# Network and Security Controls

State Of Arizona
Office Of The Auditor General
Phil Hanus

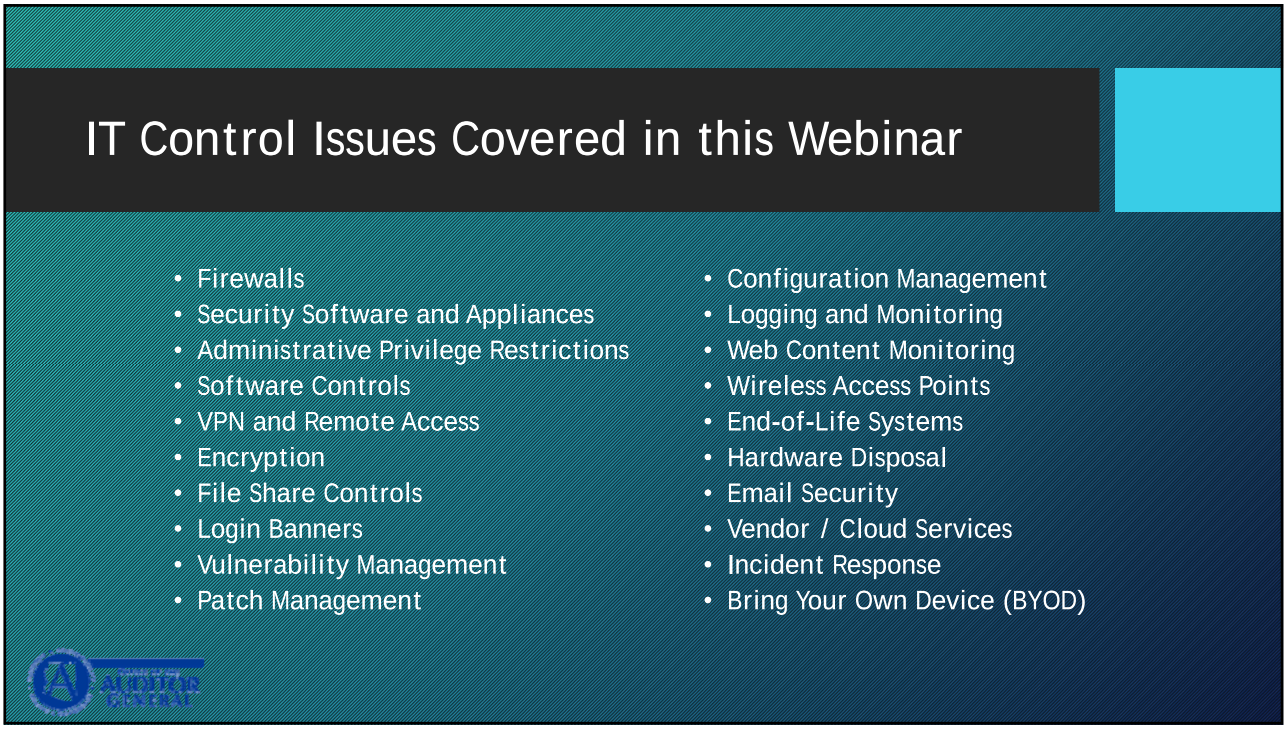
## IT Controls Webinar Series

Part I – Overview of IT Controls and Best Practices

Part II – Identifying Users and Limiting Access

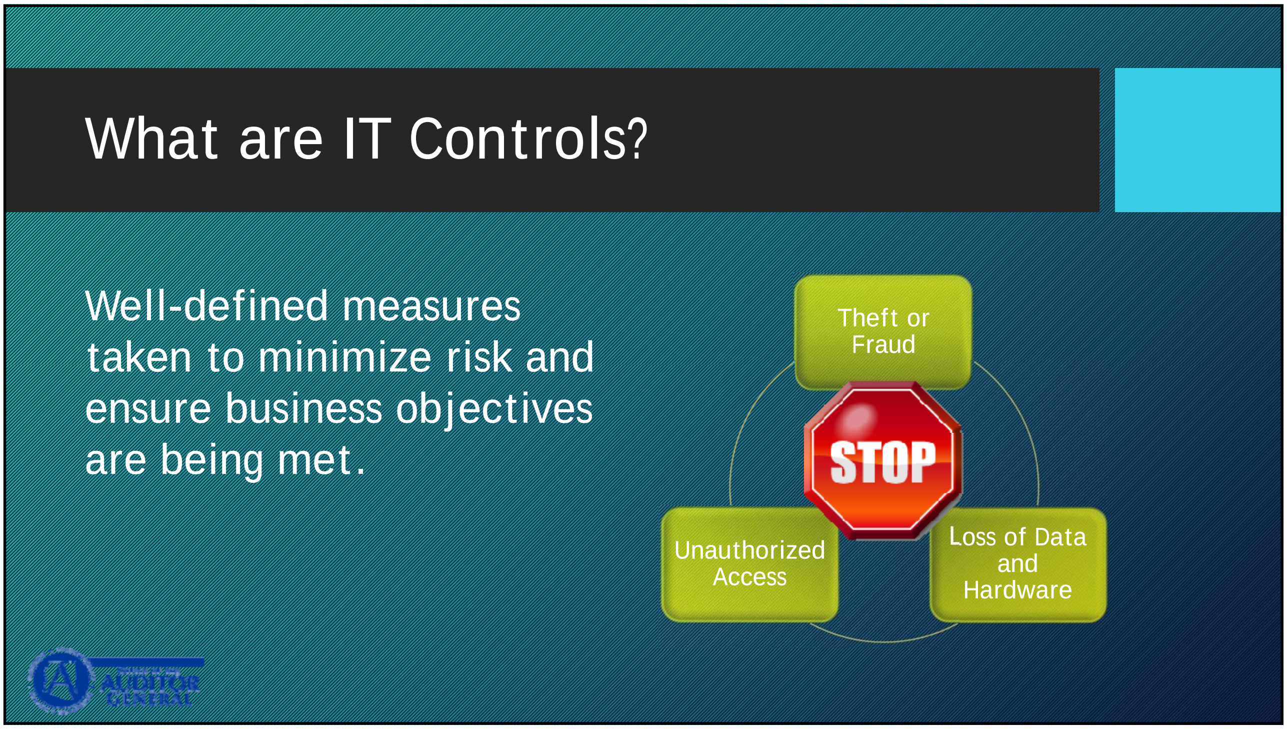
**Part III – Network Controls**

Part IV – Disaster Recovery Planning



## IT Control Issues Covered in this Webinar

- Firewalls
- Security Software and Appliances
- Administrative Privilege Restrictions
- Software Controls
- VPN and Remote Access
- Encryption
- File Share Controls
- Login Banners
- Vulnerability Management
- Patch Management
- Configuration Management
- Logging and Monitoring
- Web Content Monitoring
- Wireless Access Points
- End-of-Life Systems
- Hardware Disposal
- Email Security
- Vendor / Cloud Services
- Incident Response
- Bring Your Own Device (BYOD)



## What are IT Controls?

Well-defined measures taken to minimize risk and ensure business objectives are being met.

