BUILDING THE INTERNAL AUDIT FUNCTION OF THE FUTURE

IIA CHICAGO CHAPTER 59TH ANNUAL SEMINAR 2019
Agenda

- Presenter Bios and Session Objectives
- Background
- Agree on Risk Assessment Approach / Framework
- Execution
- Plan Development
- Q&A
Presenter Bios

Elizabeth Truelove McDermott, Northwestern Director of Internal Audit
etm@northwestern.edu | o: 847.491.4956

- Leads Northwestern’s internal audit program.
- Provides audit leadership in the development, operation and evaluation of the University’s enterprise risk management program.
- Masters of Business Administration from Keller Graduate School of Management, earned her bachelor’s degree in business from Bradley University and is a CPA.

Matt Booth, PwC National Higher Education Risk Leader, Internal Audit Partner
matt.booth@pwc.com | c: 312.802.9737

- Leads PwC’s Higher Education Internal Audit Practice and ensures Higher Ed Internal Audit institutions across the nation have access to the knowledge, tools and skillsets to address their unique challenges.
- Has led clients through a wide variety audit of projects, including comprehensive Enterprise Risk Management assessments.
- Bachelor’s in Business Administration from the University of Iowa, earned his Masters in Business Administration from the University of Chicago, and is a CPA.

John Powers, Director
john.powers@pwc.com | c: 608.628.4162

- Lead engagement director on nationally ranked research university internal audit engagements; responsible for coordinating subject matter specialist involvement, quality assurance, and bringing new ideas, technology, and processes.
- Has delivered internal audits on a wide variety of industry risks, including sponsored award and research compliance, institutional data reporting, data privacy and security.
- Bachelor’s in Business Administration from the University of Wisconsin — Madison in Risk Management and Insurance, and Accounting Information System and is a CPA.
Objective

Share leading practices on coordinating ERM, Compliance and Internal Audit risk assessments to provide coordinated risk coverage, reduce potentially duplicative work and maximize stakeholder benefit.
Background
Internal Audit

Objectives:
Responsible for providing an independent periodic assessment of the risk management and internal control systems to the Board and organizational leadership.

Role in the Risk Assessment Process:
During the risk assessment, Internal Audit works with other assurance functions to develop a common set of high-level risks. The risk assessment focuses on strategic, financial, operational, legal, compliance, and reputation risk.

1. Understand the strategic goals and identify auditable areas
2. Gather information to identify risks
3. Develop risk universe and evaluate and prioritize risks
4. Link risks to auditable units and ERM categories
5. Develop and communicate the risk-based audit, ERM, and compliance activities
6. Ongoing risk assessment and responsive activity updates
ERM

Characteristics

• ERM takes a broad, strategic approach to managing risk at all levels of an organization and is generally responsible for providing risk management structure and oversight to the business.

• ERM programs often function as standard setters for risk management activities and leave much of the process implementation to business functions. An ERM value proposition has to be simple—and it has to be powerful enough to drive functions to want to use risk management methodologies.

Objectives

• Provide timely and comprehensive risk reports to business decision-makers.

• Leverage existing processes and personnel to monitor and report risks.

• Provide uniform and sustainable risk management processes and a common risk language.

• Keep risk profiles and risk plans up-to-date.

• Encourage open and cross-functional discussions of top risks and business issues.

• Integrate risk information with planning, compliance and other business activities.

• Reinforce accountability for risk management by risk owners.
Compliance

Characteristics

• Compliance programs help institutions and their employees conduct operations and activities ethically and in line with internal policies as well as laws and other external regulations.

• Effective compliance programs must be tailored to the organization and its goals, and must be dynamic enough to adapt to a changing environment.

Objectives

• An effective compliance program strives to reduce the likelihood of regulatory non-compliance and criminal conduct in an organization and helps lessen the negative organizational impact should these activities occur.

• Programs should maintain autonomy with direct reporting lines to the Board and senior management.

• Compliance programs help protect organizations in a complex and dynamic ethical and regulatory environment. Failures can pose significant reputational and financial risks.

