practices are lacking in important ways and are a cause for more than supervisory attention. Risks may not be effectively managed. Weaknesses may include control exceptions or failures that could have adverse affects on the organization if corrective actions are not taken.</td>
</tr>
<tr>
<td>Needs Significant Improvement</td>
<td>Marginal risk management practices generally fail to identify, monitor and control significant risk exposures in many material respects. The organization may have serious identified weaknesses that require substantial improvement in internal controls or procedures. Risks are not effectively managed. Unless properly addressed, these conditions may result in a significant impact to the organization.</td>
</tr>
<tr>
<td>Unsatisfactory</td>
<td>Due to the absence of effective risk management practices, management is unable to identify, monitor or control significant risk exposure. Internal control systems may be sufficiently weak to jeopardize the continued viability of the organization. Risks are not effectively managed. Deficiencies in risk management procedures and internal controls require immediate and close supervisory attention.</td>
</tr>
</tbody>
</table>
## OVERALL AUDIT RATING SAMPLE – 2

<table>
<thead>
<tr>
<th>Rating</th>
<th>Scale</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Effective**| 1     | - Overall risk program is reliable and requires negligible improvements.  
- The risk management procedures are formalized and documented and clearly communicated and understood throughout the business. Risk management system is robust and possesses the capacity and ability to consistently identify, document and assess existing and emerging risks. |
|              | 2     | - Risk controls effectively manage, mitigate and transfer existing and foreseeable risks and do not expose the business to undue risk. Risk program does not expose the business to unwarranted financial loss or regulatory non-compliance. Audit recommendations are generally housekeeping in nature. |
| **Monitor**  | 3     | - Overall risk program is adequate for the current level of risk within the business, but requires ongoing monitoring.  
- The risk management procedures are formalized and documented, but not clearly communicated. Risk procedures need to be clearly communicated and business needs to obtain assurance that procedures are understood. Although the risk management system possesses the capacity and ability to identify, document and assess existing risk, specific improvements are needed to ensure accurate and timely incorporation of emerging risks. |
|              | 4     | - Risk controls adequately manage, mitigate and transfer existing risks but improvements are required as emerging risks and changing conditions could lead to a weakened risk management capacity. Risk program does not expose the business to immediate financial loss or regulatory noncompliance. The director must make improvements within 60 days. |
| **Needs Improvement** | 5     | - No more than one high-risk issue  
- No more than four medium-risk issues  
OR  
- No high-risk issues and no more than six medium-risk issues |
|              | 6     | - No more than two high-risk issue  
- No more than six medium-risk issues  
OR  
- No more than one high-risk issue and more than six medium-risk issues |
| **Impaired** | 7     | - No more than three high-risk issues  
- No more than four medium-risk issues |
|              | 8     | - No more than three high-risk issues  
- No more than six medium-risk issues |
| **Unsatisfactory** | 9     | - More than four high-risk issues  
- No more than six medium-risk issues  
OR  
- No more than two high-risk issues and more than six medium-risk issues |
|              | 10    | - More than four high-risk issues  
- More than six medium-risk issues |
OVERALL AUDIT RATING SAMPLE – 3

APPENDIX A – AUDIT REPORT EVALUATIONS OF CONTROL ENVIRONMENT

The Internal Audit Department issues three standard audit report evaluations as defined below:

**Acceptable**
The control environment is acceptable with minor issues having been identified, if any. The overall environment contains sufficient internal controls to address key risks, and business practices generally comply with Company policies. Corrective action should be implemented to address any weaknesses in order to maintain or enhance the control environment.

**Needs Improvement**
The control environment needs improvement with significant issues, individually or in the aggregate, having been identified, or business practices do not comply with Company policies. The overall environment contains insufficient internal controls to address key risks. Prompt corrective action should be implemented to address the weaknesses in order to strengthen the control environment.