Theft or Fraud

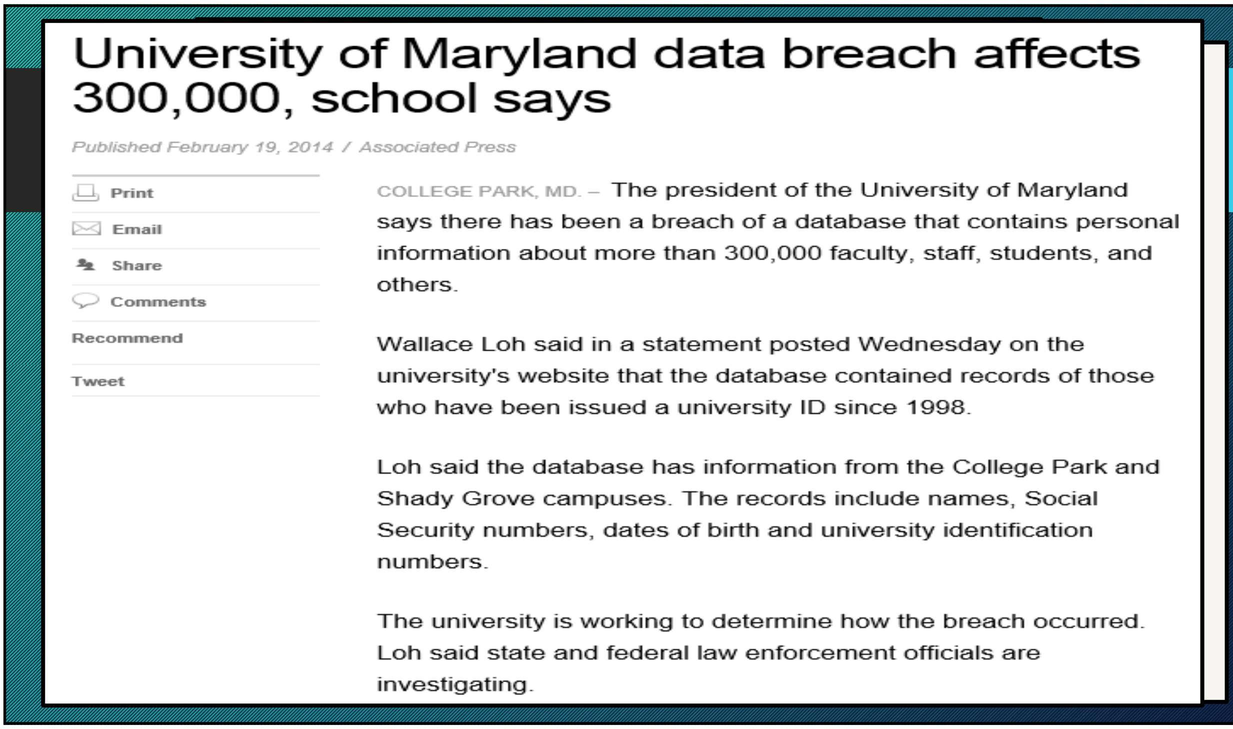
STOP

Unauthorized Access

Loss of Data and Hardware

## Resources (Appendices)

- IT Standards and Best Practices
- No One Size Fits All Solution
- Advanced Presentation on our Web site
- Appendix of resources by slide



# University of Maryland data breach affects 300,000, school says

*Published February 19, 2014 / Associated Press*

COLLEGE PARK, MD. – The president of the University of Maryland says there has been a breach of a database that contains personal information about more than 300,000 faculty, staff, students, and others.

Wallace Loh said in a statement posted Wednesday on the university's website that the database contained records of those who have been issued a university ID since 1998.

Loh said the database has information from the College Park and Shady Grove campuses. The records include names, Social Security numbers, dates of birth and university identification numbers.

The university is working to determine how the breach occurred. Loh said state and federal law enforcement officials are investigating.

