IT Audit at Brown

A collaboration between the Information Technology and Internal Audit Teams
Agenda

- Objective
- Risk Management Overview
- Internal Audit at Brown
- IT Audit at Brown
- Frequently Asked Questions (FAQ)
- Common Findings
Objective

To enhance collaboration between the University’s Office of Internal Audit Services and the Information Technology Services teams.
Risk Management Overview

Let’s start with a definition:

“a process, effected by an entity's board of directors, management and other personnel, applied in strategy-setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives”. Committee of Sponsoring Organizations (COSO)
Risk Management Overview

What is your worldview?
Risk Management Overview

A Solution Oriented Approach – The Three Lines of Defense
Let’s start with a definition:

Internal auditing at Brown University is independent, objective assurance and consultative activity designed to add value to the organization. The internal audit program is intended to assist the University in accomplishing its objectives by bringing a systematic, disciplined approach to increase the effectiveness and efficiency of risk management, control, and governance processes.
Internal Audit at Brown - Structure
## Internal Audit at Brown - Mission

<table>
<thead>
<tr>
<th>Mission</th>
<th>Vision</th>
</tr>
</thead>
<tbody>
<tr>
<td>To help the Corporation protect University resources and enhance the achievement of enterprise-wide strategies by evaluating and monitoring risks, processes and policies significant to the University's mission.</td>
<td>Excel as value-added service that is committed to your goals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authority</th>
<th>Sample Scope of Work</th>
</tr>
</thead>
</table>
| Has free, full, and unrestricted access as necessary to all and any University information, activities, records, property, manual and automated systems, and personnel for the purpose of carrying out their responsibilities. | ➢ Review design and execution of strategic priorities  
➢ Assess efficiency and effectiveness of operations  
➢ Evaluate compliance with policies, procedures, and external rules/regulations  
➢ Review integrity of financial reporting |
Internal Audit at Brown – Services

- Financial Audits
- Operational Audits
- Compliance Audits
- Information Technology Audits
- Construction Audits
- Advisory and Consulting Engagements
- Investigations
- Special Reviews
Internal Audit at Brown – Process

- Risk Based Approach
- Project Planning and Risk Assessment
- Test Work
- Reporting – Draft and Final
- Follow-up/Remediation
Internal Audit at Brown – Risk Based Approach

Audit Universe → Risk Based Prioritized Audit Universe

Emerging Risk Areas
High Priority Risk Areas
Low Priority Risk Areas

Audit Strategy → Audit Plan

News and Events
Regulatory Compliance
External Consultants
Industry Benchmarks

University Strategy
Management Interviews
Prior Audits
Enterprise Risks

THE OFFICE OF INTERNAL AUDIT SERVICES
“Committed to Excellence, Committed to You and Your Goals”
Internal Audit at Brown – Project Phases

Planning and Risk Assessment
- Identify key contacts
- Conduct interviews/meetings
- Document functions
- Identify risks and controls
- Modify audit scope as needed
- Develop audit program

Test Work
- Review/assess processes
- Identify improvement opportunities & best practices
- Discuss results with management

Reporting
- Hold client exit conference
- Issue Draft Report
- Obtain responses
- Issue Final Report
IT Audit at Brown – Risk Focus Areas

Focused on risks that impact:

<table>
<thead>
<tr>
<th>Organizational Units</th>
<th>Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized IT Processes</td>
<td>Networking</td>
</tr>
<tr>
<td>Decentralized IT Processes</td>
<td>Compute</td>
</tr>
<tr>
<td></td>
<td>Storage</td>
</tr>
</tbody>
</table>
IT Audit at Brown – A Simple Control Model (SANS 20)
## IT Audit at Brown – A Simple Control Model (SANS 20)

<table>
<thead>
<tr>
<th>Potential Risk</th>
<th>Some Related SANS Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider threat</td>
<td>14,15,16</td>
</tr>
<tr>
<td>Point of sale intrusions</td>
<td>1, 20</td>
</tr>
<tr>
<td>Cyber espionage/phishing/ransomware</td>
<td>1, 2</td>
</tr>
</tbody>
</table>
Q 1: How is my department selected for an Audit?
Answer: 1) Risk assessment and 2) Your request

Q 2: How long does an audit typically take?
Answer: It depends on size, complexity, and strength of internal controls

Q 3: How much of my time will the audit require?
Answer: We are considerate

Q 4: How can I prepare for an audit?
Answer: Have key documents ready
Q 5: How confidential will the information I provide to you and my audit report be?

Answer: All information received and managed by the Office of Internal Audit Services is held at the appropriate level of confidentiality.

Q 6: Who gets copies of audit reports?

Answer: Those in a position to see that corrective actions are taken and those with a need to know, generally, the Executive VP Finance and Administration, Senior Officials and key management personnel on a need to know basis, including members of the Audit Committee.
IT Audit at Brown – Common Findings

- Lack of formalized policies and procedures
- Inappropriate access management
- Segregation of duties
- Misconfigurations
- Change management
- Data security
IT Audit at Brown – Ethics and Compliance Reporting System (EARS)
IT Audit at Brown

- Questions
- Feedback
- Comments
“The essence of risk management lies in maximizing the areas where we have some control over the outcome while minimizing the areas where we have absolutely no control over the outcome and the linkage between effect and cause is hidden from us”. P.L. Bernstein
IT Audit at Brown – Contact Information

Utibe Offiong
Chief University Auditor
Utibe_Offiong@Brown.edu
401-863-1593
IT Audit at Brown

Thank you for your time and attention.