It’s a Risk Based Dinner Gathering – Compliance, ERM & Internal Audit

SCCE 18th Annual Compliance & Ethics Institute – September 15-18, 2019

Who We Are

Stephanie Kandel
Director, Compliance & Risk Management
AARP Services Inc.

Ryan Abdel-Mageid
Director, Internal Audit
AARP

Joe Pugh
Enterprise Risk Management & Compliance Director
AARP
We will illustrate the importance of Compliance, Internal Audit and ERM integration using two versions of the same event:

**Scene 1:** Dysfunctional

**Scene 2:** Optimized

### Polling Question #1

Which best describes your industry affiliation?

1. Not-for-Profit
2. Government
3. Financial Services/Banking
4. IT/Communications
5. Other
Polling Question #2

Which best describes your role?

1. Compliance / Ethics Professional or equivalent
2. Internal / External Audit Professional or equivalent
3. Risk Management Professional or equivalent
4. All three
5. Other

Polling Question #3

Which one of these best describes Risk Management, Compliance, and Internal Audit at your organization?

1. Integrated
2. Siloed
Polling Question #4

Which is your favorite?

1. Ice cream
2. Cookies
3. Candy
4. Cocktails

Scenario Background

• Fictional third-party experiences data breach
• Potential exposure of member/customer data
• Illustration of how Compliance, Internal Audit and ERM interact during a risk event
- Scene 1 -

*Dysfunctional*

![Image of a dysfunctional scene]

**Dialogue:**

**Man:** Yeah if you could just tell me what's going on.

**Man:** That would be great.
Poll:
Which line of defense is accountable for this breakdown?
A Dinner Gathering Requires Coordination
- *so does a strategic risk process*

- Connecting the dots
- Assessing risk earlier with a cadence
- Multiple inputs
- Formalized touchpoints between functions to enhance collaboration

![Risk-listing process](X) ![Risk-informed decision making](✓)

Compliance, Audit, and Risk Management
- *everyone needs a plate and napkin*

- ERM sets the table:
  ✓ Common risk assessment
  ✓ Taxonomy
  ✓ Rating scales
  ✓ Risk language

- Compliance and Audit have a seat at the table:
  ✓ Audit – Knowledge of control activities
  ✓ Compliance – Broad scope and unified view of regulatory risks
ERM – How it Works

**Identify using multiple inputs:**
- Strategy/innovation discussions
- Internal Audit collaboration
- Compliance & IT risk assessments
- Questionnaires/surveys
- Environmental scans
- External sources like Gartner/CEB, KPMG, Grant Thornton, industry networking groups

**Assessment criteria based on:**
- Impact - If this risk event were to materialize, what would be the impact on the organization?
- Likelihood - What is the likelihood this risk event will occur?
- Velocity - If this risk event were to materialize, how rapidly would it impact the organization?
- Mitigation Effectiveness - How well the risk is being managed; how much risk remains

Mitigation efforts are developed by risk owners that are supported by defined plans to reduce risk exposures and manage risks. The Executive Team meets routinely to discuss changes in risk (either new emerging risks, or the escalation/reallocation of existing risks) and the mitigating activities.

Internal Audit includes the key business processes for mitigating enterprise risks in the annual audit plan. Ongoing, the risks are monitored against the top risk areas as reported in the external environment as well as the not-for-profit sector which can influence the organization’s risk posture.

Formal risk reporting includes the risk heat map and risk scorecards. Reporting is ongoing to reflect risk changes in the risk profile that is provided to the Executive Team who holistically and routinely discuss results that are reflected on a risk heat map.

Board Committees have been assigned jurisdiction for oversight of each of the key risks, and discussions about Tier 1 risks are embedded within the meeting agendas, including the risk scorecards.

**A Buffet Style Risk Menu**

**Enterprise risk**

**Linked to Compliance**

**Information Security/Privacy Risk**

<table>
<thead>
<tr>
<th>Category: Information Technology</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security - The organization faces a significant and publicized security risk - Unexpected/unauthorized use or sharing data results in ………..</td>
<td></td>
</tr>
<tr>
<td>Residual Risk</td>
<td>Likelihood</td>
</tr>
<tr>
<td>Major</td>
<td>Likely</td>
</tr>
</tbody>
</table>

**Key Mitigation Efforts**

- Information Security Efforts
  - Detective controls have been …………..
  - Prevention mechanisms have been instituted to reduce the risk of unauthorized access and threats …………..
  - Developed programmatic themes to strengthen overall security risk posture and………..
  - ETC.

- Privacy Efforts
  - Monitoring potential legislative and regulatory efforts and proposals in a rapidly changing environment.
  - Timely counseling and compliance advice …………..
  - ETC.

**Key Takeaways**

- During the last quarter, the trend of breaches or material vulnerabilities that may have impacted the global threat landscape have remained steady and consequently, the Risk Outlook rating remains “Stable.”
- One year after new GDPR has been in effect, regulators (European and US) has had data breaches, e.g. $53m against Facebook authority (CNIL) fined

**Key Risk Indicators**

- Monitor the degree of …………..
- Measure incident response …………..
- ETC.

Internal Audit’s smorgasbord for control and processes testing
Keys to Better Risk Coordination

- Starts with strategy
- Shared risk language/approach/rating criteria
- Accountability/risk owners
- Multiple risk inputs to inform the risk profile
- Coordinated and aligned board reporting
- Annual audit plan aligns with the risk profile

Internal Audit Plan – Strategic Risk Alignment

- Compliance and Risk Management are often mentioned in the same breath
- Just because you have structures in place to manage your organization’s regulatory compliance, does not necessarily mean you are effectively managing risk, especially at the enterprise level
- High-functioning IA groups are developing forward-looking audit plans that evaluate both current and planned operations
- Internal Audit Plans that do not incorporate ERM inputs are likely not focused on the most significant risks
Two of the most important inputs when developing your organization’s IA plan:

1) Strategic plans/goals & supporting initiatives

2) Enterprise Risk Assessment results

Where are we trying to go?  What could prevent us from getting there?
Compliance Inputs to Risk Assessment

- How can compliance minimize the risk of failure?
- Recent examples:
  - Tone at the top
  - Problematic incentives for sales team
  - Cost-cutting efforts trump safety
  - Potential conflicts of interest
  - Failure to monitor 3rd party data

Federal Sentencing Guidelines – Compliance Risk Assessment

“(c) In implementing subsection (b), the organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in subsection (b) to reduce the risk of criminal conduct identified through this process.”
Compliance Inputs to Risk Assessment

Risk Assessment Focus:
- Legal and regulatory risks
- Ethical misconduct risk
- Policies

Testing

- Regular testing and validation of incident response/crisis management plans
- Perform tabletop exercises
- Make it engaging and fun!
- Scene 2 -

*Optimized*
Contact Information

skandel@aarp.org

rabdelmegeid@aarp.org

jpugh@aarp.org