What the Auditor’s Look For

David Maggard, CPA, CISA
System Internal Audit
Real Message:

Don’t Focus on the Auditors
Areas included in recent IT audits

- IT Governance
- Patch Management
- Password Management
- Data Privacy/Data Classification
Areas included in recent IT audits (con’t)

• Program Versions
• Administrator Accounts
• Change Management
• Disaster Recovery & Backups
Areas included in recent IT audits (con’t)

• Physical Security
• Identity & Account Management
• Risk Management
• End User Training
IT Governance

• IRM/CIO and ISO reporting lines
• IT advisory or governance committees
• DIR security controls catalog.
• Procurement of Systems (Are purchases > $250,00 reported to the SCIO?)
Patch Management

- One of our top 2 most reported issues
- Review causes behind any patching gaps
- Review system versions to determine if they are up to date and/or still supported
Password Management

• Our other most reported issue
• Password Length
• Password Expiration
• Password Complexity
• Password History
• Password Lockout Attempts
• Locking Screensaver
• Compare against each institution’s standards
Data Privacy/Data Classification

• Classification of data

• Identification of confidential information (i.e. SSN and credit card numbers)
  o Scanning tools such as Identity Finder
  o Data Loss Prevention tools such as Sophos

• Identification and encryption of confidential data
Remaining Areas

• Program Versions
• Administrator Accounts
• Change Management
• Disaster Recovery & Backups
• Physical Security
• Identity & Account Management
• Risk Management
• End User Training
Program Versions

• Internet Explorer- Version 11

• Java- Version 8 or 9 (Any version below 8 is not supported as of 4/2015)

• Anti-Virus Software
Administrator Accounts

- Determine if administrative accounts are appropriate

- Determine if administrators use the account or access privilege most appropriate for the requirements of the work being performed
Change Management

- Changes authorized, tested, and approved appropriately

- Change management process segregated
Disaster Recovery & Backups

• Current Disaster Recovery Plan (DRP)

• Evidence of periodic testing and updates

• Backup process in place

• Monitoring of backup process to ensure it is working as planned
Physical Security

• Server room security including monitoring of access

• Server room environmental controls
Identity & Account Management

• Terminated User Testing
• New User Testing
• Periodic User Access Reviews
Risk Management

• Annual IT risk assessments (eg. Archer/SPECTRIM)

• Information Security Plans submitted to DIR by October 15 of even numbered years starting in 2016 (TX Gov’t Code 2054.133)

• Information Security Programs approved annually by CEO (TAC 202.70) and receive independent biennial reviews (TAC 202.76)
End User Training

• Review TrainTraq data to determine if Security Awareness Training was assigned and completed timely
The End....

Questions?