Information Technology Internal Controls—Part 2

Presented by the Arizona Office of the Auditor General
October 23, 2014

IT Controls Webinar Series

Part I –Overview of IT Controls and Best Practices

Part II –Identifying Users and Limiting Access

Part III – Network Controls

Part IV– Disaster Recovery Planning

IT Control Issues Covered in this Webinar

- Identifying System Users
- Establishing Roles and Responsibilities
- Controls to Limit Access
- Monitoring Access, Changes & Activity

Terminology

IT – Information technology department personnel within the school district responsible for managing the hardware, software, systems, and networks of the district.

System Manager – Generally the highest supervisory-level user of a system that determines user access for all users of the system.

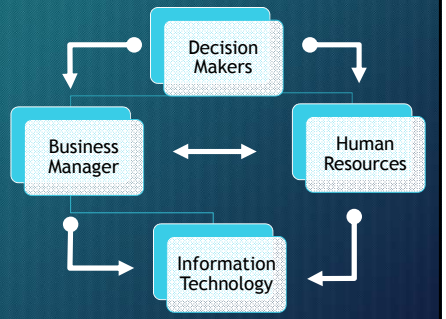
Decision Makers – Those who have the authority to approve and implement any given policy, process, or project within a school district and who are accountable for the outcome.

What are IT Controls?

Defined measures taken to minimize risk and ensure business objectives are being met.

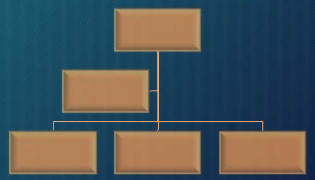
Roles and Responsibilities

Clarify everyone's responsibilities for establishing, operating and monitoring the District's system/network



Roles and Responsibilities

- Identify an IT Administrator for each system and network
  - Manages the system
  - Processes user access request
  - *Ideally* not a user on the system



Roles and Responsibilities

Identifying System Users

- What systems do you have?
- How are these systems used?
- Who needs access?
- What do they need to do in the System?

Roles and Responsibilities

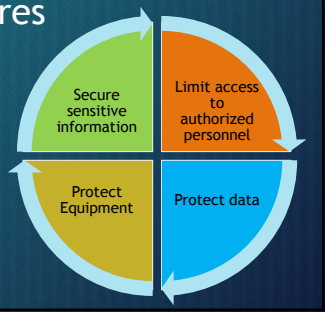
District defined process for access setup

- Employees and contractors
- HR/Personnel communication of changes
- Technology User Agreements
- Manager review of access changes

Access Controls

Establish Policies and Procedures

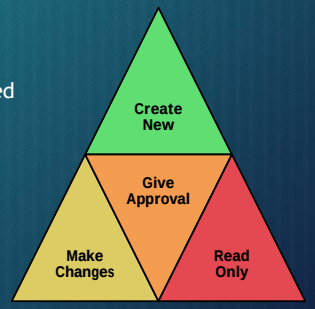
- Logical Access Controls
- Physical Access Controls
- Monitoring



Access Controls

Concept of Least Privilege

- Determine which employees require access based on their job responsibilities
- What data is needed to do the job?
- What do they need to do with that data?



Setting User Access

Segregation of Duties

- Authorization
- Record keeping/reconciliation
- Asset Custody

Setting User Access

Segregation of Duties
- Create a requisition
- Approve purchase requisitions or purchase orders
- Receive ordered items
- Review and process invoices for payment

Compensating controls?

Setting User Access (Employees)

- Role based settings
  - More than one person in the role
  - Similar needs
  - Quicker to do
  - Generic settings in system

  Extra care to ensure appropriate access only!
- Employee specific settings
  - Maybe only one person in role
  - Different needs
  - Takes more time
  - No canned settings in system

  Helps ensure you know the access is appropriate

Separation of responsibilities is key!