**Unacceptable**
The control environment is unacceptable with critical issues, individually or in the aggregate, having been identified or major noncompliance with Company policies. The overall environment contains insufficient internal controls to address key risks and the impact may be substantial in size or nature or their effect cannot be quantified. Immediate corrective action should be implemented (including oversight and monitoring) to address the weaknesses and strengthen the control environment.

**Note:** Significant issues in audit reports with adverse conclusions (Needs Improvement or Unacceptable) will be communicated to the Audit Committee. In addition, Internal Audit will conduct a follow-up audit in the future to assess the progress made in implementing the management action plans included in the audit report.
PART 2 – COMMUNICATING TO THE AUDIT COMMITTEE
KEY FACTORS IN DETERMINING CONTENT

**Understanding Board Expectations**

- The Audit Committee Charter
- The Internal Audit Department Charter
- Committee members and their backgrounds focusing on any changes since last meeting
- Prior Audit Committee Reports and Minutes
- Any arrangements that have been documented concerning report content expectations
- Board Communication Style

**Frequency of Meetings**

**Allotted Agenda Time**
### SAMPLE CALENDAR

#### Typical Audit Committee includes reports from the following groups:
- Internal Audit
- External Audit
- Risk Management
- Legal, Compliance and Regulatory
- Financial Reporting Oversight
- Committee Structure and Function

#### 1. Evaluate the Internal and Independent Audit Processes

<table>
<thead>
<tr>
<th>A. Internal Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Charter, Mission, and Objectives</td>
</tr>
<tr>
<td>Appointment and compensation of Chief Audit Executive</td>
</tr>
<tr>
<td>Budget, staffing and resources including resource constraints if any</td>
</tr>
<tr>
<td>Scope, procedures and timing of audits (i.e., audit plan)</td>
</tr>
<tr>
<td>Review of audit results and reports</td>
</tr>
<tr>
<td>Review internal and external quality assurance procedures</td>
</tr>
<tr>
<td>Confirm Internal Audit Independence</td>
</tr>
</tbody>
</table>

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
DASHBOARD SAMPLES
# Dashboard Sample – 1

## Audits

<table>
<thead>
<tr>
<th>Full &amp; Partial Scope Audits</th>
<th>Sarbanes-Oxley (SOX)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
<td><strong>Internal Control Over Financial Reporting (ICFR) Testing Summary</strong></td>
</tr>
<tr>
<td>Internal Audit performs both ‘full scope’ and ‘partial scope’ audits.</td>
<td>Total ICFR Test Cases: 256</td>
</tr>
<tr>
<td></td>
<td><strong>Exception / Deficiency Summary</strong></td>
</tr>
<tr>
<td></td>
<td>20xx Year-end Significant</td>
</tr>
<tr>
<td></td>
<td>Deficiency: Tax department resource limitations</td>
</tr>
<tr>
<td></td>
<td>Effective</td>
</tr>
<tr>
<td></td>
<td>239</td>
</tr>
<tr>
<td><strong>IT General Computer Controls and Application Controls Testing Summary</strong></td>
<td>Total IT GCC Test Cases: 228</td>
</tr>
<tr>
<td></td>
<td><strong>Exception / Deficiency Summary</strong></td>
</tr>
<tr>
<td></td>
<td>20xx Year-end Significant</td>
</tr>
<tr>
<td></td>
<td>Deficiency: IT security control failures</td>
</tr>
<tr>
<td></td>
<td>Effective</td>
</tr>
<tr>
<td></td>
<td>205</td>
</tr>
</tbody>
</table>

## Full & Partial Scope Audits

<table>
<thead>
<tr>
<th>International</th>
<th>North America</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>5</td>
</tr>
</tbody>
</table>

## Other Core and Risk-based Audits

<table>
<thead>
<tr>
<th>Audit Activities</th>
<th>Audit Name</th>
<th>Rating</th>
<th>Issues / Highlights</th>
</tr>
</thead>
</table>
|                  | IT Portfolio Management      | Medium | - Benefits Realization Standards lacking  
|                  | Data Privacy [pending issuance] | TBD    | - Leakage of personal data continues to be a risk  
|                  |                              |        | - Privacy Guidance deployment progress needs improvement.                                                                                         |
INTERNAL AUDIT DASHBOARD

