Internal Control Transformation

San Diego IIA Chapter – May 10, 2017
The Purpose of Controls Transformation

WHY CONTROLS TRANSFORMATION?

- Companies have been approaching ICOFR with a standard compliance approach, rather than additional focus on alignment with stakeholder strategic views.
- Lack of focus on process improvement and “value add” continues to undermine the effectiveness of many programs in *reducing risk, reducing cost, and driving value*. 
The Evolution of SOX

SOX Effort

- Management’s Testing
- External Auditor Testing

Level of Effort

- High number of controls, low level of testing detail
- Low number of controls, high level of testing detail
- Increased complexity of accounting and ICOFR


Events:
- Sarbanes Oxley Act passed
- AS2
- SEC issues interpretative guidance for management
- AS 5
- PCAOB SAPA 11: Considerations for audits of ICOFR
- PCAOB SAPA12: Auditing Reverse
- Revenue Recognition & Leasing Standards
I haven’t had an issue. Why should I check the health of my ICOFR program?

Potential loss of Audit Committee trust

Impact on share price/total cost of the business

Focus on total cost of control

Drive continuous improvement and efficiencies

It’s expensive to remediate once something has gone wrong

Even if you don’t think you have a problem, you should have a ‘check up’

A link between stronger controls and greater predictability of earnings/overall valuation of a company

Need for a strong 404a process, irrespective of PCAOB or external auditor perspective

You’ve had a significant deficiency or some ‘close calls’

The external auditor cost is high once you end up with a material weakness

Impact on management compensation related to MW’s

In extreme circumstances, the external auditor may resign

© 2016 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.
Do you have a healthy ICOFR program?

- If you stood back and looked at your overall program, would management, executive management and the Board conclude that is valuable?
- Does your Company culture and tone at the top support the ICOFR program?
- Do you know which are your 10-20 most critical controls? Is your internal control program geared towards those critical 10-20 controls?
- Do you have a strong set of direct entity level controls?
- Do you feel confident that your controls would pass, even without testing them each year?
- Do you have KPIs that would allow you to identify and monitor potential issues in your program?

Most decisions beyond this are an ECONOMIC DECISION.
Common Areas of Improvement

There are a few common areas in which improvements can be made with a healthy ICOFR program.

**Common Controls**
Align the design of common controls to be tested once rather than in multiple locations and streamline key control attributes

**Spreadsheets**
Include a documented purpose for key spreadsheets, and detail the IPE procedures in place to verify completeness and accuracy

**Risk Assessment**
Ensure a thorough risk assessment, in which the audit risks are identified and linked to key controls

**System Scoping**
Ensure business process and systems are aligned from a scoping perspective
Key Attributes of a Healthy ICOFR Program

— Well integrated program that does not operate in silos
— Company is able to articulate the strategy behind its ICOFR program, and is able to effectively defend the company’s position and appropriately communicate with external auditors
— Have achieved an efficient cost of control
— All five layers of the COSO model are present and functioning
— Focus on communication between external and internal auditors

— Strong risk assessment that connects risks and audit assertions, leverages direct ELCs, and ultimately impacts control testing
— Management has full ownership of the risk assessment and scoping process

— Strong set of direct ELCs operating at a sufficient level of precision to act as the company’s “insurance policy”

— Focused on non routine, judgmental and complex areas
— Good alignment between the types of controls – preventative vs. detective and automated vs. manual
— Constant improvement in the design and automation of controls
— Reviews the total cost of control
Key Attributes of a Healthy ICOFR Program (cont.)

