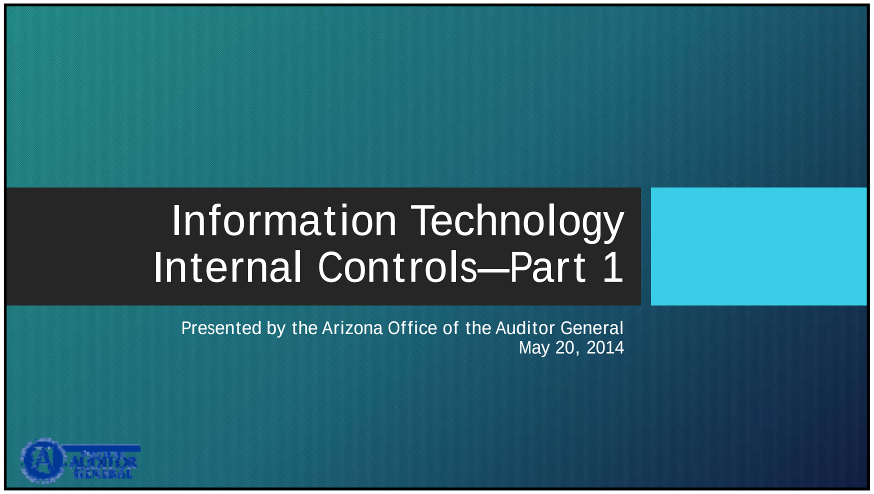


Information Technology Internal Controls—Part 1

Presented by the Arizona Office of the Auditor General
May 20, 2014

IT Controls Webinar Series

Part I -Overview of IT Controls and Best Practices

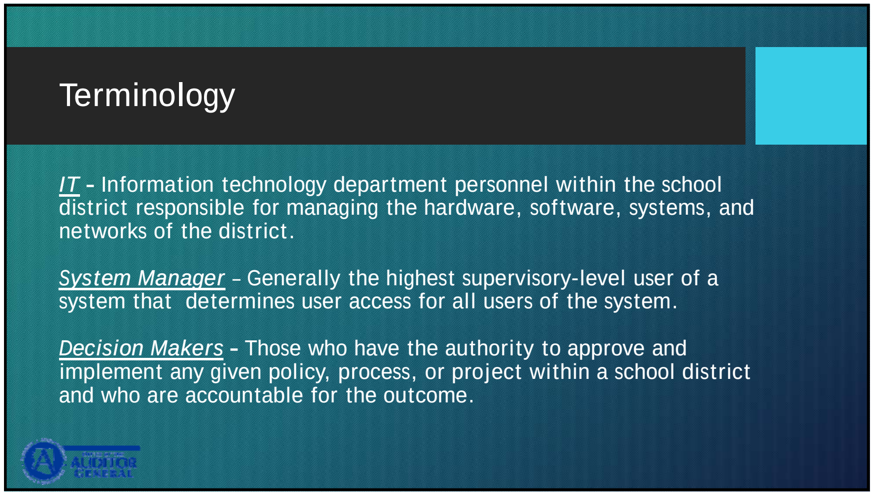
Part II -Identifying Users and Limiting Access

Part III - Network Controls

Part IV- Disaster Recovery Planning

Covered in this Webinar

- What are IT Controls?
  - Why are they important?
- Developing Policies and Procedures
  - What resources are available?
    - Standards and best practices
- General IT Controls
  - Protecting sensitive data
  - Training employees
  - Self assessment

