IT GOVERNANCE, RISK, and COMPLIANCE in Higher Education

IT GRC programs in place

- All institutions
- IT governance 56%
- IT risk management 31%
- IT compliance 27%

Who leads IT GRC?

If formal programs exist, CHIEF INFORMATION SECURITY OFFICERS or CHIEF INFORMATION OFFICERS are most likely to lead them.

They lead with a moderate to broad scope of authority, meaning they have adequate leadership involvement and backing for decisions made.

GRC maturity

Institutions with either an enterprise risk management or an IT risk management program have higher scores on all four maturity dimensions.

Institutions with more-mature IT risk management programs have stronger IT governance and IT compliance programs.

The gaps between the importance of and the effectiveness in addressing these IT risks are large.

The most important IT risks to address concern information security, privacy, and access.

Higher education institutions maintain a balance between risk control and functionality/openness.

For the unique mission of higher education, risk management leads must hone the soft skill of negotiating between the provision of risk control and ensuring data and processes are accessible and useful.

Institutions with formal IT governance bodies are more likely to involve others in decision making, make better investment decisions, have more support from leadership, faculty, and other stakeholders, and participate more in strategic planning and policy making.

When it comes to IT compliance:

2/5 say We have a process in place for reviewing and updating our IT compliance practices.

1/5 say We have an adequate budget devoted to IT Compliance.

The EDUCAUSE IT GRC program provides resources that help you define and implement IT governance, risk, and compliance activities on campus. educause.edu/it-grc.

June 2014