IT Risk Assessment: Learn from our work, leverage at your campus

Presented by:
Princeton University – Baker Tilly

Speakers
- Nadine Stern, Deputy Chief Information Officer
- David Sherry, Chief Information Security Officer
- Daphne Ireland, Senior Information Security Analyst
- Mike Cullen, Baker Tilly
Objectives

• Provide audience with information on how to develop and execute an IT risk assessment based on our recent experiences
• Understand the challenges synthesizing and prioritizing risks via an interactive, simulated mini IT risk assessment
• Leverage the challenges and lessons learned to develop or improve your institution's IT risk assessment process

Agenda

• Poll Everywhere Introduction
• University and IT Risk Assessment Background
• IT Risk Assessment Approach
• Challenges
• Results and Lessons Learned
Poll Everywhere Introduction

www.polleverywhere.com

- Interactive polling software
- Audience votes via texting or mobile app
- Real-time results shared with audience

- Let’s test it out!
INTERACTIVE POLLING QUESTIONS

University and IT Risk Assessment Background
University Background

- The ever-growing reliance on IT creates new and expanding risks that may affect the University’s mission in teaching and research
- As reliance on IT increases, the scale, scope, and complexity of IT resources must continue to mature to meet the needs of faculty, staff, students, and other constituents

IT Risk Assessment Background

- Office of Information Technology (OIT), partnered with Baker Tilly, as well the University’s Office of Audit and Compliance (OAC) to develop and execute a structured, repeatable framework for a University-wide IT risk assessment
IT Risk Assessment Approach

Plan  Study  Assess  Report
Plan

• Scope
• IT risk definition
• Initial IT risk inventory and risk criteria
• Project plan
• Project governance structure
  – Advisory Group and Steering Committee
• Stakeholders

INTERACTIVE POLLING QUESTION
IT Risk Definition

- IT Risk is comprised of the threats and vulnerabilities that may impact the confidentiality, integrity, and availability of the University’s information and underlying systems.
- IT Risk should be considered in the context of what can go wrong as well as what needs to continue to go right as it relates to people, process, and technology.

<table>
<thead>
<tr>
<th>CONFIDENTIALITY</th>
<th>INTEGRITY</th>
<th>AVAILABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring that information is protected from unauthorized access or loss</td>
<td>Ensuring the accuracy, completeness, and consistency of information</td>
<td>Ensuring that information is ready and suitable for use</td>
</tr>
</tbody>
</table>
## Project Governance

<table>
<thead>
<tr>
<th>Steering Committee</th>
<th>Advisory Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serves as strategic advisors to the Working Group</td>
<td>Serves as an intermediary filter to the Steering Committee</td>
</tr>
<tr>
<td>• VP for IT and CIO (Exec Sponsor)</td>
<td>• Deputy CIO</td>
</tr>
<tr>
<td>• Chief Audit and Compliance Officer (Exec Sponsor)</td>
<td>• Associate CIO</td>
</tr>
<tr>
<td>• VP for Finance and Treasurer</td>
<td>• Assistant Vice President for Development</td>
</tr>
<tr>
<td>• Dean of the Faculty</td>
<td>• Director of Finance Administration and Transformation Program</td>
</tr>
<tr>
<td>• Deputy CIO</td>
<td>• Associate Director for Administrative Planning</td>
</tr>
<tr>
<td>• Associate CIO</td>
<td>• Chief Information Security Officer</td>
</tr>
<tr>
<td></td>
<td>• Director, IT Audit</td>
</tr>
<tr>
<td></td>
<td>• Senior IT Auditor</td>
</tr>
</tbody>
</table>

## Study

- Surveyed and interviewed key stakeholders
  - Current state of IT
  - IT environment and objectives
- Analyzed and summarized results
INTERACTIVE POLLING QUESTION

Assess

- Synthesized information
- Prioritized IT risk statements with rationale
- Shared with Advisory Group and Steering Committee
- Incorporated feedback
INTERACTIVE POLLING QUESTION

Data Analysis

- 200+ Data points captured
- 79 Risk statements
- 26 IT Risks
- 9 Categories
Report

- Drafted and validated a summary report
- Shared with Advisory Group and Steering Committee
- Incorporated feedback
- Presented results to leadership and board
- Reported results to stakeholders
  - Signaled continuous risk assessment program

Reporting Example – Summary

<table>
<thead>
<tr>
<th>IT Risk Area</th>
<th>Impact Rating</th>
<th>Likelihood Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing devices to University standards and practices</td>
<td>High</td>
<td>Moderate</td>
</tr>
<tr>
<td>Maintaining continuity of critical infrastructure</td>
<td>High-Moderate</td>
<td>High</td>
</tr>
<tr>
<td>Securing research data to meet external requirements</td>
<td>High-Moderate</td>
<td>High-Moderate</td>
</tr>
<tr>
<td>Collecting, storing, and transmitting data as appropriate</td>
<td>High-Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>Detecting, responding, and recovering from incidents</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
### Reporting Example – Detail

<table>
<thead>
<tr>
<th>IT Risk Category</th>
<th>Impact Rating</th>
<th>Likelihood Rating</th>
<th>NIST Alignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring accuracy, completeness, and consistency of data in systems</td>
<td>Information</td>
<td>High-Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

#### IT Risk Statement

Systems of records are critical to the operations of the University. If the accuracy, completeness, or consistency of data from systems of records is compromised the University may be using or reporting inaccurate or incomplete data.

#### IT Risk Rationale

Systems are used to support the major administrative functions. Lack of data quality standards can lead to additional work. Many centralized functions have processes, although informal in nature, to manage data collection and monitoring to ensure consistency and quality.

---

### Challenges
### Challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project governance structure</td>
<td>Created steering committee and advisory group to support project team</td>
</tr>
<tr>
<td>Project timing and schedule</td>
<td>Defined generous timing initially and refined throughout the project</td>
</tr>
<tr>
<td>Stakeholders identification</td>
<td>Used wisdom of all involved to invite a broad group to participate</td>
</tr>
<tr>
<td>Data gathering</td>
<td>Used online surveys, interviews, and working sessions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST Framework applicability</td>
<td>Started with NIST CSF, reframed concepts and control requirements into common language</td>
</tr>
<tr>
<td>IT risk and criteria definitions</td>
<td>Started with generic industry definitions, refined and customized to the University</td>
</tr>
<tr>
<td>Data analysis</td>
<td>Iterate and collaborate via working sessions to synthesize the data</td>
</tr>
<tr>
<td>IT risk inventory creation and refinement</td>
<td>Drafted initial risks, had to start anew based on data analysis, refined with working sessions</td>
</tr>
</tbody>
</table>
Results and Lessons Learned

Results

- Increased the IT risk knowledge and awareness of leadership and stakeholders
- Developed repeatable, structured program for future periodic IT risk assessments
- Results of IT risk assessment influenced the staffing of the Information Security Office
- Prioritized IT plans and initiatives based on risk assessment results
- Methodology developed for the IT risk assessment was used to perform a reset of the University's enterprise risk management process
Lessons Learned

• Need a dedicated team effort
• Requires broad stakeholder engagement
• Essential to have IT and Internal Audit partnership
• Customize IT risk and criteria definitions
• Educate leadership and community continually

Speaker Contact

• Nadine Stern, nstern@Princeton.edu
• David Sherry, david.sherry@Princeton.edu
• Daphne Ireland, daphne.ireland@Princeton.edu
• Mike Cullen, mike.cullen@bakertilly.com