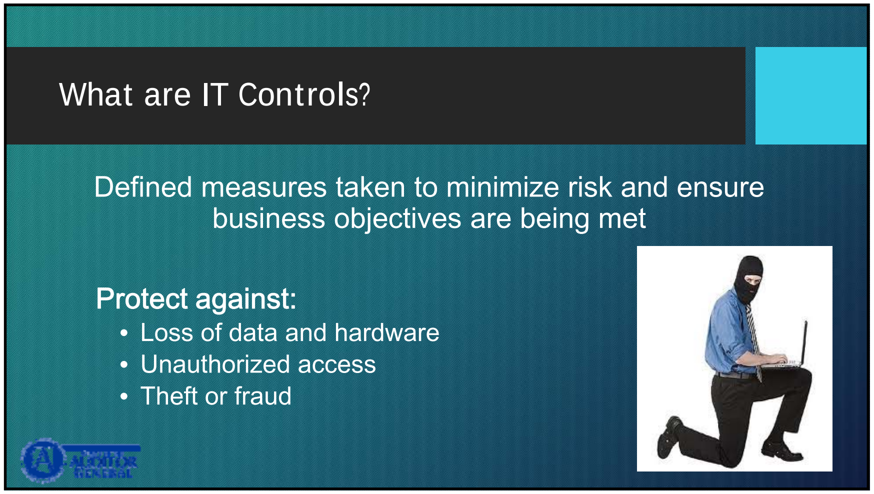


Terminology

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.

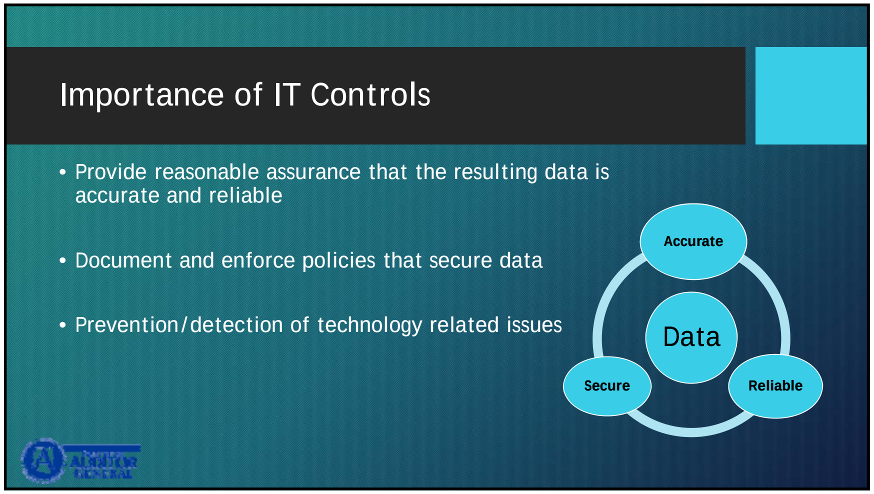


What are IT Controls?

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

Protect against:

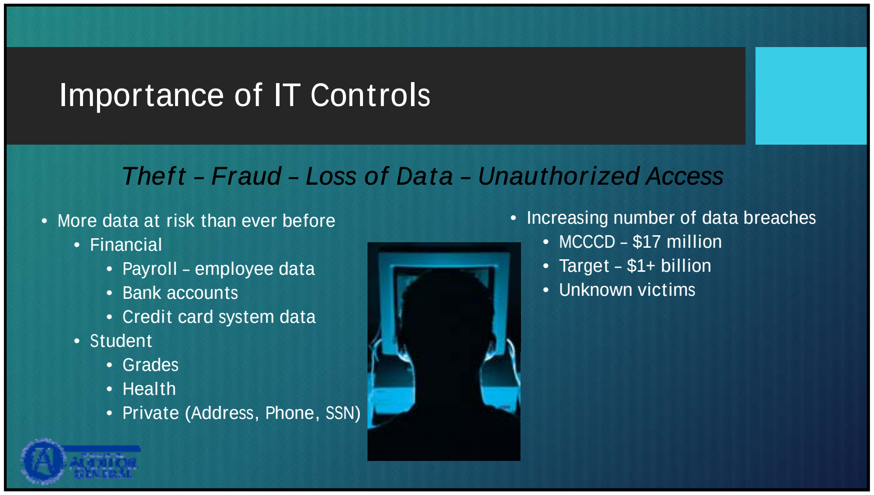
- Loss of data and hardware
- Unauthorized access
- Theft or fraud



Importance of IT Controls

- Provide reasonable assurance that the resulting data is accurate and reliable
- Document and enforce policies that secure data
- Prevention/detection of technology related issues