Setting User Access (3rd Parties)

Need to establish:
- Who will have access?
- What service will they provide?
- How will district data be protected?

Setting User Access

User Agreements-Use of district property:
- Computers
- Network
- Information
- Confidentiality
- Lawful use
- District policy enforcement

Control Points

User access can be controlled at:

- Network
- Local workstation
- Application
- Database/file

Access Controls

- User Authentication
- Other Barriers to Unauthorized Access
- Monitoring

User ID and Password Setup

1. Administrators create user accounts
   - Require users to change password on initial login
2. User ID's
   - One User ID per employee
   - Unique
   - Identifiable to user

User ID and Password Setup

3. Password Strength Requirements:
   - Minimum of 8 characters
   - Alpha and numeric
   - Upper and lower case characters
   - Special characters (!, @, #, $, etc.)

User ID and Password Setup

4. Confidential
   - Known only to user
   - Not written down by employees
5. Related account secured by lock out after failed login attempts
6. Require passwords to change at least every 90 days

Additional Access Controls

Restricted areas
- Employee work areas – work computers, documentation
- Special facilities – data center, wiring closets, controlled access
- *Controls*: Logout unattended computers, employee badges, access cards or keys

Public areas
- Conference rooms – unsupervised areas, network access
- *Controls*: Disable unused access points, monitoring by secretaries

Access Controls

Server Room
- Access to server room
  - Is the room locked?
  - Who can access? Master keys?
  - Key fobs - monitor access
- Climate control
  - Temperature of room
  - Fire detection - smoke detectors
  - Fire suppression - fire extinguisher, halon, etc.

Access Controls

Computer Access
- Lock computers when not in use
- Time out after a period of non-use
- Passwords should not be shared or openly posted

Monitoring

What to Monitor:
- User access
- User activity
- Changes in user access

How to do it:
- System generated logs/reports
- Manual access logs
- Follow the HR paper trail

Monitoring

Why do we care?

Clear Audit Trail
- Provide Accountability
- Detective Controls
- Corrective Controls

Monitoring

User Access-determine what needs to be monitored

1. Based on segregation of duties
2. Adjust when job duties change
3. Check for removal of terminated employee access
4. Review user accounts periodically
   - Ensure segregation of duties is maintained
   - Ensure user access is appropriate based on current job functions
   - Review to remove unnecessary or inactive accounts

Monitoring

User Access

1. Review user access logs for reasonableness
   - Time of access: suspicious activity
   - Users should not review their own logs

User Access

Do:

- Set user access based on job needs (Least Privilege)
- Use unique user IDs and complex passwords
- Limit generic, vendor and super users to only what is necessary
- Re-evaluate user access when job responsibilities change
- Monitor key activity of users, especially of super users

Don't:

- Automatically use default access set by software packages or vendors
- Use "Admin" or generic IDs
- Assign passwords or share them
- Make super users unless absolutely necessary for job function
- Just add more access when people change jobs
- Set it (access) and forget it

User Access

Do:

- Restrict access to servers and work areas
- Shut down unused ports
- Lock computers when not in use or inactive

Don't:

- Let just anyone walk up to the server or a live terminal
- Leave unused ports live to make it easier to expand later
- Walk away from a logged in computer

Where to start? Self evaluation!

User Access

- Does the district have any super users?
- Are job responsibilities separated to ensure no one person has complete control over a transaction cycle?
- Do personnel have access to more data or processes than they need to do their jobs?

IT Standards and Best Practices

Common Best Practice Frameworks

- COBIT
- NIST
- ISO
- FISCAM
- ITIL
- ASET State Policies
- COSO

Next Webinars

Network Controls
- Security programs
- Incident response
- Websites
- Wireless
- Remote access

Disaster Recovery Plans
- Development
- Testing

Resources

- www.azauditor.gov
  - **IT FAQs on**
  - **USFR**
- Contact Us:
  - By phone: 602-553-0333
  - By email: asd@azauditor.gov