Dynamic audit management

IIA Aksarben Chapter April Meeting
Presented by KPMG and Mutual of Omaha
Jason Coyle – Director of Internal Audit (Mutual of Omaha)
Sean Winekauf – Director (KPMG)
Anna Shimerda – Manager (KPMG)

April 27, 2016
Agenda

— Existing challenges
  — Audit universe
  — Risk assessment methodology
  — Emerging risks/Monitoring
  — Audit plan

— GRC solutions

— Examples/Takeaways
Existing challenges
Overview - Challenge

Many organizations have multiple functions that address some aspect of risk management. Unfortunately, these efforts are often poorly coordinated, creating silos of important risk information. Attempts at bringing these practices together to provide a comprehensive view of risk often backfires as various risk managers struggle to conform to the common framework.

Leading practitioners find a healthy balance between creating standardized processes and frameworks to provide consistency within the risk management process and maintaining a necessary level of flexibility to ensure that the ERM process remains dynamic and open to professional judgment.
Trends in internal audit

Integrated Assurance and Risk Coverage

Risk Assessment and Planning

Technology

Enhanced Reporting

Challenges

- Talent management – skills of internal audit
- Expectations gap – stakeholders and IA
- Push to more sophisticated data and analytics
Value of internal audit

1. Provide actionable insights into the strategic value and risk drivers of the business

2. Align assurance coverage against strategic imperatives and extended enterprise risk

3. Optimize assurance coverage by mapping and integrating assurance coverage on a risk-adjusted basis

4. Continuously identify and assess emerging risks while monitoring key risk and performance indicators in addition to control coverage and performance

5. Facilitate data-driven decisions that optimize both business performance and risk mitigation

Value proposition
Making the value real

What insights do companies receive from their IA today; what insights would be of most value?

<table>
<thead>
<tr>
<th>Insight</th>
<th>Receive today</th>
<th>Most valuable to receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help assessing risks and risk management practices today</td>
<td>22%</td>
<td>51%</td>
</tr>
<tr>
<td>Informed perspective on emerging risks</td>
<td>5%</td>
<td>36%</td>
</tr>
<tr>
<td>Focus on sustainable profit generation</td>
<td>33%</td>
<td>41%</td>
</tr>
</tbody>
</table>

Source: Seeking value through Internal Audit, KPMG International, 2016
Risk assessment methodology

Who is involved in the risk assessment process?

How are companies standardizing enterprise rating scales?

What comprises the risk assessment rating? (i.e. likelihood, impact, velocity)

Are risk assessment results being shared between audit, risk and compliance?

How does IA add insight and bring business value?
In order to be effective, Risk Management must be a continual process that informs business decision making. Measurement of risk alone is not sufficient.
The implementation of a practical and sustainable risk management framework needs to be a combination of ongoing processes that are built into key decision-making activities, enhancing the governance structure and improving accountability through oversight and monitoring.

The primary activities include:

- Risk identification and assessment on a timely and consistent basis including risk prioritization based on impact, likelihood and management effectiveness

- Analyzing key business risks to understand their potential impact at both an aggregate and sub-risk (event) basis

- Identification of current risk mitigation/response capabilities, gaps to achieve future organizational objectives and the cost/benefit of enhancing capabilities

- Enhancing key risk management activities to improve decision-making and prioritize activities to support the accomplishment of strategic objectives

- Ongoing monitoring and oversight by Committees, Management and the Board of Directors, on a consistent and timely basis
What are emerging risks?

Emerging Risks are unknown/unanticipated, developing or changing risks in the early stages of becoming known that may have a major impact on a company’s ability to meet its strategic objectives.

Emerging Risk Characteristics

— High Uncertainty – little information, impact & likelihood difficult to assess
— Difficult to Identify & Quantify – slow to appear
— Conceptual (vs. Factual) in Nature
— Communication is Difficult – phantom risks, cry “wolf”
— Industry Position – no one wants to make first move
— Regulatory Involvement Required
Taking a new approach to risk

How strongly do companies agree or disagree that their IA function adequately identifies and responds to their emerging risks?

Source: Seeking value through Internal Audit, KPMG International, 2016
Key principles of a KRI/KPI framework

In designing a robust and sustainable KRI/KPI framework, KPMG references principles it believes to be paramount.

