Information Security, Governance, and Risk Capability: How do you measure up?

Leah Lang
Director of Analytics Services
EDUCAUSE

Catherine Watt
Senior Analyst
EDUCAUSE

Tom Dugas
Director, Information Security/New Initiatives
Duquesne University

UNCOMMON THINKING FOR THE COMMON GOOD
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

<table>
<thead>
<tr>
<th>Category</th>
<th>Absent/ad hoc</th>
<th>Repeatability</th>
<th>Defined</th>
<th>Managed</th>
<th>Optimized</th>
</tr>
</thead>
<tbody>
<tr>
<td>Culture of Innovation</td>
<td></td>
<td>2.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Governance</td>
<td></td>
<td>2.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
<td>2.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Risk Management</td>
<td></td>
<td>3.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research Computing</td>
<td></td>
<td>3.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
<td>3.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-learning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.6</td>
</tr>
<tr>
<td>Student Success Technologies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.7</td>
</tr>
</tbody>
</table>
I. Introducing the EDUCAUSE Benchmarking Service

2015 EDUCAUSE Core Data Service
EDUCAUSE Information Security Maturity Index
Information Security Maturity Index
by Carnegie Class

US Non-specialized

5.0

2.8

3.0

2.4

2.9

2.6

1.0

2.6

3.0

2.4

3.0

AA

BA

MA Pub

MA Priv

DR Pub

DR Priv

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

2015 EDUCAUSE Core Data Service
Poll: Which of these areas is most challenging at your institution?

- Security services and operations
- Asset protection
- Systems review
- Policies
- Business continuity
Security Services and Operations

- **Types of items**
  - Individual with institution-wide information security responsibility
  - Information security awareness training
  - Assess security controls of contracted services with external entities

- **Recommendations**
  - Participate in security groups (REN-ISAC, EDUCAUSE, InfraGard, etc.)
  - Develop an incident management plan
Title of the highest-ranking person with primary responsibility for information security
2011-2015

2015 EDUCAUSE Core Data Service
#1: Ensuring that members of the institutional community receive information security education and training
Institutions with mandatory information security training for faculty, staff, and students

74% Faculty or Staff
27% Students
The influence of cloud-based services on IT strategy

- Tracking, but no influence yet: 2% (Not at all), 3% (A minor influence)
- A major influence: 52%
- Already incorporated: 25%
Information Systems and Applications most commonly vendor-managed (SaaS)

<table>
<thead>
<tr>
<th>Service</th>
<th>All nonspec. U.S.</th>
<th>AA</th>
<th>BA</th>
<th>MA public</th>
<th>MA private</th>
<th>DR public</th>
<th>DR private</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail: student</td>
<td>63%</td>
<td>56%</td>
<td>58%</td>
<td>63%</td>
<td>63%</td>
<td>66%</td>
<td>76%</td>
</tr>
<tr>
<td>Customer relationship management (CRM)</td>
<td>39%</td>
<td>36%</td>
<td>47%</td>
<td>33%</td>
<td>42%</td>
<td>31%</td>
<td>53%</td>
</tr>
<tr>
<td>E-mail: faculty/staff</td>
<td>36%</td>
<td>22%</td>
<td>41%</td>
<td>36%</td>
<td>43%</td>
<td>40%</td>
<td>34%</td>
</tr>
<tr>
<td>Learning management</td>
<td>35%</td>
<td>39%</td>
<td>20%</td>
<td>29%</td>
<td>43%</td>
<td>35%</td>
<td>48%</td>
</tr>
<tr>
<td>Library</td>
<td>26%</td>
<td>27%</td>
<td>29%</td>
<td>25%</td>
<td>33%</td>
<td>17%</td>
<td>24%</td>
</tr>
<tr>
<td>IT service desk management</td>
<td>21%</td>
<td>18%</td>
<td>10%</td>
<td>19%</td>
<td>19%</td>
<td>28%</td>
<td>34%</td>
</tr>
<tr>
<td>Facilities management</td>
<td>20%</td>
<td>22%</td>
<td>20%</td>
<td>20%</td>
<td>21%</td>
<td>18%</td>
<td>17%</td>
</tr>
<tr>
<td>Admissions: undergraduate</td>
<td>19%</td>
<td>2%</td>
<td>35%</td>
<td>8%</td>
<td>22%</td>
<td>21%</td>
<td>31%</td>
</tr>
</tbody>
</table>
Asset Protection

- **Types of items**
  - Procedures and technologies in place to protect sensitive data
  - Access control procedures for information systems and physical assets
  - Authorization system in place

- **Recommendations**
  - Utilize a configuration control system
  - Segregate information resources based on sensitivity and risk
#3: Planning for and implementing next-generation security technologies to respond to evolving threats
Information Security Technology Deployment

- Network access control system
- Scanning tools for private/protected...
- Secure remote access
- Log management
- Security information and event management
- Data loss prevention
- Endpoint encryption for sensitive data
- Malware protection
- Network intrusion prevention system
- Penetration testing tools
- Secure wireless access

Legend:
- No deployment
- Expected deployment
- Initial deployment
- Targeted deployment
- Institution-wide deployment

