RISK: IT’S MORE THAN JUST COMPLIANCE

Rhode Island Annual General Meeting

May 15, 2014
AGENDA

■ Thinking Beyond Compliance

■ Expanding How We Look at Risk

■ Assessing, Quantifying, & Accepting Risk

■ Are We a Risk?
WHAT ARE WE GOOD AT?

Producing detailed assessments of compliance with rules and regulations

What’s the criteria?

What is the Auditee Doing?

We use the gap to develop our recommendation
LANDING IN OZ

There are no rules or regulations
HOW DO YOU IMPOSE COMPLIANCE STANDARDS ON CONGRESS?

- Congress not bound to follow most statutes
- Separation of Powers Barrier
HOW DO YOU IMPOSE COMPLIANCE STANDARDS ON CONGRESS?

• You Don’t

• You re-craft your argument in terms they understand:
  • RISK
QUESTION

When doing a compliance audit, do our auditors really understand the underlying reason they are performing certain compliance steps

OR

Are they checking off a box on their checklist?
ARE WE SUFFERING FROM COMPLIANCE MYOPIA?

The Risk of the Checklist
ARE WE GETTING TO THE ROOT CAUSE?

Traditional Reasons for noncompliance with rules/regulations:

- Tone at the top
- Poor documentation
- Poor communication
- Inadequate training

But are we so focused on the rules that…
…ARE WE ENFORCING COMPLIANCE WITH OUT-OF-DATE CONTROLS?

Have controls kept up with changes in:

- Technology
- Process
- Organizational structure
- Management priorities
- Evolving risks
EXPANDING HOW WE LOOK AT RISK…

QUESTION

Don’t we already do Risk-based auditing?
Relevant Standards all Require an Understanding of Risk

COSO's Internal Control – Integrated Framework

COBIT for Risk

Statement on Auditing Standards (SAS) Nos. 104-111
- Commonly referred to as the "Risk Assessment Assessment Standards".
- For audits of financial statements for periods beginning on or after December 15, 2006

IIA Practice Advisory 2120-2: Managing the Risk of the Internal Audit Activity (April 2009)

IIA Practice Advisory 2120-3: Internal Audit Coverage of Risks to Achieving Strategic Objectives (June 2013)
TYPES OF RISKS

Think both broad and deep

Strategic Risks
Operational Risks
Financial Risks
Regulatory Risks
Reputation Risks
Credit Risks
Audit Risks
DEFINING RISK

“The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).”
~ Wikipedia

“A situation involving exposure to danger”
~ Oxford Dictionary

“ Possibility of loss or injury”
~ Merriam Webster Dictionary

“ Possibility than an event will occur and adversely affect the achievement of objectives”
~ COSO

“The chance that an investment’s actual return will be different than expected.”
~ Investopedia

The effect of uncertainty on objectives
~ ISO 31000
“WE DON’T KNOW WHAT WE DON’T KNOW…”

Donald Rumsfeld, Secretary
US Department of Defense
WHAT KEEPS YOUR AUDITEE UP AT NIGHT?

Talk to the people!  
Talk to the Board  
Talk to Management  
AND the people that do the work

View yourself as the “Trusted Advisor”

Make sure your people build relationships too
IMPACT ON AUDIT VALUE

When we don’t understand our organizational priorities, we:

Provide recommendations with limited value

Ultimately damage trust and relationships by:

- Showing lack of understanding of our stakeholders' priorities and challenges
- Providing lack of quality assessments/value to leadership

Miss the opportunity to make meaningful change
STRATEGIC RISK: ARE WE LOOKING AT RISKS THAT ARE AHEAD OR BEHIND US?

Bayonetting the Wounded…
HOW DO YOU (OR YOUR ORGANIZATION) VIEW RISK MANAGEMENT?

Compliance Exercise?  Strategic Tool?
STRATEGIC RISK: DO WE KNOW WHERE OUR ORGANIZATION IS GOING?

To remain relevant, audit recommendations must be:
Timely
Proactive

…And reflect an understanding of:
The organization’s strategic vision, mission, and objectives
Risks and priorities of key stakeholders
Industry best practices
STRATEGIC RISK: WHERE CAN WE IMPROVE?

Think Big Picture!

Providing risk-based frameworks for management and leadership action:

• Systems and technology

• Organizational transition/ change

• Big Picture View of risk across stakeholders
QUESTION

What is the acceptable level of Risk in your organization?

If you know, does everyone else know and can it be quantified?
RISK TOLERANCE AND ACCEPTANCE

- If risk is not quantified, it is subject to interpretation
- What is a High, Medium, Low Risk?
- Use Quantitative and Qualitative measures
- Make sure you explain to your staff what is acceptable!
- Be Suspicious of the Status Quo (In a world of constant change, risk changes, too!)
- Relying solely upon “I know a High Risk when I see it” is risky!
KEY CONSIDERATIONS IN SETTING RISK APPETITE

- Risk appetite must be linked to business strategy and objectives.
- Setting risk appetite requires extensive judgment on the part of the board (or other governing body) and executive management. One size does not fit all.
- Assigning clear ownership of risk at the management level is essential. Although the board sets risk appetite, its execution cascades down and is managed by all.
- Communication is a key enabler. Collaboration at all levels is critical.