GOALS PROGRESS

- Become a more trusted business advisor, evaluating the most critical risks to the organization
- Conduct work with relevant technical talent, leveraging audit tools and processes that optimize efficiency and effectiveness
- Communicate with key stakeholders in a more meaningful and consistent manner, with explicit measurement of value provided to the organization

PLAN COMPLETION AND HIGHLIGHTS

QUARTER HIGHLIGHTS
- 4 audits in reporting/complete stage: 2 High findings identified
- Data mining/analytics embedded; positively impacting audits
- Increased outreach to IA for assistance/discretionary time
- Re-evaluating classified testing approach
- IA tool purchased

See Appendix A for more detail

KEY AUDIT UPDATES

PLAN CHANGES
- Additions:
  - Incident Reporting
  - XYZ ABC Consulting
- Deletions:
  - N/A

HIGH FINDINGS
- Prior Quarter Open
- Plus New/Relisted
- Current Quarter Open
- Closed Audit Pending

See Appendix A for more detail

METRICS UPDATE

Alignment to Risk Categories

Client Satisfaction

% Technical Time (non-SOX)

Training Hours Per Auditor

% Certified Auditors

Turnover Ratio

Cost Center vs. Actual

Staff Utilization

Audit Report Timeliness

See Appendix C for more detail

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Key Message Points

- Cash Account Reconciliations have improved, however remediation efforts related to system design deficiencies are still ongoing.
- There is no formal communication between AP and the Merchandising (Buyer) department to develop uniform, beneficial practices for supplier management, and communication with suppliers should be managed to establish mutually agreeable practices.

Summary of Completed Activities (2nd Quarter 20XX)

- Completed Activities
  - Payroll
  - Accounts Receivable and Vendor Management
  - Continuation of Premium Accounts Reconciliation Special Project

Summary of Completed Activities (3rd Quarter 20XX)

- Audits schedules for Q3 20XX
  - Retail Stores and Back Office
  - Accounts Payable
  - Vendor Master File Maintenance

Audit Finding Remediation Status

<table>
<thead>
<tr>
<th>Risk Rating Category</th>
<th>Beginning Balance (as of May 20XX)</th>
<th>New</th>
<th>Closed</th>
<th>Currently Open</th>
<th>Open Past Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Medium</td>
<td>10</td>
<td>5</td>
<td>2</td>
<td>13</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>17</td>
<td>0</td>
<td>2</td>
<td>15</td>
<td>3</td>
</tr>
<tr>
<td>Total Findings</td>
<td>29</td>
<td>6</td>
<td>4</td>
<td>31</td>
<td>8</td>
</tr>
</tbody>
</table>

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
## Risk & Control Awareness

- Led 3 sessions of SOX orientation for worldwide controllers – team commented that this helped improve.
- Published quarterly risk trends
- CSA training
- Provided SOX orientation to new XYZ acquisition & briefed them on SOX process
- Various - responded to over 40 inquiries & reviews such as review of new Ethics video, xx, xxx, contract review ABC, etc

## Direct Support to Control Environment

- Ethics Committee participation - quarterly
- Due diligence support for XYZ acquisition
  - Identified xx control issues impacting.
- Participated in the following new system/process redesign projects
  - ABC (improved xx)
  - XYZ (improved zz)

## Cost Recovery

<table>
<thead>
<tr>
<th>Business Unit</th>
<th>Cost Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate payments in XYZ audit</td>
<td>$85K</td>
</tr>
<tr>
<td>Vendor compliance issues in ABC audit</td>
<td>$150K</td>
</tr>
</tbody>
</table>

**Total** $XX

## Future Savings/Process Improvements

- Streamlining of IT access process $XX annually
- Reduction of FTE at XYZ location due to .. $70k annually