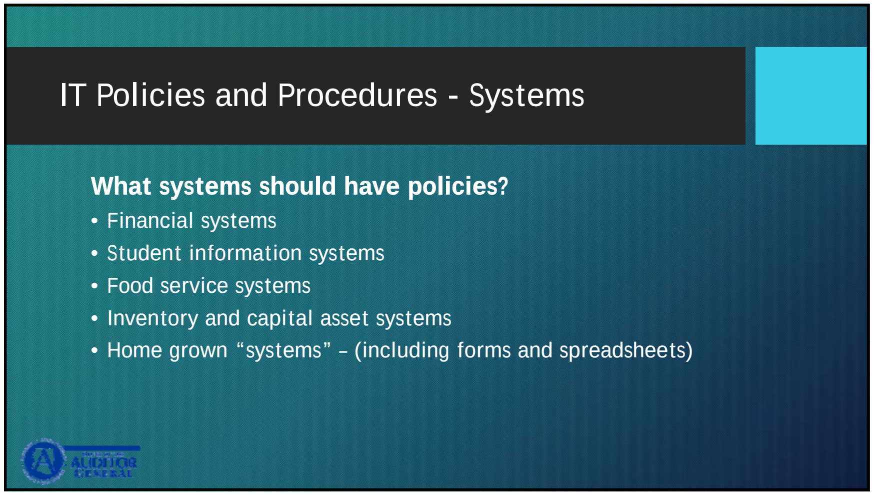
Accurate
Data
Secure
Reliable



Importance of IT Controls

Theft – Fraud – Loss of Data – Unauthorized Access

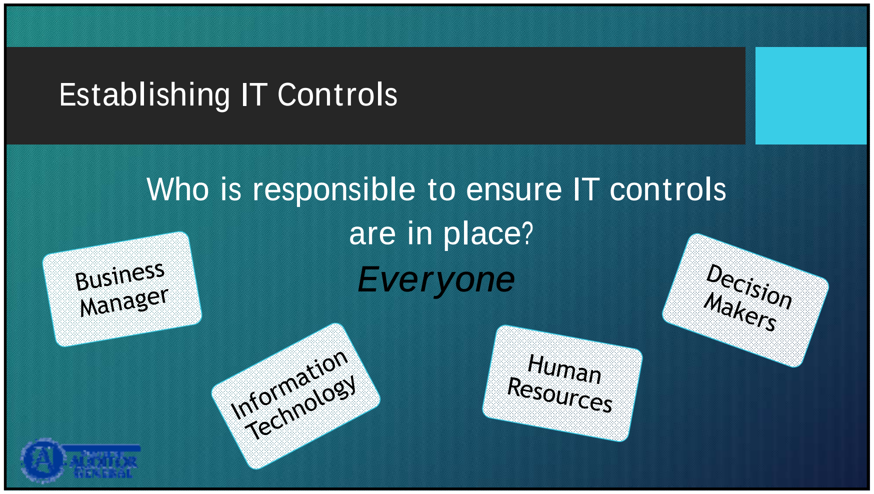
- More data at risk than ever before
  - Financial
    - Payroll – employee data
    - Bank accounts
    - Credit card system data
  - Student
    - Grades
    - Health
    - Private (Address, Phone, SSN)
- Increasing number of data breaches
  - MCCCD – $17 million
  - Target – $1+ billion
  - Unknown victims



IT Policies and Procedures - Systems

What systems should have policies?

- Financial systems
- Student information systems
- Food service systems
- Inventory and capital asset systems
- Home grown “systems” – (including forms and spreadsheets)



Establishing IT Controls

Who is responsible to ensure IT controls are in place?

