2011 Risk Assessment Workshop
Agenda

- Risk Assessment Strategy for Texas State
- Review Server Management responsibilities
- Device Registration Application
- Risk Assessment using ISAAC
Risk Assessment Strategy at Texas State

- **What we’re doing in 2011**
  - Device Registration - enhanced
  - ISAAC (Information Security Awareness, Assessment, and Compliance) - enhanced
  - Penetration Testing by IT Security
    - Core Impact, open source tools
  - Confidential Information Discovery
    - Identity Finder
Risk Assessment Strategy at Texas State

❖ Results from 2010

- 68 assessments, 669 systems
- 21 confidential, 47 non-confidential
- Average compliance of 94%
- Over 99% backup at least daily and apply regular patches
- High compliance areas include:
  - User ID and password usage, Audit logs usage, Awareness training, Non-Disclosure Strategy
- Compliance concerns include
  - Non-disclosure agreements, Encryption Measures, Incorrect password and inactive workstation lockout
Server Management Responsibilities

- Required for all server-level devices
  - See UPPS 04.01.09
  - [http://www.txstate.edu/effective/upps/upps-04-01-09.html](http://www.txstate.edu/effective/upps/upps-04-01-09.html)

- DIR Requirements
  - annual risk assessment
  - Confidential information
  - Disposal of electronic media
What's New?

- **Device Registration**
  - Activate/Deactivate device option

- **ISAAC Risk Assessment**
  - Modified questions reflecting the updated TAC 202
  - Updated HIPAA Module (reduction of over 100 informational questions)
  - Updated PCI module which covers requirement changes
  - Enhanced navigation within assessments
Device Registration

- Device Registration application
  - [https://tim.txstate.edu/ndmrs/](https://tim.txstate.edu/ndmrs/)
  - Secure application (HTTPS)
  - Search feature
  - Activate/Inactivate feature
ISAAC

- Assess Texas Administration Code (TAC) 202 compliance
- Accepted method for conducting risk assessment

https://isaacs.tamu.edu/
Hands-On Device Registration And ISAAC Assessment