**Total** $XX
RISK ASSESSMENT RESULTS
RISK MAP – 1

**Impact**
- Financial loss
- Strategic objectives achievement
- Operational impact
- Reputation

**Likelihood**
- Probability of the risk event occurring

**Velocity**
- Speed with which the impact of the risk event is realized

**Persistence**
- The period of time over which the consequences of the risk event are experienced

**Response Readiness**
- The organization’s preparedness to manage/respond to an event or a series of events (including contingency plans)

Size of bubbles represents the relative persistence of the scenarios.
Color of bubbles represents the relative velocity of the scenarios.
Bubbles can be replaced with different shapes to reflect response readiness.
RISK MAP – 2

The Risk Map depicts the relative significance and likelihood of business risks. Risk Map includes participants’ consideration of perceived internal controls and Protiviti’s professional judgment and experience.

Accounts Payable
1. Inaccurate Payments to Vendors
2. Data Integrity
3. Unauthorized Disbursements
4. Financial Exposure
5. Inappropriate Use of Systems

Accounts Receivable
6. Reliability & Efficiency
7. Consistency
8. Billing and Collections
9. Business Risk Factors

IT Projects
10. Executive Ownership
11. Process & Control Reengineering
12. Development Platform
13. Project Budget
14. Project Management (PMO)
The updated risk map represents the prioritization of IT Processes based on discussions with the individuals noted previously. As a result of our discussions, the placement of various risks has changed as indicated by the arrows and a new risk was added which has been circled.
INTERNAL AUDIT CALENDAR AND PLAN
# AUDIT CALENDAR – 1

<table>
<thead>
<tr>
<th>Audit</th>
<th>Risk</th>
<th>Type</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
<th>Apr</th>
<th>May</th>
<th>Jun</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Process</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd Party Contracts Audit</td>
<td>5</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revenue Accounting</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reimbursement Claims</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Information Technology</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Portal</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Pen</td>
<td>5</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAP SOD</td>
<td>5</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Consulting/Special Projects</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Optimization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Pre-Imp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Risk Level Legend:
- **■■■■■** Deferred Reviews
- **■ ■■■** Revised Timeline

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
20XX IT Audit Plan - Company X Audit Plan and Activities

- Accounts Payable Review
- Accounts Receivable Review
- ITIL - Change Management & Service Desk
- PIMS – Interface Engine
- Audit Committee Reporting
- Quarterly Follow Up
- IT Risk Assessment (Initial)
- Update IT Risk Assessment
- Coordinate with External Auditor

Color Legend

<table>
<thead>
<tr>
<th>Complete</th>
<th>In Process</th>
<th>Not Started</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢</td>
<td>🟠</td>
<td>🟥</td>
</tr>
</tbody>
</table>

AUDIT CALENDAR – 2
## AUDIT CALENDAR – 4

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal Audit</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accounts Payable Review</td>
<td>Accounts Receivable Review</td>
<td>Review 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Anti-Money Laundering Review</td>
<td>Review 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review 3</td>
<td>Risk Assessment</td>
<td></td>
</tr>
<tr>
<td><strong>SOX 404</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Draft 20XX 404 Scope</td>
<td>Finalize 20XX 404 Scope</td>
<td>Execute Testing</td>
<td>Validate Self-Assessments</td>
</tr>
<tr>
<td>Update Self-Assessment Program</td>
<td>Schedule Audits</td>
<td>Validate Self-Assessments</td>
<td>Monitor Deficiency Remediation</td>
</tr>
<tr>
<td></td>
<td>Roll-out Self-Assessment Program</td>
<td>Monitor Deficiency Remediation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Update Control Documentation</td>
<td>Complete Self-Assessment</td>
<td>Complete Self-Assessments</td>
</tr>
<tr>
<td></td>
<td>Complete Self-Assessments</td>
<td>Evaluate Tested Controls</td>
<td>Evaluate Tested Controls</td>
</tr>
<tr>
<td></td>
<td>Remediate Deficiencies</td>
<td>Remediate Deficiencies</td>
<td>Remediate Deficiencies</td>
</tr>
</tbody>
</table>