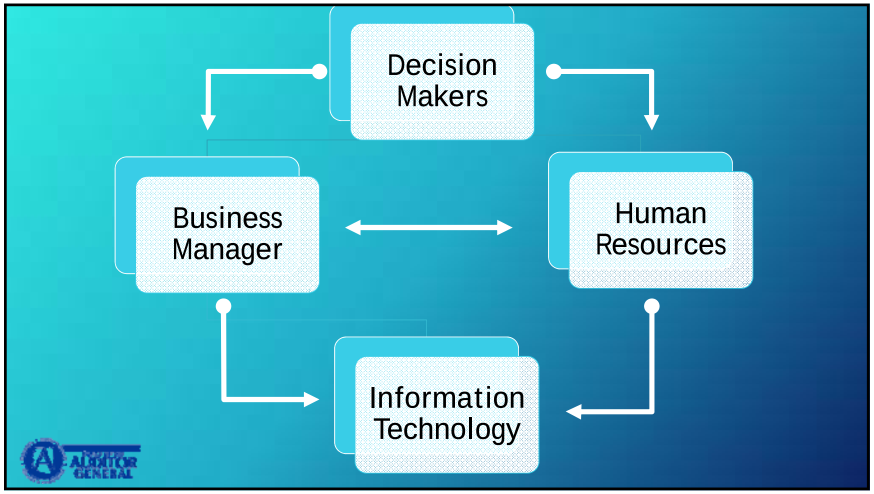
Everyone

Business Manager

Information Technology

Human Resources

Decision Makers

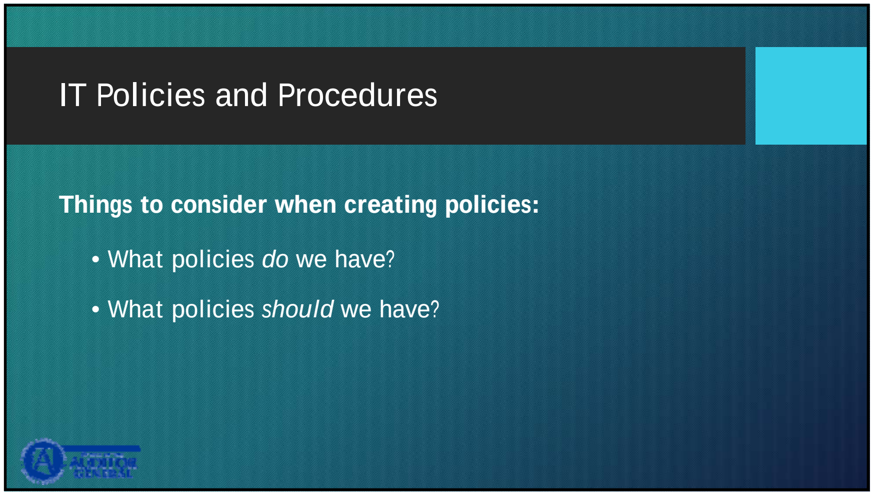


Decision Makers

Business Manager

Human Resources

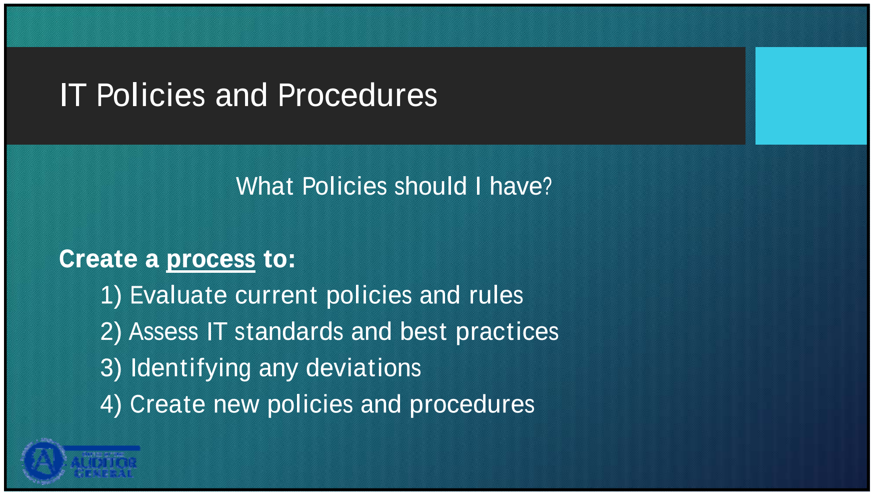
Information Technology



IT Policies and Procedures

Things to consider when creating policies:

- What policies *do* we have?
- What policies *should* we have?



