

## IT Audit & Risk Assessment

Timothy Agee  
tagee@ageesolutions.com

December 12, 2006

---

---

---

---

---

---

---

## To Download the Latest Copy of this Presentation

and Links to  
IT Audit Resources  
[www.ageesolutions.com](http://www.ageesolutions.com)

Navigate to > Resource Library

---

---

---

---

---

---

---

## SAS 104 - 111

- Effective - 12/15/2006
- Business Environment (Internal Controls)
- Risk Assessments
- Audit Procedures based on Risk
- Audit Sampling and Evidence
- <https://www.cpa2biz.com/stores/risk>

---

---

---

---

---

---

---

## Why are we talking about IT Audit?

- \*Regulatory compliance\*
  - Sarbanes-Oxley (SOX)
  - HIPAA
  - PCI, GLBA, etc., etc.,
- Integration of IT
  - Thinking outside of the "Black-Box"
  - IT Governance & Accountability

---

---

---

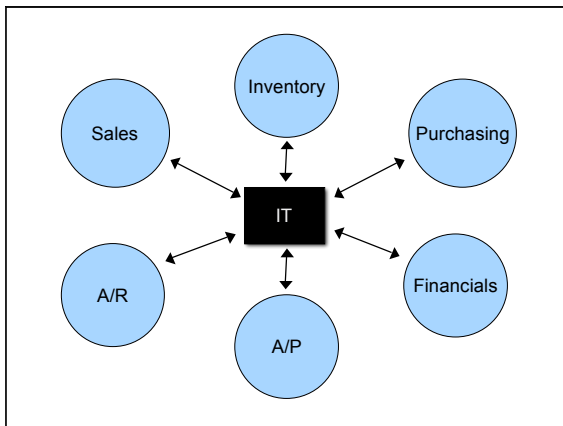
---

---

---

---

---



---

---

---

---

---

---

---

---

## Role of the IT Auditor

- Assist with integration of IT into the overall business environment (*How?*)
- Assist Management with IT risk assessment
- Ensure that IT controls are properly implemented
- Provide continuous evaluation of the effectiveness of IT controls

---

---

---

---

---

---

---

---

## Outside of the “Black Box”

- Evaluate IT in view of business objectives
- Ensure data owner involvement in IT processes
- Coordination of IT controls and application/financial controls
  - Reconciliation
  - Review

---

---

---

---

---

---

---

## Determining Scope

- Business/Operational objectives
- Regulatory compliance (SOX, HIPAA)
- Risk assessment
  - Financial
  - Operational
- Critical applications & systems

---

---

---

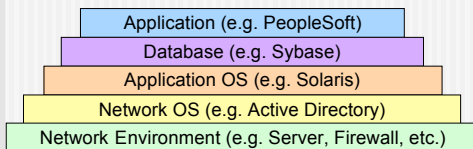
---

---

---

---

## Audit Scope



*Must understand how controls in one area affect controls in the other areas*

---

---

---

---

---

---

---

### IT Entity Level Control Examples

- Written policies and procedures
  - Security, HR, etc.
  - **Communication to employees**
- Control framework (Risk assessment)
- Control environment
- Training program

---

---

---

---

---

---

---

---

### IT General Control Areas

- Security (Logical Access)
- Manage Changes\*
  - Systems Development Life Cycle (SDLC)
- Manage Data
- Manage Operations
- *End-user computing*

*\*Can have significant impact on application controls*

---

---

---

---

---

---

---

---

### Security (Logical Access)

---

---

---

---

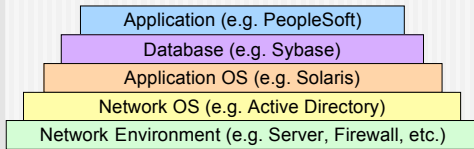
---

---

---

---

## Security Scope - Which areas are important?



Must understand how controls in one area affect controls in the other areas

---

---

---

---

---

---

---

---

## Security - Risks

- Business data owners do not approve system access to their data
- Access to in-scope applications and databases is not adequately protected
- *Confidential data could be compromised*
  - *Intellectual property*
  - *Patient / Customer Data*