- Low number of spreadsheets and queries (i.e. key reports have been automated)
- Varying the nature, timing and extent of testing based on risk
- Use of data analytics and continuous monitoring
- Remediation efforts are prioritized and sustainable solutions are implemented
- Low level of deficiencies identified, significant deficiencies are rare
- Focus on tone at the top/culture
- Frequent training for process owners and control testers, to ensure controls owners understand their processes and test procedures
- Appropriate level of resources allocated
- Reports to the appropriate level within the organization

A clean control opinion does not necessarily mean that you have a good and healthy ICOFR program
## Assessing ICOFR Program Maturity

<table>
<thead>
<tr>
<th>Lower maturity</th>
<th>Higher maturity</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic Compliance Driven</strong></td>
<td><strong>Value-driven Culture</strong></td>
</tr>
<tr>
<td>Minimal effort to achieve ICOFR compliance</td>
<td>Integrated with ICOFR and other risk management and compliance efforts</td>
</tr>
<tr>
<td>Reactive to compliance demands</td>
<td>ICOFR supports the client’s broader corporate values and strategies</td>
</tr>
<tr>
<td>Defined external audit reliance and coordination strategy</td>
<td><strong>Identifies Emerging Issues</strong></td>
</tr>
<tr>
<td>Controls Not Aligned to Business</td>
<td>Technology-enabled risk assessment, driving alignment with enterprise risk assessment</td>
</tr>
<tr>
<td>Rolled forward, unchanging risk assessment</td>
<td><strong>Integrates with Enterprise</strong></td>
</tr>
<tr>
<td>External audit-driven risk assessment</td>
<td><strong>Risk and Control Advisor</strong></td>
</tr>
<tr>
<td>Risk-based scoping methodology, using quantitative and qualitative factors</td>
<td><strong>Efficient and Evolving</strong></td>
</tr>
<tr>
<td>Continuous identification and monitoring of risks related to external and internal changes</td>
<td><strong>Proactive Management of Root Causes</strong></td>
</tr>
<tr>
<td>Management actively utilizes testing, monitors ELCs for synergies with the control environment, and focuses on accountability</td>
<td><strong>Innovative and Aligned</strong></td>
</tr>
<tr>
<td>ELCs are not integrated with the control portfolio</td>
<td><strong>Unclear or Misaligned</strong></td>
</tr>
<tr>
<td>ELCs linked to financial reporting risk and COSO 2013 Principles</td>
<td>Testing standards exist but have not evolved (i.e. IPE, MRC, Third Party, etc.)</td>
</tr>
<tr>
<td>Alignment and annual evaluation of ELC coverage over COSO 2013 Points of Focus</td>
<td>Testing approach is based upon ICOFR risk and considers external auditor reliance to minimize the compliance effort</td>
</tr>
<tr>
<td>Reactive to changes in the corporate ICOFR program</td>
<td>Utilizes technology as a central repository for sharing ICOFR testing documentation and results with stakeholders</td>
</tr>
<tr>
<td>Increased focus on control enhancement including automated controls</td>
<td>Use of data analytics and subject matter professionals</td>
</tr>
<tr>
<td>Actively contributes control improvements as part of key business changes</td>
<td><strong>Fragmented Accountability</strong></td>
</tr>
<tr>
<td><strong>Unclear roles and responsibilities, resulting in inconsistent quality</strong></td>
<td><strong>Evaluating Results</strong></td>
</tr>
<tr>
<td>Program management structure in place, with an established schedule and budgetary framework</td>
<td>Exceptions are identified and tracked without resolution validation</td>
</tr>
<tr>
<td>Actively monitored and technology-enabled program management</td>
<td>Process is in place to monitor and communicate remediation progress</td>
</tr>
<tr>
<td>Organizational investments in controls-focused training programs and quality management for the ICOFR program and team</td>
<td><strong>Exception Scorekeeper</strong></td>
</tr>
<tr>
<td>Leadership advocates integration with and innovation from the ICOFR program supporting ethics and integrity</td>
<td>Business-owned resolution with enterprise-level communication</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Leverages ICOFR results to identify operational and organizational improvements</td>
</tr>
</tbody>
</table>

© 2016 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.
Understanding the controls portfolio can help an organization balance risk management and performance improvement forces.

Legislation has forced the pendulum toward the Risk Management axis.