Reference:

Cambio Consulting Group
# QUANTIFYING RISK

## Risk Assessment Model

<table>
<thead>
<tr>
<th>Assessment Criteria 1 (Risk Driver)</th>
<th>Assessment Criteria 2 (Risk Driver)</th>
<th>Assessment Criteria 3 (Risk Driver)</th>
<th>Assessment Criteria 4 (Risk Driver)</th>
<th>Risk Score</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial</strong> - Risk of Material Financial loss or Mis-statement</td>
<td><strong>Technology</strong> - Risk of exposure to security vulnerabilities or system failure</td>
<td><strong>Operational</strong> - Risk of operational failures including inefficiency and ineffectiveness</td>
<td><strong>Customer</strong> - Requested by Management or CHA</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Driver Weight</th>
<th>3</th>
<th>5</th>
<th>4</th>
<th>2</th>
<th>Notes</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Planned Audits</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement Audit</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>3</td>
<td>40</td>
<td>Based upon Risk Assessment, this should be the third priority</td>
</tr>
<tr>
<td>Asset Inventory Audit</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>Accounts Receivable Audit</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td><strong>Proposed Audits</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Asset Tracking Audit</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>38</td>
<td>Based upon Risk Assessment, this should be the second priority</td>
</tr>
<tr>
<td>ERP Security Audit</td>
<td>5</td>
<td>5</td>
<td>3</td>
<td>1</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>Asset Disposal Audit</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>Accounts Payable Audit</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>34</td>
<td>Based upon Risk Assessment, this should be the top priority</td>
</tr>
<tr>
<td>Firewall Security Audit</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>56</td>
<td></td>
</tr>
</tbody>
</table>

Risk Driver Weight = Between 5 and 1 with 5 being most significant

Ranking Scale - 5=HIGH, 3=MEDIUM, 1=LOW

---

[ISACA Logo]
WHO’S ASSUMING YOUR RISK?

Improper assumption of risk

- Ensure risk is being assumed at the right level
WHAT IS YOUR RISK APPETITE?

Would you bet $1 at 2 to 1 odds in your favor?

Would you bet $500,000 at 2 to 1 odds in your favor?

Would you bet $500,000 at 1.1 to 1 odds in your favor?

Risk appetite for:
- A particular project/initiative
- Your Organization

How might these differ, and why?
ARE WE A RISK?

- Are we keeping up with change
- Do we have the right people?
- Are our reports effective?
GETTING OUT OF THE “RUT” OF CYCLICAL AUDITING

Do things change in your organization?
If so, shouldn’t your audits change as well?
CHANGE IS THE NEW “NORMAL”

When developing your plan and audit work, consider-

Changes in Regulation
Changes in Technology
Changes in Processes
Changes in Vendors/Suppliers
Changes in People
LEVERAGE PAST WORK - CAREFULLY

Ask “Why are we doing this audit?”
Don’t just dust-off the prior plan and redo the same audit!

Sometimes it is appropriate to do a follow-up audit but where does it stand based upon RISK

Don’t just redo an audit because “it’s been a while” or we do this audit “every couple years”

Re-assess the risks!
ARE YOU FIGHTING WITH THE TROOPS YOU HAVE OR THE TROOPS YOU NEED?

If not, what are you doing to change that?

Remember – not having people with the right skills increases audit risk…
AUDIT TEAMS THAT REDUCE RISK – DIVERSITY OF THOUGHT

Are we hiring “Mini-Me’s”?

- Extrovert vs Introvert
- Big Picture vs Details
- People vs Process
- Structure vs Flexibility
QUESTION – WE NOW UNDERSTAND RISK, BUT…

Is anybody reading our reports?!?!?
ARE OUR REPORTS EFFECTIVE?

Who are we writing our reports for?

Reports must be audience focused

- Executive level - A Bigger Picture is Required (Think PowerPoint)
- Line Manager – Technical Details (NFRs)
DO WE ADD VALUE?

Bottom Line:

If it weren't for fear of appearance, would leadership consider cutting my department during lean times?

Would they be right to do so?
What can I do today to (better) incorporate Risk Based auditing into my organization?
POINTS TO REMEMBER

- Understand your Organization and its operating environment - make sure your people do too!

- Always re-assess risk and move away from periodically doing the same audits over and over (obviously not the case if required by regulation, etc.)

- Quantify and communicate Risk levels and what is acceptable Risk tolerance. Make sure everyone is on the same page.
POINTS TO REMEMBER

- Assess the risks of not having the right people and skills in your organization and mitigate as necessary.

- Be cognizant of changes in regulation, technology, processes, and people.

- Let the Risks drive your strategy, planning, and execution.
CONTACT INFORMATION:

Theresa (Terry) Grafenstine
CPA, CISA, CIA, CGEIT, CRISC, CGAP, CGMA
Inspector General
U.S. House of Representatives
202.226.1250
Theresa.Grafenstine@mail.house.gov