Legend:
- Deferred
- Not Started
- Scoped
- In Progress
- Fieldwork Complete
- Report Drafted
- Complete
# AUDIT ACTIVITY SUMMARY – 1

We assessed the existence and effectiveness of controls in relation to …

## Completeness & Accuracy – Authority/Limit

<table>
<thead>
<tr>
<th>Description</th>
<th>Rating</th>
<th>Detailed Issues &amp; Action Plans Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppliers are properly authorized prior to procuring goods/services.</td>
<td></td>
<td>Detailed Issue and Action Plan #5</td>
</tr>
<tr>
<td>Accounts Payable disbursements are properly authorized.</td>
<td></td>
<td>Detailed Issue and Action Plan #1, #2, #5, #7</td>
</tr>
<tr>
<td>Access to applicable AP systems is properly segregated.</td>
<td></td>
<td>Detailed Issue and Action Plan #2, #9, #12</td>
</tr>
</tbody>
</table>

## Timeliness – Effectiveness/Efficiency

<table>
<thead>
<tr>
<th>Description</th>
<th>Rating</th>
<th>Detailed Issues &amp; Action Plans Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disbursements are made to maximize cash flow.</td>
<td></td>
<td>Detailed Issue and Action Plan #1, #2</td>
</tr>
<tr>
<td>Costs are reduced as much as possible.</td>
<td></td>
<td>Detailed Issue and Action Plan #2, #7, #8, #10</td>
</tr>
<tr>
<td>Processing time is minimized.</td>
<td></td>
<td>Detailed Issue and Action Plan #2, #3, #4, #5, #6</td>
</tr>
<tr>
<td>Performance measures used to control the process are reliable.</td>
<td></td>
<td>NA</td>
</tr>
</tbody>
</table>

## Controls

- **Strong Controls**
- **Moderate Controls**
- **Limited Controls**
Background

- International stations located in Europe, Latin America
- International operations processes are divided among several departments including: …
- Relative to domestic operations, the international business offices are small, with a staff of … Due to the cultural differences, country-specific regulations, and distance between international locations and corporate headquarters, the inherent risk level is increased.

Audit Summary

This review focused on:
- Understanding policies and procedures in-place related to in-scope processes;
- Evaluating the control environment around: human resources, payroll, accounts payable, month-end procedures, expense reimbursement, and contract validation;
- Evaluating the effectiveness of procedures and internal controls related to in-scope processes. Control and process improvements were identified

Observations Summary

Control Improvement Opportunities:
- Protocols around payroll change documentation…
- The process for reviewing employee…
- Current, signed contracts are not…

Controls Assessment

Controls Rating
- Satisfactory
- Marginal
- Unsatisfactory
Report Name: Information Security Audit --- issued 1/1/20xx  
Overall Rating: High

Background and Scope

Many companies store and process a large volume of personal and sensitive information on behalf …

The scope included:

• **Network Security:** Conducted a vulnerability assessment to determine …
• **User Level Security Practices:** Evaluated several business critical security processes …
• **Governance:** Reviewed the roles, responsibilities and supporting policies and procedures …

Summary Findings: The scorecard below summarizes ratings and findings by scope area.