2015 EDUCAUSE Core Data Service
Systems Review

- **Types of items**
  - Vulnerability management strategy in place
  - Log data is monitored and secure
  - Configuration-management process in place
  - Security reviews are completed regularly

- **Recommendations**
  - Establish processes to prevent unauthorized access to log data
  - Ensure changes to systems and applications are for valid business reasons
On the Rise: Information Security Risk Assessment
Policies

- Types of items
  - Usage guidance for mobile devices
  - Critical information assets are identified
  - Data are classified
  - Policies address life cycle of paper and electronic records

- Recommendations
  - Distinguish sensitivity between different resources
  - Build relationships with campus stakeholders to improve records management
Organizational unit primarily responsible for information security practices

- Network security
- Identity management
- Monitoring
- Security software procurement
- Incident management
- Configuration management
- Information security policy development
- Data security
- Training and awareness
- Information security risk management
- Information security compliance
- Data privacy

Legend:
- Primarily central IT
- Primarily other admin or academic unit(s)
- Shared between central IT and other admin or academic unit(s)
- Primarily system or district office
- Primarily outsourced
- No unit responsible
Business Continuity

- **Types of items**
  - Reviewed and approved business continuity plan
  - Periodically tested business continuity plan

- **Recommendations**
  - Make the case for business continuity with executives
  - Review responses and actions to plan for next steps after each test
EDUCAUSE IT Governance Maturity Index
5. Optimized
4. Managed
3. Defined
2. Repeatable
1. Absent/ad hoc
IT Governance Maturity
(All Non-specialized US Institutions)

- Process
- Communication and Participation
- IT Investment
- Strategic Alignment and Influence

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

2015 EDUCAUSE Core Data Service
Poll: Which of these areas is most challenging at your institution?

- Process
- Strategic alignment and influence
- IT investment
- Communication and participation
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
IT Risk Management Maturity Index
by Carnegie Class

US Non-specialized

5.0

DR Priv
3.2

3.0

DR Pub
3.1

3.1

MA Priv
2.9

MA Pub
3.0

BA

AA

1.0

2.9

2.9

3.1

3.1

3.0

3.0

5.0

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

2015 EDUCAUSE Core Data Service
IT Risk Management Maturity Index

by Carnegie Class

US Non-specialized

5.0

3.0

DR Priv

3.2

MA Priv

3.1

DR Pub

3.1

MA Pub

2.9

AA

3.1

BA

1.0

2015 EDUCAUSE Core Data Service

5. Optimized
4. Managed
3. Defined
2. Repeatable
1. Absent/ad hoc
IT Risk Management Maturity
(All Non-specialized US Institutions)

- Process and Management
- Leadership
- Acceptance
- Investment

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

2015 EDUCAUSE Core Data Service
Poll: Which of these areas is most challenging at your institution?

- Process and management
- Acceptance
- Investment
- Leadership
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
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
<table>
<thead>
<tr>
<th>Risk Scoring</th>
<th>Impact</th>
<th>Likelihood</th>
<th>Velocity</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (Score: 10, 9, 8)</td>
<td>High (Score: 10, 9, 8)</td>
<td>High (Score: 10, 9, 8)</td>
<td>Medium (Score: 7, 6, 5)</td>
</tr>
<tr>
<td>Impair Achievement of Strategic Goal</td>
<td>Probability &gt; 75%</td>
<td>Estimate may happen in 0-3 years</td>
<td>Medium (Score: 7, 6, 5)</td>
</tr>
<tr>
<td>Result in Substantial Financial Cost</td>
<td>Probability 50% - 75%</td>
<td>Estimate may happen in 4-6 years</td>
<td>Low (Score: 4, 3, 2, 1)</td>
</tr>
<tr>
<td>Create Significant Damage to Institute Reputation</td>
<td>Sometimes occurs Unpredictable</td>
<td>Estimate may happen in 7-10 years</td>
<td>Low (Score: 4, 3, 2, 1)</td>
</tr>
<tr>
<td>Require Intervention in Institutional Operations</td>
<td>Will happen frequently On-going event Predictable</td>
<td>Little Effect on Institute</td>
<td></td>
</tr>
<tr>
<td>Medium (Score: 7, 6, 5)</td>
<td>Medium (Score: 7, 6, 5)</td>
<td>Medium (Score: 7, 6, 5)</td>
<td></td>
</tr>
<tr>
<td>Create Inefficiency or Re-Work</td>
<td>Result in Fines</td>
<td>Moderate Loss</td>
<td></td>
</tr>
<tr>
<td>Result in Fines</td>
<td>Minor Injury</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low (Score: 4, 3, 2, 1)</td>
<td>Low (Score: 4, 3, 2, 1)</td>
<td>Low (Score: 4, 3, 2, 1)</td>
<td></td>
</tr>
<tr>
<td>Small Limited Loss</td>
<td>Result in Warning or Reprimand</td>
<td>Little Effect on Institute</td>
<td></td>
</tr>
</tbody>
</table>
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
Thank you!

For more information:

EDUCAUSE Benchmarking Service Beta

benchmarking@educause.edu