Jumpstart your 2020 SOX program:

Sue King, Partner, KPMG LLP

March 11th, 2020
Agenda

- PCAOB focus areas
- ICFR hot topics
- SOX point of view
- SOX reimagined – Data-driven SOX
PCAOB focus areas
PCAOB areas of inspection focus

- ICFR, ICFR, and more ICFR!
- System of quality control
- Recurring inspection deficiencies
  - Internal control over financial reporting
  - Revenue recognition
  - Estimates and reserves (e.g., allowance for loan losses)
  - Risks of material misstatement
- External considerations
- Cybersecurity risks
- Software audit tools
- Implementation of new accounting standards
- IT/technology considerations
ICFR
— Did not sufficiently test review controls (e.g., did not understand the activities performed and the factors considered by the control operator related to estimates and assumptions)
— Did not test the controls that addressed the risks of misstatement

Accounting estimates (e.g., ALLL, business combinations, fair value of financial instruments)
— Did not understand the methodology used to develop the estimate
— Did not test the completeness and accuracy of data
— Did not test the reasonableness of significant assumptions
— Did not evaluate corroborating and contradictory evidence over such assumptions
ICFR hot topics
ICFR hot topics

Risk assessment
- Big picture of risk
- Specifics of each risk
- Data lineage

Auditing accounting estimates and fair value measures

Critical audit matters
IT hot topics

- Focus on risk assessment
- SOC report evaluations
- GITC and ITAC scoping
- Completeness and accuracy (IPE)
- Software change management
- Tools used in the execution of controls
Bot governance

Risk management in

Risk & Strategy

Risk & Operations

Risk Profile & Tolerance

Bots, Apps & infrastructure

Use Cases & Roadmap

Risk & Delivery

Training, Tools, and Enablement

Automation and cognitive drive business transformation

Risk & governance Center of Excellence

Identity and Access Management

Information Security and Privacy

Change Management

Availability and Business Continuity

Secure Code Development

Logging, Auditing and Traceability

Processing Integrity

Completeness and Accuracy

Compliance
Cyber risk

- Risk assessment
- Monitoring
- Communication of “incidents” to accounting and within the organization
- Evaluation of:
  - Impact and magnitude if it “did” impact systems and data
  - If it “could have” impacted the financial systems
SOX point of view
SOX point of view

- Increased documentation level
- Focus on completeness and accuracy
- Precision levels
- Sample sizes
- Testing period requirements

Flexibility to use daily activities and year over year knowledge to support control conclusions

Areas of tension/difference

Open dialogue to understand the “whys”

- Fee gap
- Expectation gap
- Level of effort gap
Misalignment of risk and ICOFR focus/effort

Current work effort vs. Risk based work effort

High risk

Low risk

Low risk

High risk
SOX reimagined
Data-driven SOX

- G/L analytics for insight into Risk Assessment
- Analytics for scoping in the selection of control activities
- Implement analytics as control activities: Monitoring controls, key process controls
- Reduce SOX testing in related processes
- Completeness and accuracy leverages GITCs over G/L and subledger data which is already in scope
Considerations for using bots in testing

<table>
<thead>
<tr>
<th>I. High manual effort</th>
<th>II. System or structured data</th>
<th>III. Low-Judgement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Individual engagement effort</strong></td>
<td><strong>System reports</strong></td>
<td><strong>Data analytics/manipulation</strong></td>
</tr>
<tr>
<td>A given activity takes a relatively large number of hours in the annual budget.</td>
<td>The required data is able to be generated directly from standardized system reports.</td>
<td>The process involves generating data insights or predictably combining/manipulating data sets.</td>
</tr>
<tr>
<td><strong>Collective effort</strong></td>
<td><strong>Database extracts</strong></td>
<td><strong>System configurations analysis</strong></td>
</tr>
<tr>
<td>A given activity takes a relatively large number of hours in the annual budget.</td>
<td>The required data is able to be extracted directly from a database using new or existing queries.</td>
<td>The process involves the analysis of key system configurations or settings.</td>
</tr>
<tr>
<td><strong>Opportunities for expanded scope or new offerings</strong></td>
<td><strong>Excel/CSV/Txt Files</strong></td>
<td><strong>Predefined compliance criteria</strong></td>
</tr>
<tr>
<td>Opportunities exist to test larger sample sizes or data sets using automation as an accelerator.</td>
<td>The required data sits in structured or semistructured formats such as excel, csv, or txt files.</td>
<td>The process involves the review of data against a predefined list of criteria for compliance.</td>
</tr>
</tbody>
</table>
Thank you
Sue King
Partner – Advisory,
Internal Audit and Enterprise Risk
KPMG LLP
E: susanking@kpmg.com
T: +1 213-955-8399
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. NDP050884-2A

The KPMG name and logo are registered trademarks or trademarks of KPMG International.