• A strong program can enable an organization to confidently identify risks and seize new opportunities.
The Three Lines of Defense

- **First Line of Defense**
  - Mgmt Controls
  - Internal Control Measures

- **Second Line of Defense**
  - Regulatory Compliance
  - Information & Systems Security/Compliance
  - Enterprise Risk Management
  - Ethics and Compliance Office
  - Office of General Counsel
  - Financial Operations

- **Third Line of Defense**
  - Internal Audit

- **Audit Committee / Board of Directors**

- **Senior Management**

- **External Audit**

- **Regulator**
Approach & Execution
Goals of Harmonization

By combining efforts between ERM, Compliance and Internal Audit, it is possible to:

1. Create a unified understanding of the current state and a common baseline
2. Provide coordinated risk coverage across the organization
3. Increase stakeholder satisfaction and reduce interview fatigue.
Risk Assessment Inputs

Quantitative Data
- Financial Statements
- Operational Data

Risk Assessment Inputs
- Interview Results
- Survey Responses

Qualitative Inputs

Individual Component Risks
to be compiled and analyzed by Internal Audit, ERM, and Compliance
Interview Approach

Each risk assessment interview should include representatives from each function -- Compliance, ERM and Internal Audit. In conducting these interviews, both a top-down and bottom-up risk assessment approach should be used. Combining both approaches to risk identification helps create a more comprehensive risk universe.

**Top Down Approach**

The top down portion of the approach involves identifying organizational **goals** and **strategies** as well as the associated risks that could impact the attainment of these goals. Top-down focuses on the organization’s **top strategic initiatives** and associated risks from the enterprise perspective. Risks would impact the organization more holistically, rather than one unit or process.

In the top-down approach, interviewees **speak to the risks of their unit as they align to organizational goals**, as well as to observations on organizational goals outside their unit.

**Bottom Up Approach**

The bottom up portion of the approach involves documenting the entity’s organizational components such as legal entities, business units, and key processes, and linking these “auditable units” to risks. Bottom-up is focused on **understanding the organization’s business operations and risks that exists within**, primarily focused on operational, financial and compliance impacts.

In this approach, interviewees **speak to risks in their unit that tie to organizational goals** as well as risks that do not necessarily tie to stated organizational goals.
Plan Development/Output
Art and Science

There are two approaches to analyzing the output of the data gathering process:

As a Science:
- During the risk assessment process, the combined team gathers objective data points to identify risks and determine the magnitude of the risks.
- Risks are measured based on quantitative criteria (e.g., financial information).

As an Art:
- Risks are identified qualitatively based largely on concerns raised during interviews with stakeholders.
- Interview data gathered is unstructured and weighted differently depending on frequency, source and context.
- Additional context such as industry trends, strategic goals, and management activities also factor into the unstructured data analysis.
Based on the results of the interviews, Internal Audit, Compliance, and ERM collaborated to determine the inherent component risks (i.e., activities/events that could prevent a business unit from fulfilling its initial objectives) faced by the organization.

These component risks were then grouped into larger key risk themes (e.g., finance, IT). As the risk assessment was a collaborative effort, the same set of risk themes were used by Internal Audit, Compliance, and ERM.

Based on the risk themes identified, and the underlying component risks, Internal Audit developed a three-year audit plan. Specific projects were mapped to the corresponding risk theme. Additionally, Internal Audit considered if areas have not been audited as part of recent audit plans.

Similar plans were developed by Compliance and ERM. Plans were shared across the three functions to minimize duplicative efforts and maximize risk theme coverage. The proposed plans are then presented to the relevant governing bodies (e.g., audit committee).
## Aligning Assurance Activities with Risks

<table>
<thead>
<tr>
<th>Risk Theme</th>
<th>Second Line of Defense</th>
<th>Third Line of Defense</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Compliance</td>
<td>ERM</td>
</tr>
<tr>
<td>Human Resources</td>
<td>• Conflict of Interest Review</td>
<td><em>No Planned Activities</em></td>
</tr>
<tr>
<td></td>
<td>• ERISA Compliance Review</td>
<td></td>
</tr>
<tr>
<td>Cybersecurity and Privacy</td>
<td><em>No Planned Activities</em></td>
<td>• Data Breach Notification Assessment</td>
</tr>
<tr>
<td>Budgeting, Finance, and Procurement</td>
<td><em>No Planned Activities</em></td>
<td><em>No Planned Activities</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Post-Risk Assessment Activities

Internal Audit, Compliance, and ERM should continue to engage in information sharing after the risk assessment is complete. This can be done through periodic cross-functional meetings or the use of a GRC system. The three functions should also meet periodically with key management stakeholders (e.g., IT, HR leadership) to stay abreast to management concerns and changes in the risk environment.

Changes in the risk environment mean changes to the risk universe, reflecting current and emerging risks facing the organization. This includes capturing changes in the external environment and business model that may impede an organization’s ability to achieve its objectives. As such, the audit, ERM, and compliance plans were also designed to be dynamic, incorporating ad hoc audits to address changing risks and management requests.
Questions
Thank you for your time and attention!