---

---

---

---

---

---

---

---

## Security - Risks (cont.)

- Terminated employees access rights are not removed on a timely basis
- Attempts to gain access to systems are not monitored
- Network is not protected from external threats
- Physical devices are not properly protected

---

---

---

---

---

---

---

---

## Security Controls

- System Security Configuration
  - General settings
    - e.g. System values on AS400
    - IP services (FTP, HTTP)
    - Auditing enabled
  - Password controls (see next slide)
  - Idle time-out

---

---

---

---

---

---

---

## Security Controls (cont.)

- Passwords
  - Minimum length / other complexity
  - Temporary passwords (one-time use)
  - Forced password changes
  - Password history
  - Account lockout
- *Two-Factor Authentication*
- *Biometrics*

---

---

---

---

---

---

---

## Security Controls (cont.)

- User Access Authorization / Setup / Monitoring
  - New-user setup
  - Terminations
  - Transfers
  - Periodic review of access rights
  - Monitoring of user access
  - ***Ensure that business data owner is involved!!***

---

---

---

---

---

---

---

## Security Controls (cont.)

- New User Setup / Employee Transfers
  - Process for requesting access
    - Who can make this request?
  - Process for approving access (data owner)
    - Who can approve access?
  - How is access given? (*Role-based?*)
  - Does access given match what was approved?

---

---

---

---

---

---

---

---

## Security Controls (cont.)

- Terminations
  - Timely removal of logical access
    - Logins, keycards, etc.
  - How are system owners notified?
    - Who provides notification?
    - *Manager?*
    - *Human Resources?*
    - *Payroll?*

---

---

---

---

---

---

---

---

## Security Controls (cont.)

- Periodic Review of Access
  - Performed by data owners
    - Who provides this information?
  - Performed at least quarterly
    - Review is documented
    - Appropriate action is taken
  - Detective control for inappropriate access
    - *Terminations and Transfers*

---

---

---

---

---

---

---

---

## Security Controls (cont.)

- Monitoring of Access
  - Repeated failed logon attempts
  - Attempts to access sensitive data
  - Use of powerful system logons
  - *How are identified issues addressed?*
  
  - *How are these logs filtered?*

---

---

---

---

---

---

---

## Security Controls (cont.)

- Powerful User Rights (Examples)
  - Administrator rights (Windows)
  - Root access (Unix)
  - Special authorities (AS400)
  - *What accounts have these rights, or what users know these passwords?*
  - *Password controls for these accounts?*

---

---

---

---

---

---

---

## Security Controls (cont.)

- Network security
  - Virus protection
    - Regular / Automated updates
    - Regular / Automated scanning
  - Firewalls
    - Appropriately placed
    - Appropriately secured
  - Wireless
    - Encryption enabled (WEP, WPA, etc.)

---

---

---

---

---

---

---

## Security Controls (cont.)

- Physical security
  - Access to data center (approval process?)
  - Battery backup
    - Generator?
    - Alternate Power Source?
  - Fire suppression
  - Climate control (detection?)
  - Raised floor

---

---

---

---

---

---

---

---

## Security Controls (cont.)

### *Special Considerations:*

- Social Engineering (*SPAM, Phishing*)
  - Security awareness and training
- Encrypted Data/Communication
  - WAN, Email, etc.
  - Data on local hard drives

---

---

---

---

---

---

---

---

## Manage Changes

---

---

---

---

---

---

---

---

## Manage Changes - Scope

- Applications / Databases
  - What is the source of the change?
    - Internal development
    - Third party
- Operating System
  - Patches
  - Service packs
  - Upgrades

---

---

---

---

---

---

---

---

## Manage Changes - Risks

- Changes to production applications might not be authorized
- Changes to production applications might produce unexpected results
  - *Requirements might not be fully documented*
  - *Changes might not be fully tested*
  - *Changes might negatively impact application security*
  - *Changes might interrupt operations*

---

---

---

---

---

---

---

---

## Manage Changes - Controls

- Change Classification
  - Separate streams for different levels of risk / complexity
  - Identified when project is in the planning stage

