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

Catherine Watt  
Senior Analyst  
EDUCAUSE

Jim O’Connor  
Vice President for Information Technology & CIO  
Georgia Institute of Technology

Mia Reini  
Director of Enterprise Risk Management  
Georgia Institute of Technology

UCOMMON THINKING FOR THE COMMON GOOD
Objectives:

Our activities for today include:

I. Introduce the new EDUCAUSE Benchmarking Service & IT Risk Management index

II. Learn how Georgia Tech 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
I. Introducing the EDUCAUSE Benchmarking Service

2) Benchmark maturity and technology deployment
I. Introducing the EDUCAUSE Benchmarking Service
3) Receive recommendations for improvement

### 3. Data Security and Data Management Processes

<table>
<thead>
<tr>
<th>Item</th>
<th>ProU</th>
<th>CIC</th>
<th>Pub DR</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Means</td>
<td>1.9</td>
<td>2.9</td>
<td>2.8</td>
<td></td>
</tr>
<tr>
<td>3.5 We have procedures and technologies in place to protect sensitive data from unauthorized access and tampering.</td>
<td>4.0</td>
<td>3.4</td>
<td>3.1</td>
<td>Your institution has procedures and technologies in place to protect sensitive data from unauthorized access and tampering.</td>
</tr>
<tr>
<td>3.3 We classify data to indicate the appropriate levels of information security.</td>
<td>3.0</td>
<td>3.3</td>
<td>3.0</td>
<td>Data classification. Determine classification levels for institutional data based on the criticality and risk levels of the data. To take a risk-based approach to data protection, one must first distinguish the sensitivity between different resources. Add this information to the information asset inventory.</td>
</tr>
<tr>
<td>3.4 We have standards for isolating sensitive data to protect it from unauthorized access and tampering.</td>
<td>3.0</td>
<td>3.5</td>
<td>3.0</td>
<td>Data protection standards. Establish common, repeatable best practices for isolating sensitive data to protect it from unauthorized access and tampering.</td>
</tr>
<tr>
<td>3.1 We have a process for identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of records containing sensitive information.</td>
<td>2.0</td>
<td>3.1</td>
<td>2.9</td>
<td>Risk assessment. Develop or improve processes for identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, integrity, or availability of records containing sensitive information. Risk assessment should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. Consider all risk assessments including those that may be performed by third parties and internal audit.</td>
</tr>
</tbody>
</table>
IT Risk Management Maturity Index
by Carnegie Class

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

2015 EDUCAUSE Core Data Service
IT Risk Management Maturity Index

by Carnegie Class

US Non-specialized 5.0

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

2015 EDUCAUSE Core Data Service
Enterprise Risk Management at Georgia Tech

Enterprise Risk Management works with senior leadership at Georgia Tech to:

1) Identify risks
2) Mitigate risks that may interfere with Georgia Tech’s Strategic Plan Goals and Institutional Initiatives.

Enterprise Risk Management’s goal is to:

1) Prioritize risk resources
2) Embed risk resources into existing business processes with the objective of being strategic, efficient, and supportive of entrepreneurship at Georgia Tech.
ERM Steps

Step 1: Develop Risk Inventory of Risk Factors (financial, operational, strategic, reputational, compliance)

Step 2: Score Risk Factors for Inherent Risk (likelihood, impact, velocity)

Step 3: Risk Owners present Controls for Risk Factors with high scores

Step 4: Re-score for Residual Risk (risk after controls)

Step 5: Present Risk Management Plans for Risk Factors with high Residual Risk
## Risk Scoring

<table>
<thead>
<tr>
<th>Impact</th>
<th>High (Score: 10, 9, 8)</th>
<th>Medium (Score: 7, 6, 5)</th>
<th>Low (Score: 4, 3, 2, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Impair Achievement of Strategic Goal</td>
<td>Create Inefficiency or Re-Work</td>
<td>Small Limited Loss</td>
</tr>
<tr>
<td></td>
<td>Result in Substantial Financial Cost</td>
<td>Result in Fines</td>
<td>Result in Warning or Reprimand</td>
</tr>
<tr>
<td></td>
<td>Create Significant Damage to Institute Reputation</td>
<td>Minor Injury</td>
<td>Little Effect on Institute</td>
</tr>
<tr>
<td></td>
<td>Require Intervention in Institutional Operations</td>
<td>Moderate Loss</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>High (Score: 10, 9, 8)</th>
<th>Medium (Score: 7, 6, 5)</th>
<th>Low (Score: 4, 3, 2, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Probability &gt; 75%</td>
<td>Probability 50% - 75%</td>
<td>Probability &lt; 50%</td>
</tr>
<tr>
<td></td>
<td>Will happen frequently</td>
<td>Sometimes occurs</td>
<td>Will seldom happen</td>
</tr>
<tr>
<td></td>
<td>On-going event</td>
<td>Unpredictable</td>
<td>Has not happened</td>
</tr>
<tr>
<td></td>
<td>Predictable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Velocity</th>
<th>High (Score: 10, 9, 8)</th>
<th>Medium (Score: 7, 6, 5)</th>
<th>Low (Score: 4, 3, 2, 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Estimate may happen in 0-3 years</td>
<td>Estimate may happen in 4-6 years</td>
<td>Estimate may happen in 7-10 years</td>
</tr>
</tbody>
</table>
Data Security One of Top Overall Risks

Unauthorized disclosure of protected information
Data Security One of Top IT Risks

Unauthorized disclosure of protected information
Once You Know…

You must do something about it:

• Phishing Training – full campus every semester
• Sensitive Server Registration
• Sensitive Server Scanning
• SEIMs to detect attacks

• Training
  – GTRC trains PIs and their research staff
  – Compliance with GT standards and BoR IT Handbook (now annual training for the entire campus)
  – Communication via campus media
“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

Investment

Acceptance

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

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

US Non-specialized

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

DR Priv
MA Priv
MA Pub
BA
AA

2015 EDUCAUSE Core Data Service
IT Governance Maturity Index

by Carnegie Class

US Non-specialized

5

2.6

2.7

2.8

2.5

2.6

2.7

1

0

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)

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

2015 EDUCAUSE Core Data Service
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!
Need more information? Please contact us.

Dr. Catherine Watt  
EDUCAUSE  
Clemson, SC home office  
864-903-3266  
cwatt@educause.edu

MIA REINI  
Dir, Enterprise Risk Management  
Georgia Inst of Technology  
760 Spring St. NW, Suite 324  
Atlanta, GA 30332-0495  
404-894-9340 Direct  
mia.reini@gatech.edu