Impact of Cloud Computing on Standards

- In cloud computing, contract is king
  - Manage technological and compliance control via contract when technology is off premise
  - Assumes a different skill set among negotiators
  - Requires collaboration among principle stakeholders on campus

- Fulsome provisions, keep up with the Jones
  - Sign of the scramble past

- Introducing standards
  - Privacy, security and accessibility
Legal

- Basic contract formulation, negotiation and execution
  - Consideration

- Basic contract provisions
  - Jurisdiction, conflict of laws, warranty, etc.

- Regulatory Compliance
  - Coordination with privacy/security officers
  - Compliance Office
  - Risk Management
Technology

• Plug-In
  • Technologically
  • Authentication
  • Harmonization with business process

• Functionality
  • How to
  • Harmonization with business process

• Policy
  • Institutional and operational
  • Harmonization with business process
Communications

• Translation of rules, guides and best practices from the law, policy, security and technology of the tool to the end user.

  • Information Management
  • Steward and Custodian Roles, Rules and Obligations
    • Appropriate Use
Information Security

• Technical controls
  • Cryptography, networks, systems, applications, authentication and authorization

• Process controls
  • Risk Assessment

• Incident Management
  • Who does what, when and who pays

• Data privacy
  • How protected, preserved, managed and/or destroyed according to contract, i.e. storage and transmission

• Administrative controls
  • Audit
• WHAT DOES THE COMPANY DO WITH THE DATA AND INFORMATION UNDER THEIR CONTROL, AND IS IT IN COMPLIANCE PROFILE OF THE INSTITUTION FOR THE TYPE OF DATA/INFORMATION USED

• How does the vendor’s appropriate use policies harmonize with institution?
  • Especially stewardship and custodianship roles

• Harmonization of information technology, information and risk management processes.
• Among these distinct areas, what is the common denominator?
STANDARDS
Standards

• Contract law, standards of contract formation, and regulatory compliance exist in the form of laws.

• Technology has “code” in terms of software and “policy” in terms of operations

• Security and Privacy rules, regulations and guidelines

• Policy harmonizes international, national and local law with institutional compliance and risk management profile.
Regulatory Compliance Prominent Examples

- Family Education Rights Privacy Act
  - Privacy and “reasonableness” standard for security

- Financial Services Modernization Act
  - Privacy and security

- Health Insurance Portability Accessibility Act
  - Privacy and Security

- Health Information Technology for Economic and Clinical Health Act
  - Technical security controls

- Americans with Disabilities Act
  - W3C 2.0 AA or section 508 (soon refresh)
Security and Privacy Standards

- International Standards Organization (ISO)
  - 2700 series
  - Emphasis on 27013 and 27018 (technical security controls and data privacy)
  - Incorporates European Union data protection rules

- National Institute of Science and Technology
  - 800-171
  - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
  - U.S. centric
Criminal Justice Information Service (CJIS)

- Storage and transmission of data
  - Highest standard
  - Incorporates not only security controls and privacy practices but evidentiary needs and chain of custody for criminal court system

- CJIS Policy Resource
Why?

• Because law enforcement requires not merely appropriate executive of body worn cameras but the proper transmission and maintenance of the video content.

• Evidentiary standard levels cross-examination and takes guess work out of the institutional or criminal process

• Chain of custody a stable of “reasonable doubt,” especially with sophisticated Photoshop capabilities

• Level field favors neither prosecution (law enforcement or institutional)

• No political or viewpoint misuse of data allowing it to speak for itself
Recap: Cloud Computing and Procurement

- Cloud computing changes the game for procurement, regulatory compliance and risk management.

- Contract is kind in cloud computing.

- Therefore, procurement process no longer linear and asynchronous but dynamic and synchronous planning with specific experts and stakeholders.
Recap: Cloud Computing and Standards

• The necessity of an entity to use the contract process and provisions for regulatory compliance and risk management has resulting in a reliance on the use of internationally and nationally recognized standards.

• Rather than spelling out every provision for data and information privacy practices and security technology, acceptable use and audits, standards provide a short hand between parties.

• And create a foundation against which vendors can design and entities can manage liability of their information technology operations and effectiveness.
Recap: The Standards

• For entities that use products and services and/or that operate internationally, the International Standards Organization (ISO) hosts those most comprehensive set.
  • Information privacy and security contained in the 27000 series.

• For entities that operate mainly within the United States, and/or that must comply to US standards because of grants or other government contracts, the National Institute of Standards and Technology, or NIST, has a nationally comprehensive set.
  • Information privacy and security contained in 800-171
Recap: Cloud Computing, Standards and CJIS

• Cloud computing emerges along side other emerging technologies such as body worn cameras for law enforcement.

• The transmission and storage of video metadata and content captured on body worn cameras for law enforcement requires attention at the procurement stage of contracting.

• Given its use in institutional disciplinary proceedings as well as U.S. courts, law enforcement body worn camera metadata and content must be kept under the CJIS standard.
Cloud Computing, Standards and CJIS

- All of a piece!