---

---

---

---

---

---

---

---

### Manage Changes - Controls (cont.)

- Change Approval
  - Requests
    - Business data owner / IT application owner
  - Testing
    - Requestor / Business data owner / Developer
  - Promotion / Migration
    - Business data owner / IT application owner

---

---

---

---

---

---

---

---

### Manage Changes - Controls (cont.)

- Access to Production Source-Code
  - Programmers/developers do not have access to production source-code or tables
  - Separate development environment
  - Version control
  - Migration process / Approval

---

---

---

---

---

---

---

---

### Manage Changes - Controls (cont.)

- Testing Documentation
  - Developer testing (Unit & System Testing)
  - User testing (User Acceptance Testing)
  - Quality Assurance

*Documentation of Test Plans & Results*

---

---

---

---

---

---

---

---

### Manage Changes - Controls (cont.)

- Emergency Changes
  - *Required changes where time is not available for the formal change management process*
  - Temporary access to production code
  - Mechanism for monitoring/auditing access
  - Mechanism for disabling access
  - Mechanism for obtaining proper approvals / testing once emergency is over

---

---

---

---

---

---

---

---

### Manage Changes - Controls (cont.)

- Operating System Patches / Upgrades
  - Methodology for testing
    - Non-critical servers/workstations
  - Methodology for deployment

---

---

---

---

---

---

---

---

### Systems Development Life Cycle (SDLC)

- *New Systems or Large Change Projects*
  - Feasibility
  - Requirements
  - Design / Selection
  - Development / Configuration
  - Implementation
  - Post-Implementation Review

---

---

---

---

---

---

---

---

## Systems Development Life Cycle (SDLC)

- Deliverables (examples)
  - Security plan
  - Disaster recovery plan
  - Data conversion plan
  - Test cases (for UAT)
  
- *The IT Auditor can ensure that the necessary controls are included in the implementation of the new system*

---

---

---

---

---

---

---

---

## Manage Data

---

---

---

---

---

---

---

---

## Manage Data - Risks

- Critical data is not available
  - *Hardware failure, disaster, corruption, etc.*
- Critical data is lost
  - Critical data is not being backed up
  - Data backups are not sufficient to allow for successful data recovery procedures
  - Disaster recovery is not possible

---

---

---

---

---

---

---

---

## Manage Data - Controls

- System redundancy (availability)
- Regular backups
  - Monitoring / Error resolution
- Backup retention
- Off-site rotation
- Periodic restore testing

---

---

---

---

---

---

---

---

## Manage Data - Controls (cont.)

- Business Continuity / Disaster Recovery
  - Resuming critical processes and data
    - Documented recovery plan/procedures
    - Training/awareness
    - Regular testing / documentation
    - Alternate processing facilities
  - *Mechanism should be based management's tolerance for downtime and data loss*

---

---

---

---

---

---

---

---

## Manage Operations

---

---

---

---

---

---

---

---

## Manage Operations - Risks

- Operations procedures are not performed or not completed resulting in incomplete or inaccurate data
  - Processes might be duplicated
  - Processing errors might not be detected or resolved

---

---

---

---

---

---

---

---

## Manage Operations - Controls

- Monitoring / tracking of job / batch execution
  - Manual jobs - documentation of completion
  - Automated jobs - documentation of review
- Error identification and resolution
  - Error tracking

---

---

---

---

---

---

---

---

## IT Audit Resources

- [www.isaca.org](http://www.isaca.org)
  - COBIT - IT Control Objectives
  - IT Control Objectives for SOX
- [www.auditnet.org](http://www.auditnet.org)
  - Audit programs
- <https://www.cpa2biz.com/stores/risk>
  - SAS 104 - 111
  - Standards for Risk Assessment

---

---

---

---

---

---

---

---

---

## Questions or Comments

Timothy Agee  
[tagee@ageesolutions.com](mailto:tagee@ageesolutions.com)  
[www.ageesolutions.com](http://www.ageesolutions.com)

---

---

---

---

---

---

---

## To Download the Latest Copy of this Presentation

---

**and Links to  
IT Audit Resources**  
**[www.ageesolutions.com](http://www.ageesolutions.com)**

Navigate to > Resource Library

Latest Revision 12/11/06 - 11:30am

---

---

---

---

---

---

---