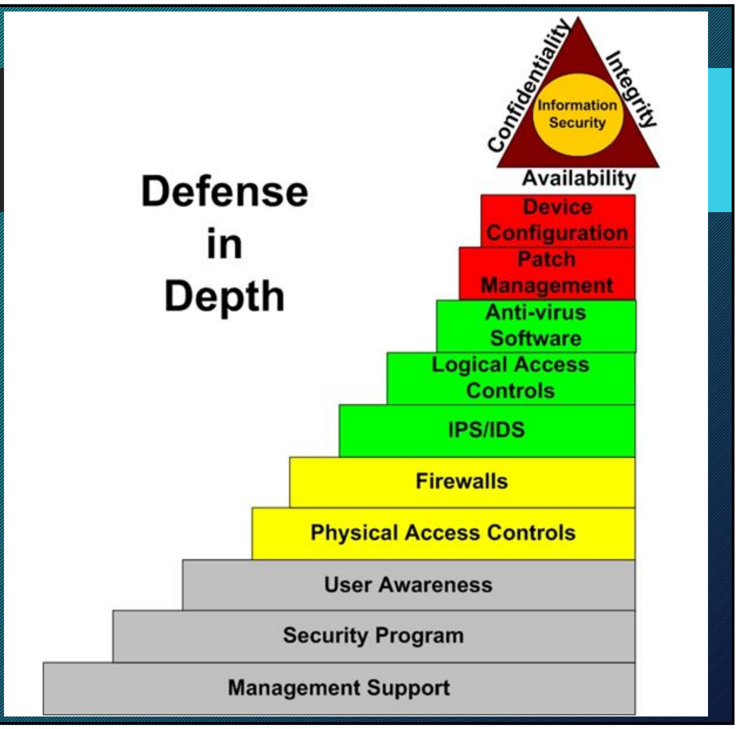
GM64

## US Department of Education privacy resources

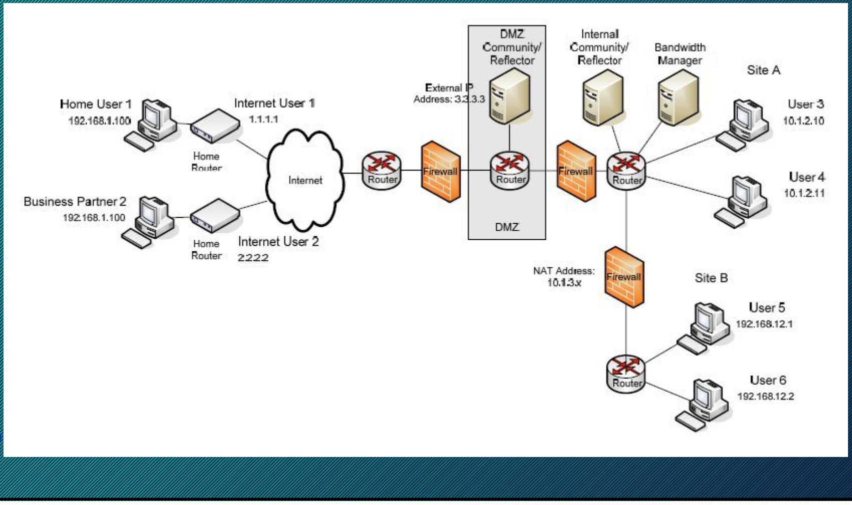
Privacy Technical Assistance Center
U.S. Department of Education

- PTAC Mission
  - Improve privacy, security, confidentiality of student data systems
  - Provide tools, resources, opportunities
  - States to share best practices
  - Focus points for queries and responses to privacy needs
  - Resources to promote compliance with FERPA and other best practices

## Layered Security



## Firewalls



## Security Software and Appliances

- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)
- Antivirus / Anti-malware
- Email Spam Filters

# Administrative Privilege Restrictions

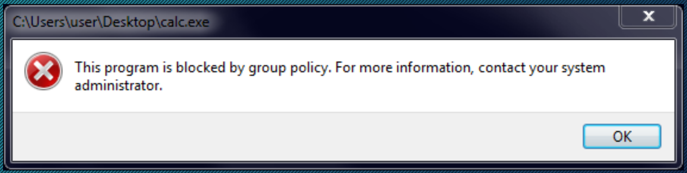
**Restrict Admin Privileges for System Administrators**

- Separate accounts
  - Standard User Account -- Everyday Duties
  - Administrative Account -- Only used for specific administrative tasks
- Tied to specific user
  - Ex: phanus (Standard) and phanus-admin (Admin)
- Monitor activity