IT Policies and Procedures

What Policies should I have?

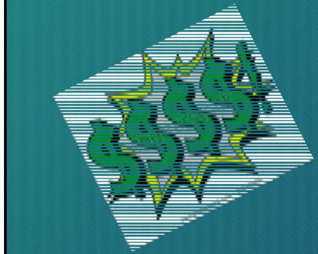
Create a <u>process</u> to:

1) Evaluate current policies and rules
2) Assess IT standards and best practices
3) Identifying any deviations
4) Create new policies and procedures

IT Policies and Procedures

How to:
- communicate
- disseminate
- enforce

Best Practices Discussed in this Webinar



How do I know which controls to consider?

Look to IT standards and best practices!

- What is a best practice?
  - Procedures that are accepted or prescribed as being correct or most effective
  - A set of guidelines, ethics, or ideas that represent the most efficient or prudent course of action
- Why should we use best practices?
  - There is no universal “compliance checklist” for IT, and no one way to implement IT controls
  - From knowledgeable IT experts

Assess IT Standards and Best Practices

Common Best Practice Frameworks
- COBIT
- NIST
- ISO
- FISCAM
- ITIL
- ASET State Policies
- COSO

Which one should I choose?

- Many overlap and have similar information, but some have more detail on certain topics
- Different focus
- Cost ranges ($0- ?)

- *Each district should consider the framework that best fits their needs, or use a mixture of all frameworks as necessary*

IT Standards and Best Practice Frameworks

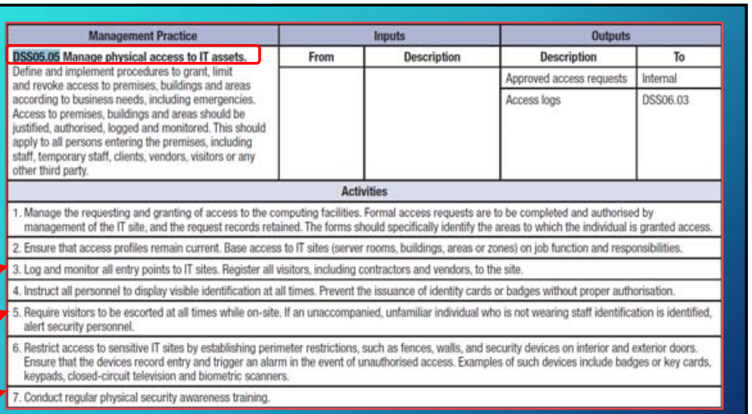
COBIT

- Created by ISACA (Information Systems Audit and Control Association)
- IT management and governance
- $135-$165 for main publication
- http://www.isaca.org/cobit/pages/default.aspx

IT Standards and Best Practice Frameworks

Information Technology Infrastructure Library (ITIL)

- Set of practices for IT service management
- Published in 5 volumes
- Fairly lengthy
- Created as an implementation guide
- $500+
- http://www.axelos.com/officialsite.asp?FO=1253138&ProductID=9780113313235&Action=Book



Management Practice	Inputs		Outputs	
DSS05.05 Manage physical access to IT assets. Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	**From**	**Description**	**Description**	**To**
			Approved access requests	Internal
			Access logs	DSS06.03
Activities				
1. Manage the requesting and granting of access to the computing facilities. Formal access requests are to be completed and authorised by management of the IT site, and the request records retained. The forms should specifically identify the areas to which the individual is granted access.				
2. Ensure that access profiles remain current. Base access to IT sites (server rooms, buildings, areas or zones) on job function and responsibilities.				
3. Log and monitor all entry points to IT sites. Register all visitors, including contractors and vendors, to the site.				
4. Instruct all personnel to display visible identification at all times. Prevent the issuance of identity cards or badges without proper authorisation.				
5. Require visitors to be escorted at all times while on-site. If an unaccompanied, unfamiliar individual who is not wearing staff identification is identified, alert security personnel.				
6. Restrict access to sensitive IT sites by establishing perimeter restrictions, such as fences, walls, and security devices on interior and exterior doors. Ensure that the devices record entry and trigger an alarm in the event of unauthorised access. Examples of such devices include badges or key cards, keypads, closed-circuit television and biometric scanners.				
7. Conduct regular physical security awareness training.				

