IT Risk Management & Governance: How do you measure up?

Catherine Watt
Senior Analyst
EDUCAUSE

Jeffrey Battaglino
Director, IT Service Management, Compliance and Security
Seton Hall University

Objectives:

Our activities for today include:
I. Introduce the new EDUCAUSE Benchmarking Service & IT Risk Management index
II. Learn how Seton Hall University navigates the challenges of IT Risk Management
III. Collaborate to discuss the obstacles, successes, and action plans for your own institutions
IV. Initiate a discussion about what services are needed in next steps
I. Introducing the EDUCAUSE Benchmarking Service

1) Build reports on demand with customized peer groups

2) Benchmark maturity and technology deployment
EDUCAUSE Benchmarking
Service Beta

EDUCAUSE IT Risk Management Maturity Index
3) Receive recommendations for improvement
5. Optimized
4. Managed
3. Defined
2. Repeatable
1. Absent/ad hoc
## IT Risk Management at Seton Hall University

---

### Seton Hall Risk Registry

<table>
<thead>
<tr>
<th>Risk ID</th>
<th>Name</th>
<th>Description</th>
<th>Created</th>
<th>Status</th>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>RISK0000576</td>
<td>Support is ending for NF241</td>
<td>Chrome ended support in 2020 and Firefox will end support in 2021. Various other browsers may not support NF241, but they are not considered a threat.</td>
<td>2015-02-28 16:03:28</td>
<td>Open</td>
<td>IT</td>
<td>2015-02-28 16:03:28</td>
</tr>
<tr>
<td>RISK0000585</td>
<td>Windows Server 2003</td>
<td>There are Windows 2003 servers that are no longer supported and one of these will be running the end of its life and may need to be upgraded.</td>
<td>2015-05-14 11:55:57</td>
<td>Open</td>
<td>IT</td>
<td>2015-05-14 11:55:57</td>
</tr>
<tr>
<td>RISK0000545</td>
<td>SF1 Access System</td>
<td>The current Access system has reached end of life and needs to be upgraded.</td>
<td>2014-01-30 14:11:48</td>
<td>Open</td>
<td>IT</td>
<td>2014-01-30 14:11:48</td>
</tr>
</tbody>
</table>
Seton Hall Risk Registry

- Risk ID
- Name
- Description
- Updates
- State - status
- Category
- Created

Seton Hall Risk Remediation
Seton Hall Risk Management Process

Identify – Risks are identified in a number of ways:
• Brainstorming
• Root Cause Analysis
• Audit Findings

Categorize and Prioritize – Determine the severity of risks and respond accordingly.

Document – Enter risks in a clear and concise manner where remediations are assigned to specific individuals or groups. All invested parties should have access to this information.

Assess – Determine the level of effort needed to remediate the risk and assign tasks, changes, and projects that will get the job done.

Remediate – Perform all tasks, changes, and projects to remediate the risk.

Monitor – Ascertain that all steps have been made to remediate the risk, and fully document the remediation steps for future reference.

“Moving the Needle” on IT Risk Management
Discussion logistics

- Work in groups at each table
- Explore the Maturity Index dimension assigned to your table
- Resources:
  - Key factors handout
- Identify specific ideas to increase the maturity level of your institutions’ analytics initiatives
- Make action plan for when you return home

Discussion Questions

- What is the **obstacle** keeping you from the next maturity level for this dimension? What can help you overcome that obstacle?
- Where you have had **success** in this dimension? What were the keys to that success? What helped you get there?
- What are you going to do next week and in the next 90 days? What **actionable steps** will you take?
IT Risk Management Maturity
(All Non-specialized US Institutions)

- Leadership
- Process and Management
- Acceptance
- Investment

5. Optimized
4. Managed
3. Defined
2. Repeatable
1. Absent/ad hoc

2015 EDUCAUSE Core Data Service

Process and Management

- Types of items
  - IT risks are tracked and prioritized
  - Policies and controls for IT risks are implemented
  - Adequate staff training for risk management activities

- Recommendations
  - Develop a formal procedure to identify IT risks
  - Develop a common language and understanding around IT risk management
Acceptance

- Types of items
  - Faculty, staff, and administration are not resistant to IT risk management policies and controls
  - Authority to effectively manage end-user actions

- Recommendations
  - Work with stakeholders to get buy-in on policies and controls
  - Work with institutional leadership to gain sufficient authority

Investment

- Types of items
  - Adequate investment in IT services
  - Adequate budget and staff for IT risk management

- Recommendations
  - Implement a staff development plan to ensure appropriate resources are available for IT risk management
  - Develop an IT services investment plan
Leadership

- Types of items
  - Institutional leadership understands and is involved in IT risk management
  - IT participates in institutional risk assessment

- Recommendations
  - Help institutional leaders understand the benefits of IT risk management
  - Build cross-departmental teams to help central IT leaders participate in institutional risk assessment

EDUCAUSE IT Governance Maturity Index
IT Governance Maturity Index
by Carnegie Class

5. Optimized
4. Managed
3. Defined
2. Repeatable
1. Absent/ad hoc

2015 EDUCAUSE Core Data Service
**IT Governance Maturity**

(All Non-specialized US Institutions)

- 5. Optimized
- 4. Managed
- 3. Defined
- 2. Repeatable
- 1. Absent/ad hoc

---

**Process**

- **Types of items**
  - Formal governance structure
  - Process assigns clear responsibility/accountability
  - Coordinated distributed IT efforts

- **Recommendations**
  - Determine where to assign responsibility and authority
  - Research frameworks such as COBIT and ITIL
Strategic Alignment and Influence

- Types of items
  - Clear institutional vision for IT
  - Goals for IT outcomes are aligned with institutional strategy
  - IT governance influences decisions

- Recommendations
  - Align operational plan with strategic goals
  - Demonstrate how IT governance can help with decision-making

IT Investment

- Types of items
  - Full life-cycle costs are considered in decision-making
  - IT investments are prioritized in alignment with institutional goals

- Recommendations
  - Propose funding models for IT projects
  - Evaluate time to reach a decision for projects or initiatives
Communication and Participation

- Types of items
  - Faculty, administrative, and academic leadership are committed to IT governance
  - Technology standards and services are visible and broadly understood
- Recommendations
  - Communicate decisions transparently
  - Include stakeholders in IT decisions

Thank you!

For more information:

EDUCAUSE Benchmarking Service Beta

benchmarking@educause.edu