# Software Controls

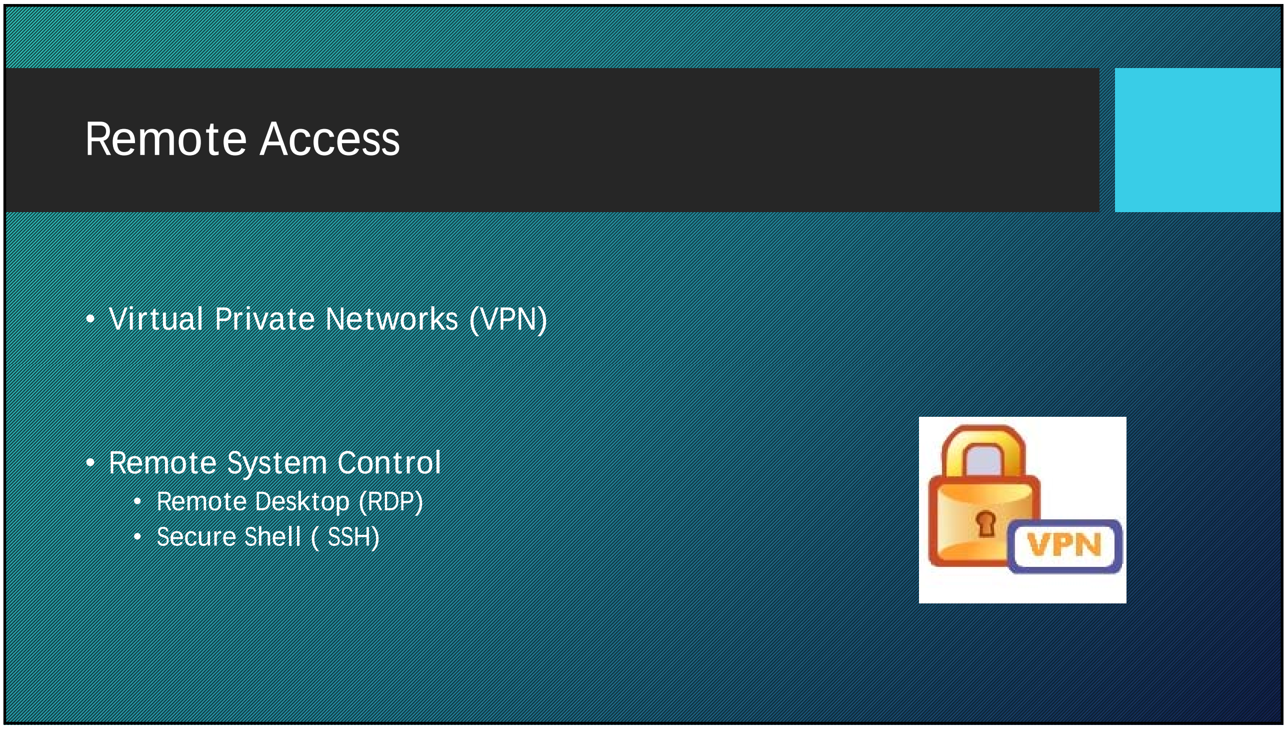
**Managing Software**

- Monitoring
- Application whitelisting



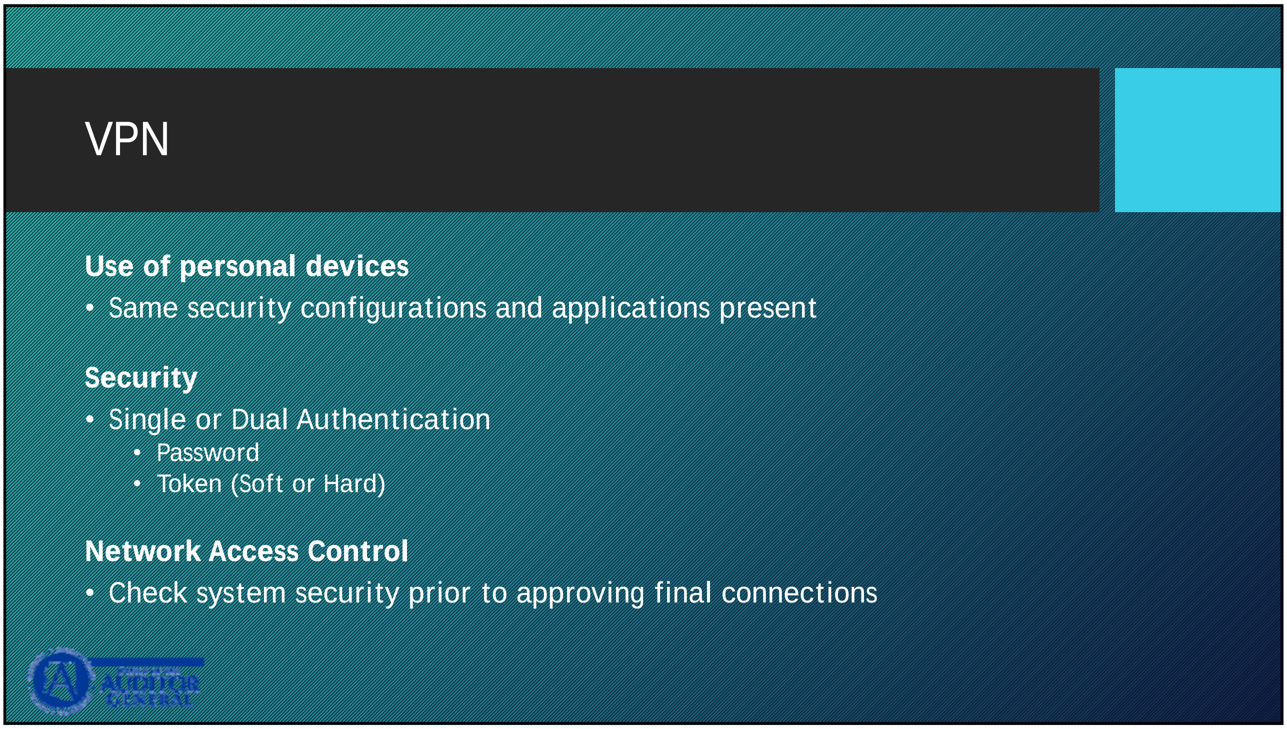
C:\Users\user\Desktop\calc.exe

This program is blocked by group policy. For more information, contact your system administrator.



