Understanding Cybersecurity Policy from a Risk Management Lens

Rodney Petersen, Managing Director of Washington Office

July 16, 2013
Higher Education Information Security Council

- Awareness & Training (People)
- Governance Risk Compliance (Process)
- Operations & Practices (Technology)
Paradigm Shift: Print to Digital
Paradigm Shift: IT to Data
Paradigm Shift: Critical Infrastructure

- People Assets
- Physical Assets
- Cyber Assets
Data is Central

Data

- Management
- Privacy
- Analytics
- Availability
- Protection
- Quality

EDUCAUSE
What should we do in IT?

- Implement Governance
  - Authority, decision-making, accountability, standards, policies, and procedures

- Assess Risk
  - Threats and vulnerabilities to information security, privacy, business continuity

- Enforce Compliance
  - International, federal, state, local laws, standards, and contracts
Governance

Institutional
- Governing Board
- Fiduciary Responsibilities

InfoTech
- Information Technology Council
- Vision, Strategy, and Priorities

InfoSec
- Information Security Governance Committee
- Process and Framework for Information Assurance

Identity
- Identity and Access Management Committee
- Policies and Coordination of Digital Credentials

Data
- Data Governance Council
- Policies and Processes for Data Stewardship
Data Governance

Data governance is an emerging discipline with an evolving definition. The discipline embodies a convergence of data quality, data management, data policies, business process management, and risk management surrounding the handling of data in an organization.

Wikipedia
Types of Risks

- Strategic
- Operational
- Financial
- Legal
- Reputational
Risk Management Steps

- Asset Identification
- Risk Assessment
- Risk Mitigation
- Monitoring and Evaluate
Layers of Compliance

- Institutional
  - Athletics
  - Employment
    - Students
    - Research
      - Business
      - Information Technology

- IT Compliance
  - Data: FERPA, GLBA, HIPAA, PCIDSS . . .
  - Tech: P2P Filesharing, Export Controls . . .
The Higher Education Compliance Alliance was created to provide the higher education community with a centralized repository of information and resources for compliance with federal laws and regulations.

Spearheaded by the National Association of College and University Attorneys (NACUA), the Compliance Alliance is now comprised of 29 participating associations representing a broad cross-section of higher education interests.

Featured Resources

- Compliance 101: A Guide to Building Effective Compliance Programs
  November 1, 2011
- Policy Statement and Order on Non-Commercial Educational Radio Stations Operated by College and University Students
  May 13, 2013
- The Impact of Export Controls on Higher Education Scientific Institutions Conference
  Mar 26, 2013
- The Application of Title VII and the ADA to Applicants or Employees Who Experience Domestic or Dating Violence, Sexual Assault, or Stalking
- CRS Report: The Family Educational Rights and Privacy Act (FERPA): A Legal Overview
  May 1, 2013

Compliance News

- NCAA Punishes Mississippi State U. for Recruiting Violations in Football
  Mar 7, 2013
Policy Process Lifecycle

- Event
- Compliance
- Regulation
- Action
- Legislation
Discussion

- How is **Governance** implemented at your institution?
- How is **Risk Management** applied to data and other cyber assets?
- How is your institution organized to address **Compliance** obligations?