<table>
<thead>
<tr>
<th>Scope Area</th>
<th>Rating</th>
<th>Issues Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Security [internal]</td>
<td>High</td>
<td>Multiple network security controls are not operating effectively…</td>
</tr>
<tr>
<td>Network Security [external]</td>
<td>Medium</td>
<td>Employees provided valid email user names and passwords during electronic and telephonic social engineering exercises.</td>
</tr>
</tbody>
</table>

Management Response (at report issuance): *Management agrees with the items outlined in the report and will take corrective action to address identified issues.*
### AUDIT ACTIVITY SUMMARY – 4

<table>
<thead>
<tr>
<th>Overall Rating</th>
<th>Plats</th>
<th>Distribution Centers</th>
<th>Corporate Functions</th>
<th>Service Centers</th>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>⚫</td>
<td>⚫</td>
<td>◆</td>
<td>◻</td>
<td>◆</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audits</th>
<th>Plats</th>
<th>Distribution Centers</th>
<th>Corporate Functions</th>
<th>Service Centers</th>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>(P) Audit 1</td>
<td>⚫</td>
<td>[1 high item]</td>
<td>(CF) Audit 1 [3 high items]</td>
<td>(SC) Audit 1 [2 high items]</td>
<td>(IT) Audit 1 [1 high item]</td>
</tr>
<tr>
<td>(P) Audit 2</td>
<td>⚫</td>
<td>[0 high items]</td>
<td>(CF) Audit 2 [4 high items]</td>
<td>(SC) Audit 2 [1 high item]</td>
<td>(IT) Audit 2 [2 high items]</td>
</tr>
<tr>
<td>(P) Audit 3</td>
<td>[2 high items]</td>
<td>[0 high items]</td>
<td>(CF) Audit 3 [1 high item]</td>
<td>(SC) Audit 3 [1 high item]</td>
<td>(IT) Audit 3 [3 high item]</td>
</tr>
<tr>
<td>(P) Audit 4</td>
<td>[0 high items]</td>
<td>[0 high items]</td>
<td>(CF) Audit 4 [2 high items]</td>
<td>(SC) Audit 4 [0 high items]</td>
<td>(IT) Audit 4 [2 high items]</td>
</tr>
<tr>
<td>(P) Audit 5</td>
<td>[0 high items]</td>
<td>[0 high items]</td>
<td>(CF) Audit 5 [0 high items]</td>
<td></td>
<td>(IT) Audit 5 [1 high item]</td>
</tr>
<tr>
<td>(P) Audit 6</td>
<td>[0 high items]</td>
<td></td>
<td>(CF) Audit 6 [2 high items]</td>
<td></td>
<td>(IT) Audit 6 [2 high items]</td>
</tr>
<tr>
<td>(P) Audit 7</td>
<td>[0 high items]</td>
<td></td>
<td></td>
<td></td>
<td>(IT) Audit 7 [5 high items]</td>
</tr>
</tbody>
</table>

### RATING LEGEND

- ⚫ Low Risk
- ◼ Medium Risk
- ◆ High Risk *(immediate action required)*
CONTINUOUS AUDITING

At the start of 20XX, IA developed and implemented routines (i.e., scripts) in ACL to automate expense reporting, journal entry, and user administration analytics. A core team of three resources is responsible for managing our continuous auditing program. Quarterly results are provided below.

<table>
<thead>
<tr>
<th>Frequency</th>
<th>% of Population Tested</th>
<th>Issues Identified this Quarter</th>
<th>Significant Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expense Reporting</td>
<td>Monthly 100%</td>
<td>40 🔴</td>
<td>2 🟢</td>
</tr>
<tr>
<td>Journal Entries</td>
<td>Quarterly 100%</td>
<td>20 ⇨</td>
<td>0 🟢</td>
</tr>
<tr>
<td>User Access Removal</td>
<td>Monthly 100%</td>
<td>0 ⇨</td>
<td>0 ⇨</td>
</tr>
</tbody>
</table>

Significant Issues Summary:
• Two expense reporting issues related to FCPA…
ISSUE FOLLOW UP STATUS
**FOLLOW UP STATUS – 1**

*Internal Audit performs follow-up reviews for each report issued to ensure that all control improvement action items have been completed.*