IT Standards and Best Practice Frameworks

National Institute of Standards and Technology (NIST) -

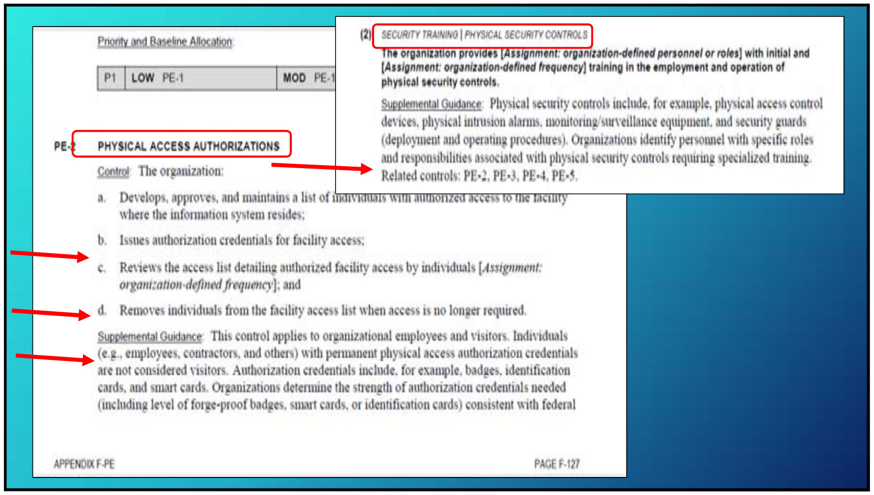
- 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- More focused on security
- Required for Federal Government
- Free - $0
- http://csrc.nist.gov/publications/PubsSPs.html

IT Standards and Best Practice Frameworks

Government Accounting Office (GAO)-

- Developed Federal Information Systems Controls Audit Manual (FISCAM)
- Federal Standard
- Audit Manual
- Free ($0)
- http://www.gao.gov/special.pubs/fiscam.html

FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM)



Priority and Baseline Allocation:

P1	LOW PE-1	MOD PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides;

b. Issues authorization credentials for facility access;

c. Reviews the access list detailing authorized facility access by individuals [*Assignment: organization-defined frequency*]; and

d. Removes individuals from the facility access list when access is no longer required.

Supplemental Guidance: This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Authorization credentials include, for example, badges, identification cards, and smart cards. Organizations determine the strength of authorization credentials needed (including level of forge-proof badges, smart cards, or identification cards) consistent with federal

APPENDIX F-PE PAGE F-127

(2) *SECURITY TRAINING | PHYSICAL SECURITY CONTROLS*

The organization provides [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures). Organizations identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training. Related controls: PE-2, PE-3, PE-4, PE-5.

IT Standards and Best Practice Frameworks

International Organization for Standards (ISO) and International Electro Technical Commission (IEC)

- ISO 27002 – Information Technology – Security techniques – Code of practice for information security management
- For those responsible for initiating, implementing and maintaining IS management systems
- International Standard
- Security focused
- $200+

http://www.iso.org/iso/catalogue_detail?csnumber=54533

IT Standards and Best Practice Frameworks

ASET - Arizona Strategic Enterprise Technology

- Arizona Statewide Policies
- Many policies
- Areas such as: management practices, security, web services, enterprise architecture and privacy
- http://aset.azdoa.gov/
- Based off of other frameworks such as NIST
- Free ($0)

ASET Arizona Strategic Enterprise Technology

General IT Controls

Other General IT Controls for your IT Environment

- Protecting Sensitive Data
- Training Staff
- Performing Risk Assessments

Protecting Sensitive Data

Identification, documentation, and classification:

- What data do you have?

How would you classify:

- Employee evaluations?
- Payroll and student data?
- SSN's?
- Prior year financial data?
- Emergency contact list, allergy list?
- Teachers websites or assignments?

