Transitioning from Risk Based Auditing to Enterprise Risk Management Auditing

Hosted by the Dallas IIA Chapter

Presented by
Raven Catlin
Raven Global Training
Raven Catlin, CPA, CIA, CFSA, CRMA

Call me: 571-283-1878
Email me: raven@ravenglobaltraining.com
Check out www.ravenglobaltraining.com
LinkedIn.com/in/ravenhenderson
Twitter: @raventraining

Providing training services to corporations, not-for-profits, associations, including the IIA since 2001
At the end of this session, you will be able to …

- Explain the difference between Risk Based Auditing (RBA) and Enterprise Risk Management Auditing (ERMA)
- Sell the Board, Management, and Auditors on the need to transition to ERMA
- Create a transition plan towards ERMA
• **2010.A1** – The internal audit activity’s plan of engagements must be based on a risk assessment, undertaken at least annually.

• **2120.A1** – Based on the results of the risk assessment, the internal audit activity must evaluate the adequacy and effectiveness of controls encompassing the organization’s governance, operations, and information systems.
What is your purpose?
Leverage the good things that management is already doing
Save time by communicating what “they” don’t already know
Great assurance on the management of risks
Reduce audit fatigue
Less testing for auditors
Better coordination with other assurance functions
More collaboration with management

**BENEFITS OF ERMA**
IIA Support of ERMA

- Creating a foundation for audit judgments based on organizational strategy and objectives, risk appetite, and governance maturity.
- Developing an assurance framework for assessing the adequacy of ERM and governance activities.
- Synchronizing the auditor’s tolerance for risk with management’s tolerance for risk rather than focusing solely on the former as in prior audit methods.
- Emphasizing the critical need to base performance measurements on what will provide real incentives to accomplish organizational objectives.
- Focusing on the organization’s future capability to assess and manage risk rather than on just its historical risk response track record.

© 2014, Raven Global Training / Raven Catlin

IIA CIA Part 2-Section I: Managing the Internal Audit Function (Kindle Locations 1641-1642)
What Does RBA Look Like?

Gather Information → Perform Data Analytics → Identify Business Objectives → Identify Risks

Adequately designed?

YES → Identify Controls

NO → Risk based Finding → Pass/Fail?

FAIL → Risk based Finding

YES → Design Tests of Controls / Attribute Test

PASS → Give client a hi-five

NO → Risk based Finding

PASS → In Scope?

FAIL → Risk based Finding

YES → Assess Inherent Risk Impact & Likelihood

FAIL → Risk based Finding

PASS → Substantive Testing?

FAIL → Risk based Finding

YES → Pass/Fail?

FAIL → Risk based Finding

YES → Risk based Finding
“The **degree of probability** that an **event** will significantly impact a functional area’s ability to meet the organization’s objectives”
Risk: Types and Assessment

What types of risk are there?
- Inherent
- Residual

How do we assess risk?
- Impact
- Likelihood
- Velocity
- Persistence
Assessing the Risks

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Insignificant Wouldn't Blink</th>
<th>Minor Flinch</th>
<th>Moderate Ouch Bearable</th>
<th>Major It’s Broken Excruciating</th>
<th>Catastrophic Earth Shattering Shut-down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Almost Certain</td>
<td>Yellow</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Certain Definite</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Likely Probable</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Impending</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Possible</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Unlikely Doubtful</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Rare Remote</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Once in a lifetime</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>
Challenges of ERMA

- Defining the expectations
  - Board
  - Management
  - Regulators
- Defining best practice
- Risk Management Fatigue
- Fragmented and silo-ed
  - Risk teams
  - Risk information
ERMA is Not

- Just auditing the ERM process
- Dependent on a defined ERM process
- Auditing all risks
- Auditing all controls
- Founded on substantive testing
ERMA

Start with organizational objectives
Then assess the “Internal Environment”
Then we identify and assess risks
Next we look at how management is responding to those risks to determine what we audit
- Take risks
- Terminate risks
- Transfer risks
- Treat risks
Next, we assess management’s response
Finally, we make sure management is managing
How Do You Know if Management is Managing

- Plan
- Organize
- Direct
- Control
- Risk Appetite
- Risk Tolerance
- Key Performance Indicators
- Key Risk Indicators
- Management Reports
- Dashboard Reports
- Balanced Scorecard

© 2014, Raven Global Training / Raven Catlin
Other Noteworthy Challenges

Sell" ERMA to the audit committee, senior management, line management, and other auditors

Can I start an ERMA audit

And decide not to “finish” it?
And decide not to do any testing?
And not test every control?
And not reporting every issue?
Setting the Scope

- Define the audit
- Look for related audits
- Determine audit intensity
- Assess reliance on entity level controls
- Consider use of technology / CAATs
- Rank and prioritize risks and controls
- Discuss with audit management
- Go / No Go decisions
- Types of audit tests
- Sampling method
- Budgeted hours and costs
Identify Management’s Controls

- Categories
- Experience
- Guidance material
- Other risk and control matrices
- Risk examples for others in industry
- Team effort
- Interviews / walkthroughs
- Process maps / flowcharts
- ICQs / Surveys

© 2014, Raven Global Training / Raven Catlin
## Process Step vs. Control Objectives

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tasks</td>
<td>• Authorization</td>
</tr>
<tr>
<td>• Activities</td>
<td>• Accuracy</td>
</tr>
<tr>
<td>• Must be done to complete the process</td>
<td>• Completeness</td>
</tr>
<tr>
<td></td>
<td>• Existence</td>
</tr>
<tr>
<td></td>
<td>• Valuation</td>
</tr>
<tr>
<td></td>
<td>• Classification</td>
</tr>
<tr>
<td></td>
<td>• Timeliness / Cutoff</td>
</tr>
<tr>
<td></td>
<td>• Segregation of Duties</td>
</tr>
<tr>
<td></td>
<td>• Safeguarding Assets</td>
</tr>
</tbody>
</table>
Types of Audit Tests

- Design only (no control testing)
- Interviews only (must corroborate)
- Procedural review (not representative)
- IT testing (analyze files, screens, procedures, logs, and audit trails)
- Tests of controls
- Substantive tests
- CAATs
Evidence Criteria

- **Sufficient**
  - 100% testing
  - Sampling
  - How much is enough?

- **Competent**
  - Trustworthy & believable

- **Relevant**
  - Related to the audit
  - Related to the testing objective
Testing other controls

1st you must know a deficiency is still a deficiency even if a compensating control is present

Test complementary and compensating controls as needed to assist with deficiency assessment

Redundant controls are “redundant”
Questions?

Raven Catlin  raven@ravenglobaltraining.com
DC Metro 571-283-1878  www.ravenglobaltraining.com
LinkedIn.com/in/ravenhenderson

Twitter: @raventraining