<table>
<thead>
<tr>
<th>Completed Reviews</th>
<th>Rating</th>
<th>Report Date</th>
<th>Follow up Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales Review</td>
<td>N/R</td>
<td>&lt;Date&gt;</td>
<td>Complete</td>
</tr>
<tr>
<td>Human Resources – Leave of Absence Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vacation Systems Development Review</td>
<td>N/R</td>
<td>&lt;Date&gt;</td>
<td>Complete</td>
</tr>
<tr>
<td>Site Audits</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Follow up in Progress</th>
<th>Rating</th>
<th>Report Date</th>
<th>Follow up Comments (ETC – Estimated Time to Completion)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service Training Audit</td>
<td></td>
<td>&lt;Date&gt;</td>
<td>Open item related to iLearning (online training) interface upgrade. ETC &lt;Date&gt;</td>
</tr>
<tr>
<td>Corporate Payroll Process Audit</td>
<td></td>
<td>&lt;Date&gt;</td>
<td>Open item related to edit report creation, IT request pending. ETC &lt;Date&gt;</td>
</tr>
<tr>
<td>Website Review</td>
<td>N/R</td>
<td>&lt;Date&gt;</td>
<td>Delays due to resource allocation to ReShop/Choice Seats. ETC &lt;Date&gt;</td>
</tr>
<tr>
<td>Human Resources Review</td>
<td>N/R</td>
<td>&lt;Date&gt;</td>
<td>Comprehensive process changes due to in-progress review. ETC &lt;Date&gt;</td>
</tr>
<tr>
<td>Inventory Management</td>
<td></td>
<td>&lt;Date&gt;</td>
<td>Open action plans are on-track for completion by &lt;Date&gt;</td>
</tr>
</tbody>
</table>
### Process Controls

<table>
<thead>
<tr>
<th>Process</th>
<th>Control Ref.</th>
<th>Controls</th>
<th>Status of Remed.</th>
<th>Testing Status</th>
<th>Comments</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Design Remediation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll/ Benefits &amp; Insurance</td>
<td>PR33</td>
<td>Access to process payroll runs is restricted ...</td>
<td>Complete</td>
<td>Complete</td>
<td>Access to be reviewed and necessary remediation to be identified during SOD Analysis. SOD Analysis pending validation by Protiviti.</td>
<td>Payroll Mgr.</td>
</tr>
<tr>
<td></td>
<td>PR34</td>
<td>Access to generate the ledger distribution, which automatically creates ...</td>
<td>Complete</td>
<td>Complete</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PR35</td>
<td>Access to add or update employees is restricted to the HR Representatives.</td>
<td>Complete</td>
<td>Complete</td>
<td>See PR21 NEW MONITORING CONTROL for PR33</td>
<td></td>
</tr>
<tr>
<td><strong>Operational Remediation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Entity Level</td>
<td>EL41</td>
<td>Functional segregation of duties within key processes are reviewed annually. Where conflicts exist, ...</td>
<td>Delayed</td>
<td>Delayed</td>
<td>SOD Analysis pending</td>
<td>Sr. Manager and Protiviti</td>
</tr>
<tr>
<td>Inventory</td>
<td>IN15</td>
<td>Inventory Control Associates verify the Inventory Adjustment Form is approved by a ...</td>
<td>Complete</td>
<td>Complete</td>
<td>Discussed with Management – remediation underway.</td>
<td>Inventory Control Manager</td>
</tr>
<tr>
<td>Expend.</td>
<td>AP03</td>
<td>Accounts Payable verifies non-merchandise expenditures and employee expense reimbursements ...</td>
<td>At Risk</td>
<td>At Risk</td>
<td>Testing in progress</td>
<td>Assistant Controller</td>
</tr>
</tbody>
</table>
## FOLLOW UP STATUS – 3