- KRI is directly related to the measurement of a risk within the defined risk appetite OR measures whether risks taken are outside defined risk appetite
- Supports the organization in determining risk levels at several layers of aggregation
- Calibrated through review of RCSA and Loss Data
- Linked to an annual process with the business to ensure that KRI framework is aligned with business strategic direction and risk strategy
- Key risks are identified
- Identified risks are measurable
- Identified measurable risks are judged by severity and dependencies on or to other development goals
- Reports and aggregation levels differs by recipients
- Board-level, management level, business-level, etc.
- Monitored, reported and actionable by different groups/audiences
- Empirically justifiable (loss data/scenario)
- Trigger scenario design/testing
- Measurable on multiple levels/layers
- Thresholds/Triggers are set in accordance with the defined risk appetite
- Thresholds/Triggers are calibrated using loss data, near miss and scenarios analysis, including external events
- Predictive
- Detective
- Indicative
Internal audit plan components

The internal audit plan is based on the risk portfolio identified during the risk assessment and validated by management. In an effort to help clients prioritize limited resources, the audit plan is structured over three years. In each year, there is a mix of risk-based internal audits, Sarbanes-Oxley Section 404 (SOX) Compliance assistance and continuous monitoring. We also include an estimate of the number of hours each audit may take.

— Risk-based Internal Audits

— Sarbanes-Oxley Compliance

— Continuous Monitoring

— Required Audits
Evaluation of audit plan

- Process/IT: 35%
- Value-added: 29%
- Monitoring: 12%
- Admin/Start-up: 0%
- SOX-related: 24%

Process/IT: 24%
Value-added: 0%
Monitoring: 13%
Admin/Start-up: 12%
SOX-related: 22%

Meetings: 31%
Reporting: 22%
Training: 15%
Planning: 8%
Start-up (200X): 13%
GRC solutions
Enterprise Governance, Risk and Compliance (GRC) considerations

1. GRC Vision
2. Guiding Principles
3. Executive Buy-in
4. Functional Commitment
5. Roadmap
6. Link between Business Requirements and Business Process Design
7. Requirements to System Mapping/Proof of Concept
8. Data Conversion
10. GRC Business Case Development
11. Tool Selection, RFI/RFP
12. Vendor Demonstrations, RFP Scoring

Convergence & Foundational Elements

Program Management

Enterprise GRC Considerations Components

Strategy

Technology Enablement

Vendor Selection

People & Change

— Foundational Elements
— Future State Process Flows
— Convergence Opportunities, Alignment of Shared Functionality, and Integration Points with GRC Tool
— High-level Business, Functional, and Technical Requirements Definition

— Project Governance
— Project Plan, Timeline and Budget
— Project Risks/Issue Tracking
— Project Resource Management

— Stakeholder Analysis
— Roles and Responsibilities
— Communication Plan
— Learning, Development and Training
— Adoption Plan/Roll-out
Examples/Takeaways
Taking a new approach to risk

How should IA evolve?

Become more diversified: skills

- Become more diversified: activities

- Become more proactive:
  - with stakeholders
  - as a function

Be able to match the sophistication/complexity of the audit targets

Source: Seeking value through Internal Audit, KPMG International, 2016
Leading practices - Conceptual framework

**Positioning** – Is Internal Audit strategically positioned to achieve its mission and objectives (as defined by the Board and management), and is IA viewed as a valued contributor to business strategy and performance.

**People** – Does IA have the right people strategy to successfully deliver on its mission/objectives.

**Processes** – Is IA’s processes efficient, effective and aligned with the organization’s strategy.
Leading practices - Process

- Leveraging Technology
- Dynamic/Continuous Risk Assessment
- Management Control Awareness Ratings
- Other “Process” Leading Practices
Leading practices - People

- PMO within Internal Audit
- IT Audit Complement
- Offshoring
- Use of Subject Matter Professionals
- Other “People” Leading Practices
Leading practices - Positioning

Internal Audit Strategy

Integrated Assurance/Risk Convergence

Knowledge Sharing

Other “Positioning” Leading Practices
Integrated audit approach

Operationalize into repeatable and sustainable analytics

Data & Analytics-enabled Internal Audit

Analytics-Driven Continuous Risk Assessment

Dynamic Audit Plan

D&A Audit Scoping and Planning

D&A enabled Audit Workplan

Enhanced Dynamic Reporting

Business Monitoring
Thank you

Jason Coyle (Mutual of Omaha)
Director of Internal Audit
Mutual of Omaha Plaza
Omaha, NE 68175
402.351.8763
Jason.coyle@mutualofomaha.com

Sean Winekauf (KPMG)
Director
1212 North 96th Street, Suite 300
Omaha, NE 68114
402.661.5205
swinekauf@kpmg.com

Anna Shimerda (KPMG)
Manager
1212 North 96th Street, Suite 300
Omaha, NE 68114
402.659.0245
ashimerda@kpmg.com
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. NDPPS 561027

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