Convergence of Internal Audit, Compliance, and Risk Management

Frank Bossle
Executive Director-
Office of Hopkins Internal Audits
April 2014
Summary

• Plan to share with you the maturation process at Johns Hopkins University
• How the Internal Audit role has changed
• How three processes have become much more aligned:
  – Risk Management
  – Regulatory Compliance
  – Internal Audit
History

• Office of Hopkins Internal Audits was formed in 2000 to provide internal audit services to both the University and the Johns Hopkins Health System.

• At that time, we constructed the first “audit universe” and risk assessment. Realistically, this focused on auditable risk, not an all-encompassing identification or prioritization of risks.
Going It Alone

• Internal Audit projects focus on:
  – Assessing the adequacy of control
  – Testing control for effectiveness
• This often leads to discussions about acceptable levels of risk (and risk appetite)
• As there was no forum for “institute wide” agreement on risks, Internal Audit frequently had to negotiate issues on an ad-hoc basis
Emergence of Compliance Focus

• In 2005-6, JHU decided we needed a focus on compliance with laws and regulations
• An Institutional Compliance Oversight Committee was formed, with 10-12 high-level executives who owned key risks, such as HR, IT, Sponsored Research, Human Subjects, and Health & Safety
• A universe of 150 compliance topics was created, and assigned to risk owners
Examples of Regulatory Compliance Topics

<table>
<thead>
<tr>
<th>Student</th>
<th>Research</th>
<th>Clinical</th>
<th>Administrative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student and Financial Aid</td>
<td>Animal Care and Use</td>
<td>Clinical Trials</td>
<td>Health safety and Environment</td>
</tr>
<tr>
<td></td>
<td>Human Subjects</td>
<td>Billing Compliance</td>
<td>Information Technology</td>
</tr>
<tr>
<td></td>
<td>Conflicts of Interest in Research</td>
<td></td>
<td>Human Resources</td>
</tr>
<tr>
<td></td>
<td>Post-award Administration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compliance Takes Hold

- Risk owners prioritized the inventory and selected the highest risk areas for self assessment
  - Assessment based upon the Federal Sentencing Guidelines - steps to an effective compliance plan
  - Subcommittee reviewed and challenged the assessment
  - Institutional Compliance Oversight Committee reviewed the assessment and endorsed any recommended changes
Executive Leadership Engagement on Compliance

• Annual summary of compliance status and initiatives presented to the two Sr. Vice Presidents (CFO and Provost)
• Request support and/or funding for areas needing more emphasis
  – Example: hiring an Export Control Officer
Emergence of Institutional Risk Management

• New Sr. Vice President of Finance and Admin had prior experience with ERM (or IRM)
• Trustees were requesting a broader focus on risks
• 2011 official kickoff of the formal IRM program
• General Counsel had prepared an infamous list of 62 risks facing JHU - this provided a starting point
Institutional Risk Management Primer

• Iterative Process:
  – Identification and Prioritization
  – Assessment of management controls
  – Update for new risks

• Four types of risk:
  – Strategic
  – Operational
  – Financial
  – Compliance
  – (some also add Reputational, but we consider this a secondary risk that arises from the others)
IR M Process

Risk Assessment

Risk Framework → Individual Risk Identification → Risk Mapping → Quality of Current Controls

Risk Management

Risk Mitigation Analysis → Risk Mitigation Prioritization

Risk Appetite Analysis

Mitigating Some Risks → Monitoring Some Risks

Revisit
Risk Assessment

- Likelihood of Occurrence
- Impact (if it did occur)
  - Likelihood and Impact = Inherent Risk
- Quality of management controls
  - Reduces inherent risk to residual risk
Risk and Risk Management

Risk = Likelihood × Impact

Inherent Risk - Managed Risk = Residual Risk

Quality of Management Controls

IRM ICOC
IRM in Operation

• Senior leaders (IRM Leadership Group) meets quarterly to provide input on their perceptions of highest and emerging risks
  – Looking beyond the list of 62!
  – Facilitated assessment identified 12 highest risks, with particular emphasis on the top 4

• IRM Operations Group (middle to upper managers) meets monthly to discuss individual risks
Examples of “Institutional Risks”

- Faculty recruiting and retention
- International activities
- Threat to name and reputation
- IT Security
- Other more specialized risks applicable to JHU
Institutional Risk Management Program: Committees and Reporting Structure

Board of Trustees Audit Committee

IRM Leadership Group

IRM Operations Group

Committee on Crisis Management

Insurance Committee

Joint Health, Safety & Environment Committee

Institutional Compliance Oversight Committee
The Glue

• JHU appointed a chief risk officer in 2012
• Faculty member who did extensive work in crisis management, became interested in ERM as a concept, and linked up with the new Sr. VP
• Integrates crisis management, compliance, and IRM
• Has also assumed responsibility for Insurance and Health, Safety & Environment
IRM is now a two way street

• Academic exercise carried out to assess risks that have already been identified and prioritized
• Front line involvement in emerging and pressing risks, such as cyber attacks, student safety, government inquiries
• Provides real time update to IRM and executives on activities
Internal Audit Has Changed

• We do proactive/probe audits to:
  – Confirm that areas we think are well-managed are
  – Assess areas for which our understanding of the adequacy of management is weak
  – Shine a spotlight on areas for which we have concerns

• Risk issues that emerge in audits are shared in the IRM forum
New Forum for Discussion about Adequacy of Controls

- CRO systematically convenes affected risk owners, to help reach agreement on adequacy of controls (instead of the old ad-hoc discussions)