

# 2009 Risk Assessment Workshop



# Agenda

- Risk Assessment Strategy for Texas State
- Device Registration Application
- Introduction to ISAAC and User Registration
- Break
- Risk Assessment using ISAAC
- Q&A

# Risk Assessment Strategy at Texas State

- DIR Requirements - annual risk assessments
- Results from 2008
- What we're doing in 2009
  - Device Registration
  - ISAAC (Information Security Awareness, Assessment, and Compliance)
  - Penetration Testing
    - Core Impact, open source tools
  - Confidential Information Discovery
    - Identity Finder reports
    - Interviews

# Risk Assessment Strategy at Texas State

- DIR Requirements - annual risk assessments
- Results from 2008
  - 65 assessments, 295 systems
  - 33 confidential, 32 non-confidential
  - Average compliance of 85.6%
  - 95% backup at least daily
  - 91% at patch within 2 days of patch release
  - High compliance areas include:
    - User ID and password compliance
    - Awareness training
    - Anti-virus software scanning and updates
  - Compliance concerns include:
    - Non-disclosure agreements
    - automatic workstation lockout

# Device Registration

- Required for all server-level devices
  - See UPPS 04.01.09
  - <http://www.txstate.edu/effective/upps/upps-04-01-09.html>
- Device Registration application
  - <https://virtualwebapp.cr.txstate.edu/ndmrs/>
  - Secure application (HTTPS)
  - Search feature



# Hands-On Device Registration

# ISAAC

- ISAAC Development
- Purpose:
  - Assess Texas Administration Code (TAC) 202 compliance
  - Accepted method for conducting risk assessment
- <https://isaacs.tamu.edu/TAC/index.cfm>
- User ID Registration
  - Manager of the server/device



# Hands-On ISAAC Assessment

Q & A