

Information Security Got ^ Risk?

Cuc N. Du, ISO
Chancellor's Office
November 6, 2008

Agenda

- Who We Are
- Objectives
- Roles and Responsibilities
- Current Initiatives
- Future Initiatives
- Panel Discussion

Information Security Advisory Committee

- Organized in 2004
- A forum with representation from key information security leaders at the CSU
- CSU-wide representation to develop and validate policies

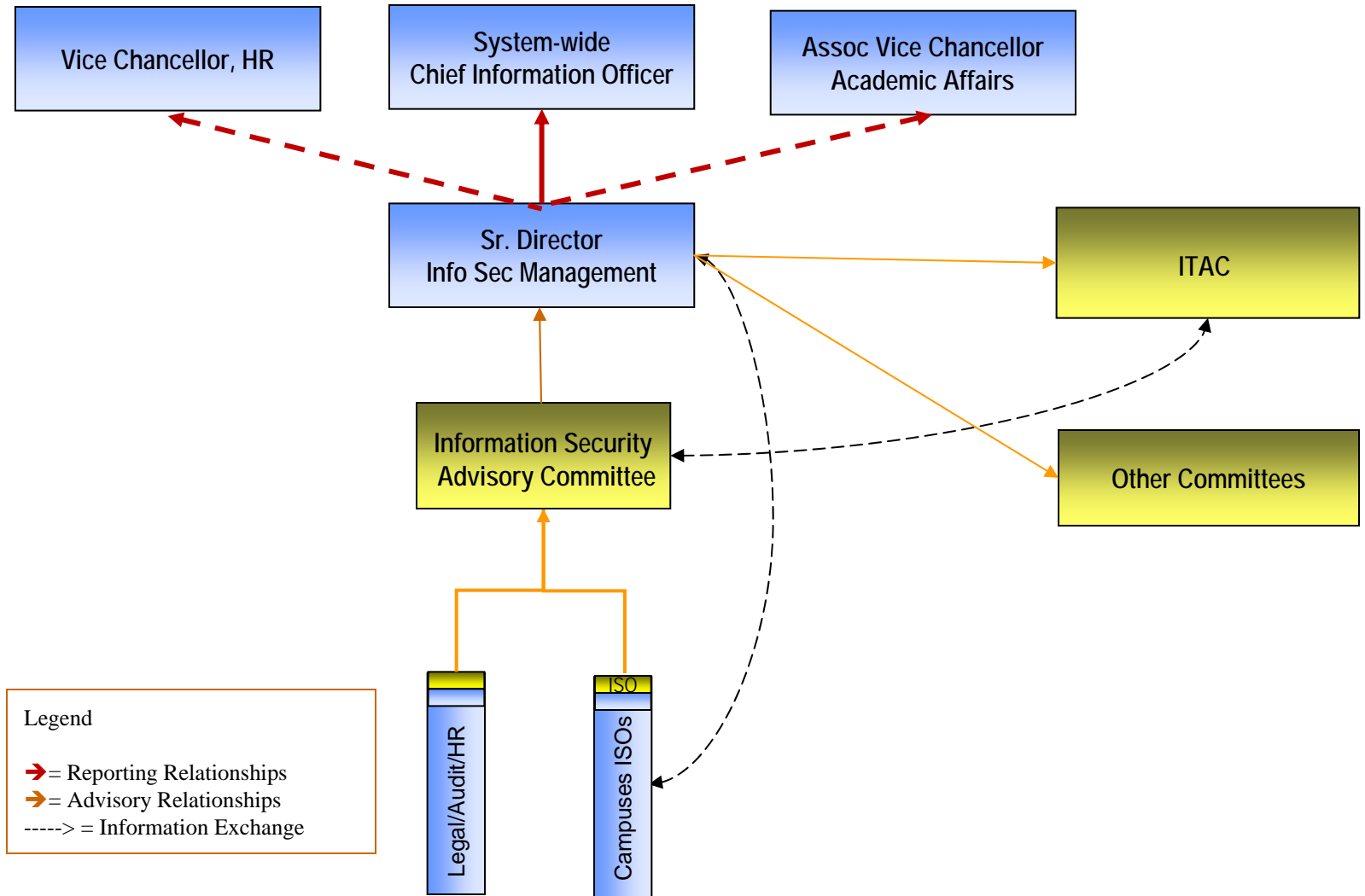
ISAC Objectives

- Develop a common understanding of...
 - Information Security Governance Initiative
 - Information Security Policy Framework
- Establishes a forum to identify and safeguard critical information assets
- Provides for system-wide representation to validate policy
- Enables a proactive process to communicate CSU information security requirements

ISAC Roles and Responsibilities

- Develop Policy Framework consisting of information security policies, standards, and high level processes
- Communicate implementation and operational concerns and security-related issues and activities affecting the University
- Raise security concerns for Information Security to research
- Education, Awareness, and Training

Information Security Advisory Committee



Information Security Governance Defined

“Information Security Governance focuses on establishing acceptable information technology security risk thresholds for the University; developing corresponding policies, standards, and processes; and measuring compliance.”