Competition and market pressures are forcing the pendulum toward the Performance Improvement axis.
**Total Cost of Control**

**Control cost drivers:**
- Automation level
- Frequency of performance
- Duration of performance
- Level of staff performing the control
- Number of instances of control performance (number of locations and people that perform the control)
- Testing costs

**Cost of Control Components**

- Testing and Audit Costs
- Management Review
- Errors/Corrections/Turnover
- Performance

"Visible Costs" of Compliance

Typically organizations don’t consider “Hidden Costs” associated with control operation when calculating their cost of control.
The Controls Journey

Accountability

Maturity of Controls

Fragmented

Functional

Integrated

Embedded

Finance =
Compliance =
Operations =
Do you have a defined strategy for your ICOFR Program?

A company’s ICOFR strategy should be impacted by:

- Company Culture
- Economic Decisions
- Organization’s Risk Tolerance
Management of the Company is responsible for establishing and maintaining adequate internal control over financial reporting. The Company’s internal control over financial reporting has been designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with GAAP and includes those policies and procedures that:

— *Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the Company;*

— *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the Company are being made only in accordance with authorizations of management and directors of the Company; and*

— *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the Company’s assets that could have a material effect on the financial statements.*

*Excerpt from an Example 10-K*
SEC and PCAOB Conceptual Alignment

- Increased documentation levels
- Focus on C+A
- Precision levels
- Memos documenting positions
- Expectation that the auditor knows more than the company

Areas of tension/difference

Open dialogue to understand the “Whys”

- Fee Gap
- Expectation Gap
- Level of Effort Gap

Increased level of comment letters pushing for more disclosures
Creating Business Value

Operations

Conceptual Alignment

PCAOB

Areas of tension/ difference

SEC

ICOFR Program embedded in Operations

ACCOUNTING/ FINANCE

Increased Business Value

ACCOUNTING/ FINANCE

Lower Business Value

ICOFR Program driven by Accounting/ Finance

External Auditors

SEC Registrants

— Fee Gap
— Expectation Gap
— Level of Effort Gap

© 2016 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.
# Reliance should be a Deliberate Economic Decision

## Company’s Regulator

<table>
<thead>
<tr>
<th>SEC</th>
<th>Less Auditor Reliance</th>
<th>More Auditor Reliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>— No requirement to update formal walkthroughs or flowcharts on an annual basis</td>
<td>Level of detail in process documentation</td>
<td>Depth of Testing</td>
</tr>
<tr>
<td>— Management’s judgment plays a critical role in determining design of controls and how they are evidenced</td>
<td>More specificity around review controls</td>
<td></td>
</tr>
<tr>
<td>— More flexibility in determining how much to test and when</td>
<td>More testing later in the year</td>
<td></td>
</tr>
<tr>
<td>— No sample size requirements</td>
<td>Completeness &amp; Accuracy testing</td>
<td></td>
</tr>
<tr>
<td>— Completeness and accuracy should be considered by process owners when executing a control</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## External Auditor’s Regulator

| PCAOB | |
|-------| |
| — Understand the flow of information through updated narrative/flowchart information | Level of precision, documentation around what attributes are reviewed for vis-à-vis expectations |
| — Guidance around timing of testing (interim and rollforward) and sample sizes for each | Larger sample sizes, particularly for high risk controls and test procedures that dig deep (via firms’ methodologies) |
| — Completeness and accuracy testing on all key spreadsheets and system generated reports with stringent baseline approach or annual testing | |
Types of External Audit Coordination

Reliance to modify substantive approach

- Auditor places reliance on an effective control environment to lessen the amount of required substantive audit testing
- Need a strong control environment over time
- This approach may not work for all types of companies (e.g. newly public)
- Management may push reliance to reduce testing, and ultimately, audit fees.
- Controls alignment with auditor is not necessarily a key consideration

Use of the work of others

- Auditor relies on the control work performed by management (or 3rd party on behalf of management), with limited reperformance
- Reliance is based on control ratings
- May result in limited audit fee savings; however, management likely must comply with auditor’s sample sizes, testing & documentation requirements
- Controls alignment with the auditor is necessary for this method of reliance

Direct Assist

- A member of management (or 3rd party on behalf of management) serves as a resource reporting directly to the auditor to perform testing
- Resources utilized must be knowledgeable and competent
- A primary goal is to reduce auditor fees
- Controls alignment with auditor is not necessarily a consideration
“Allows for Management and the Auditor to have different testing approaches.”