## Remote Access

- Virtual Private Networks (VPN)
- Remote System Control
  - Remote Desktop (RDP)
  - Secure Shell ( SSH)



## VPN

**Use of personal devices**

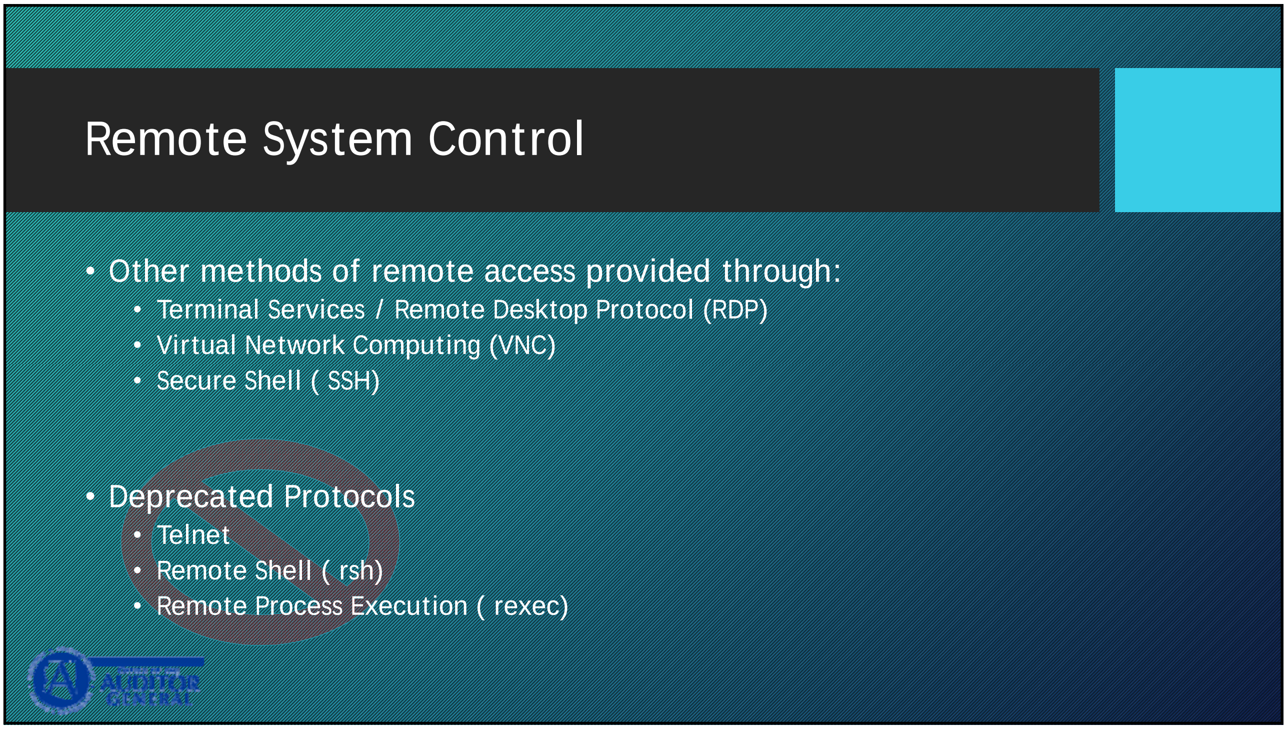
- Same security configurations and applications present