- **Key Characteristics:**

- Senior executive support
- Business driven, rather than information technology driven
- HR, Legal, Internal Audit, & Risk Management alignment

Current Initiatives

- Systemwide Audit
- Systemwide Security Policies & Standards
- Systemwide Security Awareness

Future Initiatives

- Data Classification
- Encryption
- Identity and Access Management (IAM)
- Payment Card Industry Data Security (PCI DSS)
- Risk Assessment Management

Panel Discussion

Panel Speakers

- Al Arboleda – ISO, Pomona
- Brooke Banks – ISO, Chico
- Jason Musselman – Network Security Analyst, Sacramento
- Javier Torner – ISO, San Bernardino

Topics of Discussion

- Convergence of Risk Management and Information Security
- e-Discovery
- PCI Compliance
- Risk Assessment Framework

Convergence of Risk Management and Information Security

*Jason Musselman, - Network Security Analyst,
Sacramento*



e-Discovery

Brooke Banks – ISO, Chico



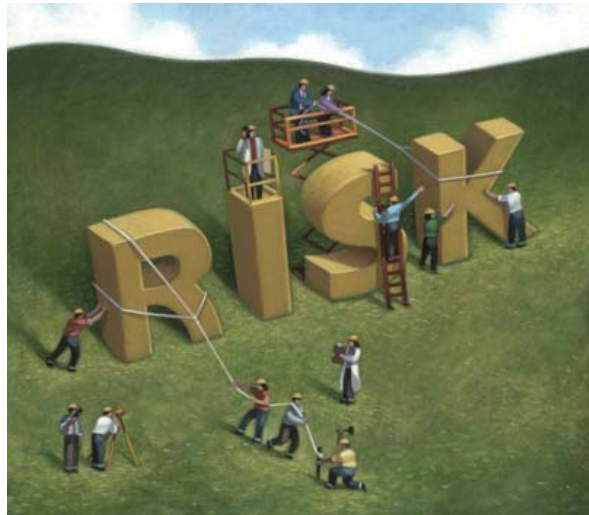
PCI Compliance

Al Arboleda – ISO, Pomona



Risk Assessment Framework

Javier Torner – ISO, San Bernardino



Resources

E-Discovery

- http://www.calstate.edu/gc/hot_topics_022208.shtml

PCI Compliance

- <https://www.pcisecuritystandards.org/>

Risk Assessment Framework

- <http://connect.educause.edu/Library/Abstract/RiskManagementFramework/36695>
- <https://wiki.internet2.edu/confluence/display/secguide/Risk+Management+Framework>
- <http://www.cert.org/octave/> (Operationally Critical Threat, Asset & Vulnerability Evaluation)

Effective Security Practices Guide from Educause

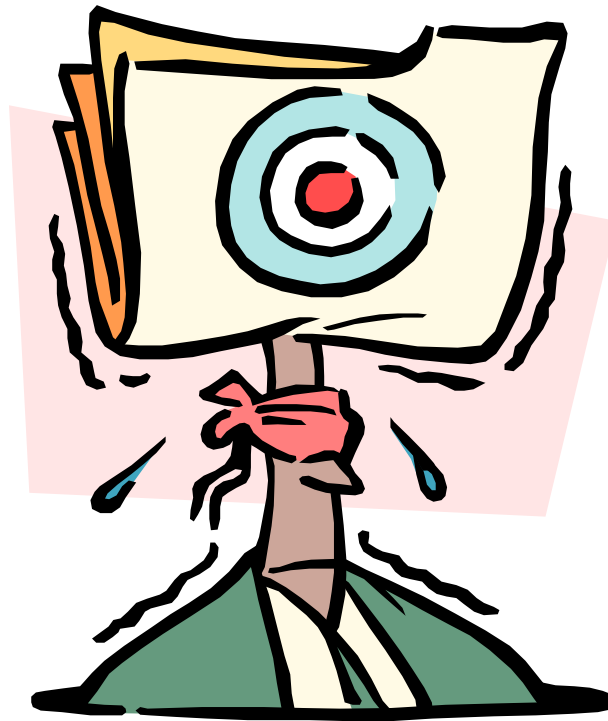
- <https://wiki.internet2.edu/confluence/display/secguide/Home>

ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management

Contacts

- Al Arboleda – ISO, Pomona
 - aarboleda@csupomona.edu
- Brooke Banks – ISO, Chico
 - bfbanks@csuchico.edu
- Cuc N. Du – ISO, Chancellor's Office
 - cdu@calstate.edu
- Jason Musselman – Network Security Analyst, Sacramento
 - jason@csus.edu
- Javier Torner – ISO, San Bernardino
 - jtorner@csusb.edu

Questions?



CSU The California State University

www.calstate.edu