“When more than one control exists and each adequately addresses a financial reporting risk, management may decide to select the control for which evidence of operating effectiveness can be obtained more efficiently.”

Two overarching principles in the guidance:

1. **Management should evaluate whether it has implemented controls that adequately address the risk that a material misstatement of the financial statements would not be prevented or detected in a timely manner.**
   a. No requirement to identify every control in a process
   b. No requirement to document the business process impacting ICOFR

2. **Management’s evaluation of evidence about the operation of its controls should be based on its assessment of risk – the nature and extent of evaluation procedures should align with those areas of highest risk to reliable financial reporting.**
   a. Test of Design - Documentation of the design of “key” controls is an integral part of reasonable support – the form and extent will vary depending on the size, nature and complexity of the company.
   b. Testing timeframe – Management’s evaluation would ordinarily consider evidence from a reasonable period of time during the year, including the fiscal year end.

Key Differences between Management’s Roles/Responsibilities vs. Independent Auditor’s

— Management is responsible for designing and maintaining ICOFR and performing an annual evaluation to support whether ICOFR is effective at year end.

— Management’s daily involvement with its internal control system provides it with knowledge and information that may influence its judgments about how best to evaluate ICOFR and the sufficiency of evidence it needs to assess its effectiveness.

— The independent auditor is responsible for conducting an independent audit that includes appropriate professional skepticism.

— The independent auditor integrates its tests of ICOFR with the financial statement audit.

— The independent auditor does not have the same knowledge and information as management.

— The nature and extent of the evidence supporting management’s assessment of ICOFR (including its documentation) will impact the efficiency of the audit.

— Higher risk areas – less ability for the independent auditor to use the work of others.

— Lower risk areas – opportunity to use the work of others is maximized.
Control Selection and Alignment

- Company’s informal ICOFR testing—newly acquired BU’s, high growth BU’s
- Company’s universe of all internal controls – ICOFR and other
- External Auditor’s key control population for integrated testing
- Company’s key control population for ICOFR testing
- Alignment is modified for each Company based on the Company’s strategy
Differences in Controls - Management vs. Auditor

**Independent Auditor**
- Review of Financial Reporting
- Assessment of GAAP application

**Management/IA**
- Financial Reporting RA
- SOX Control Testing
- Corporate Governance
- Efficient Business Operations
- Compliance – Regulatory & Organizational
The Importance of Control Substructure

Is your ICOFR program structured to function as intended and reduce misstatements?

- Do you understand what could cause the 10-20 most critical controls to fail?
- Are those controls robust enough and working effectively?
- If you still have control failures – have you examined your control substructure recently?
Inherent Risk Assessment
Identify risks to financial reporting elements considering qualitative and quantitative factors. Map identified risks to financial statement assertion level.

Entity level Control ("ELC") Review and Assessment
Evaluate high-level company-wide controls including the strong direct ELCs that act as the Company’s ‘insurance policy’.

Residual Risk Assessment
Evaluate the design and precision of entity level controls and determine remaining financial statement assertion risk.

Controls Rationalization/Key Control Identification
Identify relevant monitoring and process-level controls based on level of residual risk.

Testing Approach
Develop testing approach which is generally a combination of entity level and process-level control.

Control framework to make certain adequate ICOFR are in place.

There must be a linkage between the risk assessment and the selection of controls to ensure the right controls are tested.
ICOFR testing addresses a small set of the overall control universe. A risk-based Internal Audit function can provide coverage in remaining key areas.

The bulk of ICOFR testing is focused in this relatively small section of the COSO cube. Risks that should be addressed in the remaining universe may be covered by Internal Audit.
Evolution from Pure ICOFR to IA

- Identification of financial risk areas, documentation of controls and stabilization of control environment
- SOX Compliance, improved governance structure, remediation and control optimization
- Broader risk assessment, process improvement integration and focus on value creation audits
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 on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2016 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.

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