**Security**

- Single or Dual Authentication
  - Password
  - Token (Soft or Hard)

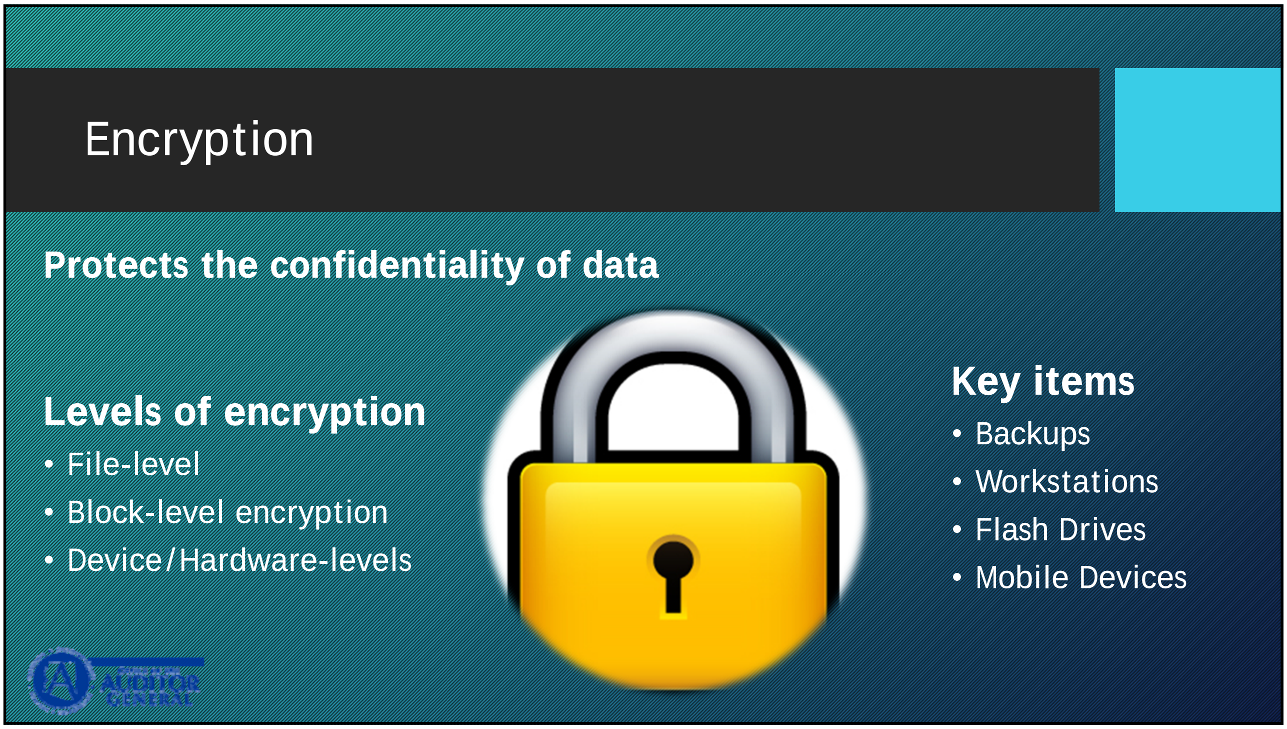
**Network Access Control**

- Check system security prior to approving final connections



## Remote System Control

- Other methods of remote access provided through:
  - Terminal Services / Remote Desktop Protocol (RDP)
  - Virtual Network Computing (VNC)
