Get Your Ducks in a Row: IT Governance, Risk, and Compliance in Higher Education
Today’s Speakers

Joanna Grama
*Director of IT GRC and Cybersecurity Programs*
EDUCAUSE

Jacqueline Bichsel, Senior Research Analyst
EDUCAUSE

Patrick J. Feehan, Director, IT Policy and Cybersecurity Compliance
Montgomery College

Cathy Bates, Associate Vice Chancellor and CIO
Appalachian State University

Michael J. Chapple, Senior Director, IT Service Delivery
University of Notre Dame
Presentation Agenda

• Introduction to the EDUCAUSE IT GRC Initiative
• 2014 ECAR Study on IT Governance, Risk, and Compliance in Higher Education
• Panel Discussion
EDUCAUSE IT GRC Program
EDUCAUSE IT GRC Program

- Initiative began in January 2014
- Advisory committee helps guide the program
- Advisory committee includes subject matter experts in IT GRC and representation from NACUBO, NACUA, and URMIA for additional expertise

<table>
<thead>
<tr>
<th>Name</th>
<th>University/Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cathy Bates</td>
<td>Appalachian State University</td>
</tr>
<tr>
<td>L. Sue McCormick</td>
<td>University of Virginia</td>
</tr>
<tr>
<td>Niraj Bhagat</td>
<td>Southern Methodist University</td>
</tr>
<tr>
<td>Steven J. McDonald</td>
<td>Rhode Island School of Design</td>
</tr>
<tr>
<td>Michael J. Chapple</td>
<td>University of Notre Dame</td>
</tr>
<tr>
<td>Peter J. Murray</td>
<td>University of Maryland, Baltimore</td>
</tr>
<tr>
<td>Michael Corn</td>
<td>Brandeis University</td>
</tr>
<tr>
<td>Marty Ringle</td>
<td>Reed College</td>
</tr>
<tr>
<td>Elias G. Eldayrie</td>
<td>University of Florida</td>
</tr>
<tr>
<td>Cheryl Washington</td>
<td>University of California, Davis</td>
</tr>
<tr>
<td>Merri Beth Lavagnino</td>
<td>Indiana University</td>
</tr>
<tr>
<td>Madelyn F. Wessel</td>
<td>Virginia Commonwealth University</td>
</tr>
</tbody>
</table>
EDUCAUSE IT GRC Program

  - Includes separate links for IT governance, risk, and compliance resources from the EDUCAUSE library
- Discussion list: [ITGRC-DG@listserv.educause.edu](mailto:ITGRC-DG@listserv.educause.edu)
- IT governance and risk management maturity indices (part of the 2014 Core Data Service survey)
- Upcoming mini-briefs that define governance, risk, and compliance in the higher education context, with lists of resources and questions leaders should ask. (4Q 2014)
- 2015 anticipated deliverable: Gap analysis toolkit of institutional IT risks that institutions can compare against their own list of institutional IT risks. (3Q 2015)
ECAR Study:
IT GRC in Higher Education
EDUCAUSE Center for Analysis and Research (ECAR)
IT GRC Survey

246 member institutions
Risk Management
Risk management programs in place

- All institutions: 54%
- Enterprise risk management: 21%
- IT risk management: 10%
- Enterprise RM and IT RM: 15%
Most allow the risk management lead a moderate to broad scope of authority.
Balance between risk control and functionality/openness.
81% of institutions do not include IT risk in their institution’s strategic plan.
Compliance

- No process/procedures
- Ad hoc/informal
- Formal program planned
- Formal program in place
Compliance programs in place

- 57% All institutions
- 23% Institutional compliance
- 16% IT compliance
- 4% Institutional compliance and IT compliance
Compliance lead allowed a very broad scope of authority.
IT Compliance Issues

- We have a process in place for reviewing and updating our IT compliance practices.
- We have enough qualified staff devoted to IT compliance.
- We have adequate staff hours devoted to IT compliance.
- We have an adequate budget devoted to IT compliance.

Percentage of institutions
Governance
Those with an ITGB are more likely to:

• Involve other departments in decision-making
• Influence leadership
• Formulate binding policy
• Guide IT risk management
• Have a clear IT vision, mission, or strategy
ECAR Maturity Indices

• Provide starting point for institutions to assess strengths and weaknesses
• Allow comparisons across the institution to benchmark progress across time or departments
• Allow comparisons inter-institutionally to provide peer comparisons
Risk Management Maturity

Acceptance

Risk assessment/management

Communication/End-user management

Investment

OVERALL

2.9
Communication/End-User Management

- Communication about IT risk throughout the organization
- Management of end-user activities
Acceptance

• Lack of resistance of faculty, staff, and administration to risk management efforts
Risk Assessment/Management

- Identifying, tracking, prioritizing, and reporting risks
- Implementing policies and controls
- Involvement of leadership
Investment

- Adequate investment in risk management staff and services
More mature institutions...

- Have a formal risk management program (enterprise or IT)
- Allow the risk management lead a broad scope of authority
- Use a framework (any framework) for RM
- Are more effective in addressing specific IT risks
More mature institutions ALSO...

- Invest more in IT compliance
- Are better at reviewing and updating IT compliance practices
- Have less difficulty addressing compliance rules and laws
- Have better support from leadership and faculty in IT governance issues
- Have better IT governance in every respect
Panel Discussion
Today’s Panelists

Patrick J. Feehan, Director, IT Policy and Cybersecurity Compliance  
Montgomery College

Cathy Bates, Associate Vice Chancellor and CIO  
Appalachian State University

Michael J. Chapple, Senior Director, IT Service Delivery  
University of Notre Dame