<table>
<thead>
<tr>
<th></th>
<th>Plants</th>
<th>Distribution Centers</th>
<th>Corporate Functions</th>
<th>Service Centers</th>
<th>Information Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overall Rating</strong></td>
<td>![Low Risk]</td>
<td>![Low Risk]</td>
<td>![Medium Risk]</td>
<td>![Medium Risk]</td>
<td>![High Risk (immediate action required)]</td>
</tr>
<tr>
<td><strong>Total Issues</strong></td>
<td>28</td>
<td>19</td>
<td>31</td>
<td>23</td>
<td>48</td>
</tr>
<tr>
<td><strong>Open Issues</strong></td>
<td>4</td>
<td>7</td>
<td>12</td>
<td>8</td>
<td>21</td>
</tr>
<tr>
<td><strong>PAST DUE</strong></td>
<td>0</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td><strong>Owner</strong></td>
<td>Owner Name, Vice President</td>
<td>Owner Name, Vice President</td>
<td>Owner Name, Senior Director</td>
<td>Owner Name, Senior Director</td>
<td>Owner Name, 2nd Vice President</td>
</tr>
</tbody>
</table>

### RATING LEGEND
- ![Low Risk]
- ![Medium Risk]
- ![High Risk (immediate action required)]
SOX PROGRAM OVERVIEW AND RESULTS
<table>
<thead>
<tr>
<th></th>
<th>Q1 20xx</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>APR</td>
<td>Form 10-Q due</td>
<td>MAY</td>
<td>JUN</td>
<td>JUL</td>
<td>AUG</td>
</tr>
</tbody>
</table>

**SOX APPROACH AND TIMELINE**

1. **Implement 302 Certification Process**
2. **Evaluate Entity-level Controls**
3. **Control Design Assessment**
4. **Test Key Controls**
   - Remediate Design Gaps
   - Remediate Control Deficiencies

**Key External Auditor Checkpoints**

**Status Reporting**

**Ongoing Communication/Project Management**

**Legend**
- Internal Audit activity
- Management activity
- Milestone
- Auditor Checkpoint
- Audit Committee Meeting

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Current Events/Trends

- Interim testing is complete and preliminary results indicate that processes are well controlled and operating effectively.

“Not Tested” includes controls that had no sample to test at Interim and controls that are only scheduled for testing during Update/Year End testing. The following control cycles will primarily be tested during Update/Year End testing:
## INTERNAL CONTROL SUMMARY – 2

### 20YY SOX Significant Deficiency Summary (Client Management)

<table>
<thead>
<tr>
<th>Internal Controls Information</th>
<th>Rating</th>
<th>Remediation Status</th>
<th>Actions to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Entity Level Controls</td>
<td>Medium</td>
<td>Complete</td>
<td>Finance/Legal/Development Communication; Whistleblower Hotline</td>
</tr>
<tr>
<td>Adjustments &amp; Account Reconciliations</td>
<td>Low</td>
<td>Complete</td>
<td>N/A</td>
</tr>
<tr>
<td>Financial Accruals</td>
<td>Medium</td>
<td>In-process</td>
<td>New issues identified resulting in $X correction booked in Q1 –</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Finance leader recruited in Q2 for process enhancement</td>
</tr>
<tr>
<td>Board Level Entity Level Controls</td>
<td>Low</td>
<td>Not Applicable</td>
<td>N/A</td>
</tr>
<tr>
<td>Business Unit #2 Management Group (Financial Reporting, Treasury &amp; Process Level)</td>
<td>Medium</td>
<td>Complete</td>
<td>Subsidiary books were reopened to book approximately $X in adjustments</td>
</tr>
<tr>
<td>Business Unit #2 Management Group (IT Security &amp; Change Management)</td>
<td>Low</td>
<td>Not Applicable</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 20XY SOX Significant Deficiency Summary (External Auditor)

<table>
<thead>
<tr>
<th>Internal Controls Information</th>
<th>Rating</th>
<th>Remediation Status</th>
<th>Actions to Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>No additional SOX significant deficiencies or material weaknesses identified to-date in 20XY</td>
<td>Low</td>
<td>Complete</td>
<td>Rating based on testing done to-date; substantial year end controls to be tested in Q3</td>
</tr>
</tbody>
</table>

© 2018 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services. All registered trademarks are the property of their respective owners.
Face the Future with Confidence