Protecting Sensitive Data

Consistent process

- Have data and systems been inventoried and documented by process?

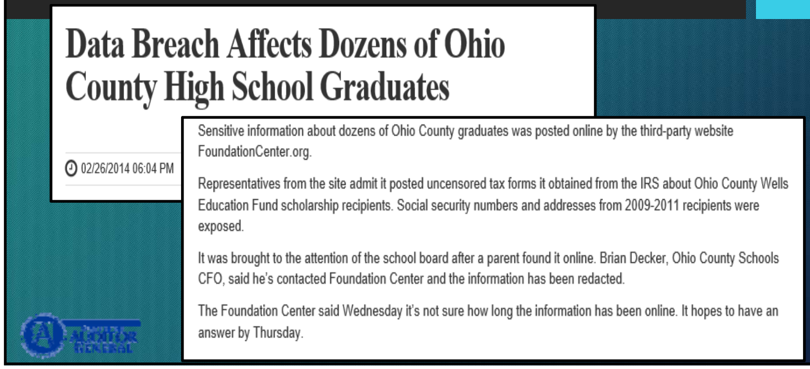
Compliance

- Compliance with laws and regulations (FERPA, HIPAA, CIPA, etc.)

Policies and procedures

- Security and user agreements
  - What data should not be accessed from home?

Why identify and classify data?



Data Breach Affects Dozens of Ohio County High School Graduates

02/26/2014 06:04 PM

Sensitive information about dozens of Ohio County graduates was posted online by the third-party website FoundationCenter.org.

Representatives from the site admit it posted uncensored tax forms it obtained from the IRS about Ohio County Wells Education Fund scholarship recipients. Social security numbers and addresses from 2009-2011 recipients were exposed.

It was brought to the attention of the school board after a parent found it online. Brian Decker, Ohio County Schools CFO, said he's contacted Foundation Center and the information has been redacted.

The Foundation Center said Wednesday it's not sure how long the information has been online. It hopes to have an answer by Thursday.

Training

- Communicate controls and policies to staff
- Provide training to staff on IT controls and polices
  - Security awareness training on security controls such as securing passwords
- Identify ongoing training needs

Evaluating your environment through assessments

Evaluate your environment and controls against IT best practices
- Gap analysis of current polices to best practices
- Risk assessment

Self reporting vs. audit

Frequency of assessment

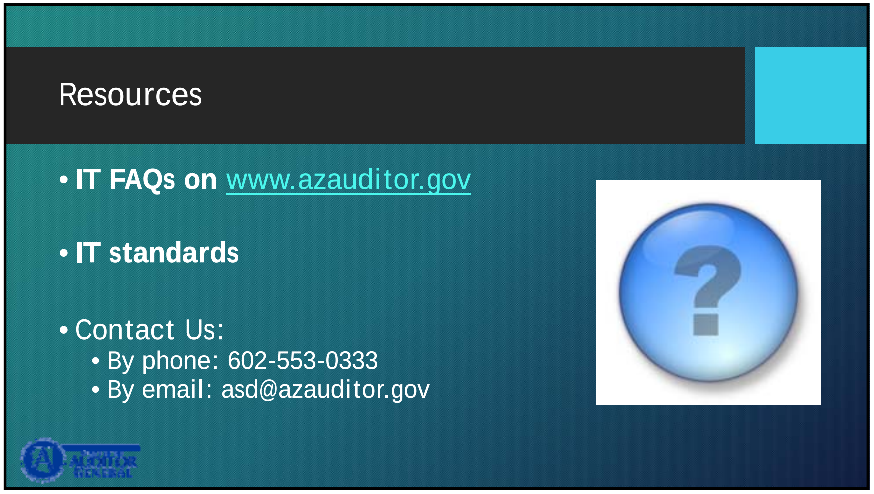
Remediate risks/ gaps in process vs. best practice
- Cost / benefit and risk tolerance for certain controls

Next Webinars

Identifying users and limiting access
- Systems and network accounts
- Physical Access to server rooms

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

Disaster Recovery Plans
- Development
- Testing



Resources

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