  - Secure Shell ( SSH)
- Deprecated Protocols
  - Telnet
  - Remote Shell ( rsh)
  - Remote Process Execution ( rexec)



## Encryption

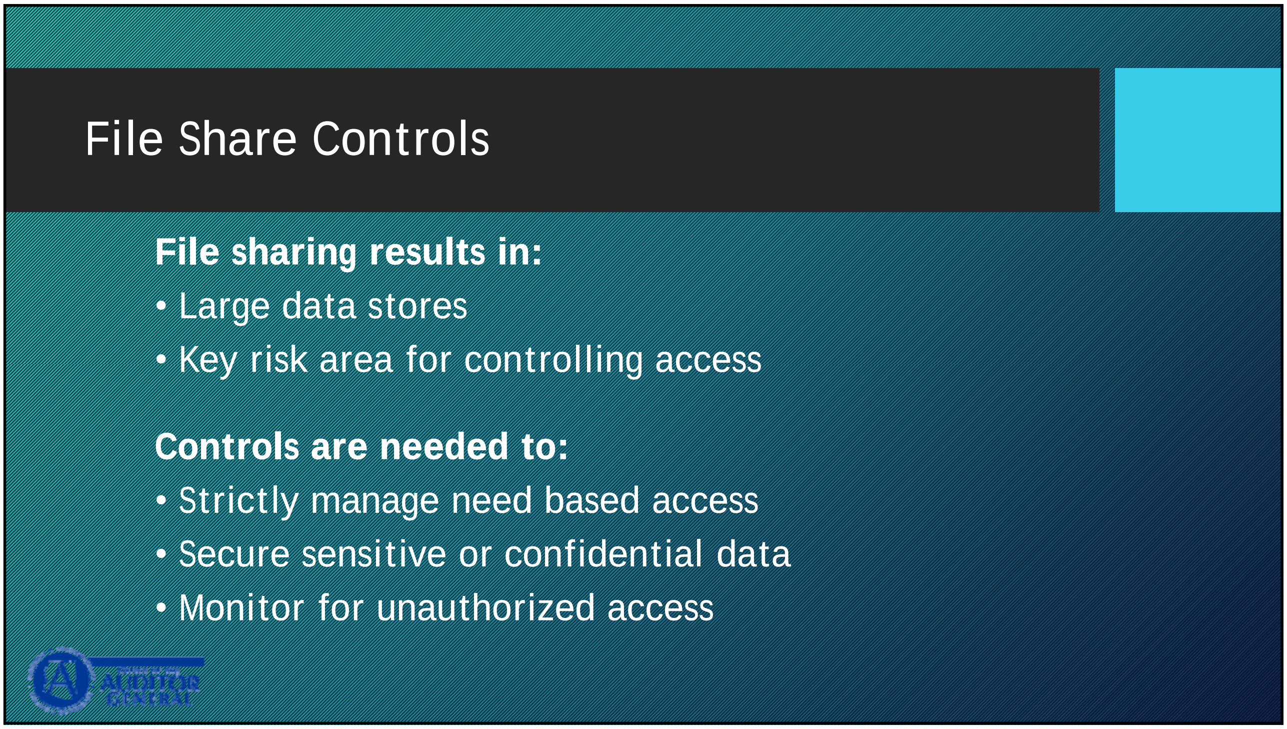
**Protects the confidentiality of data**

**Levels of encryption**

- File-level
- Block-level encryption
- Device/Hardware-levels

**Key items**

- Backups
- Workstations
- Flash Drives
- Mobile Devices



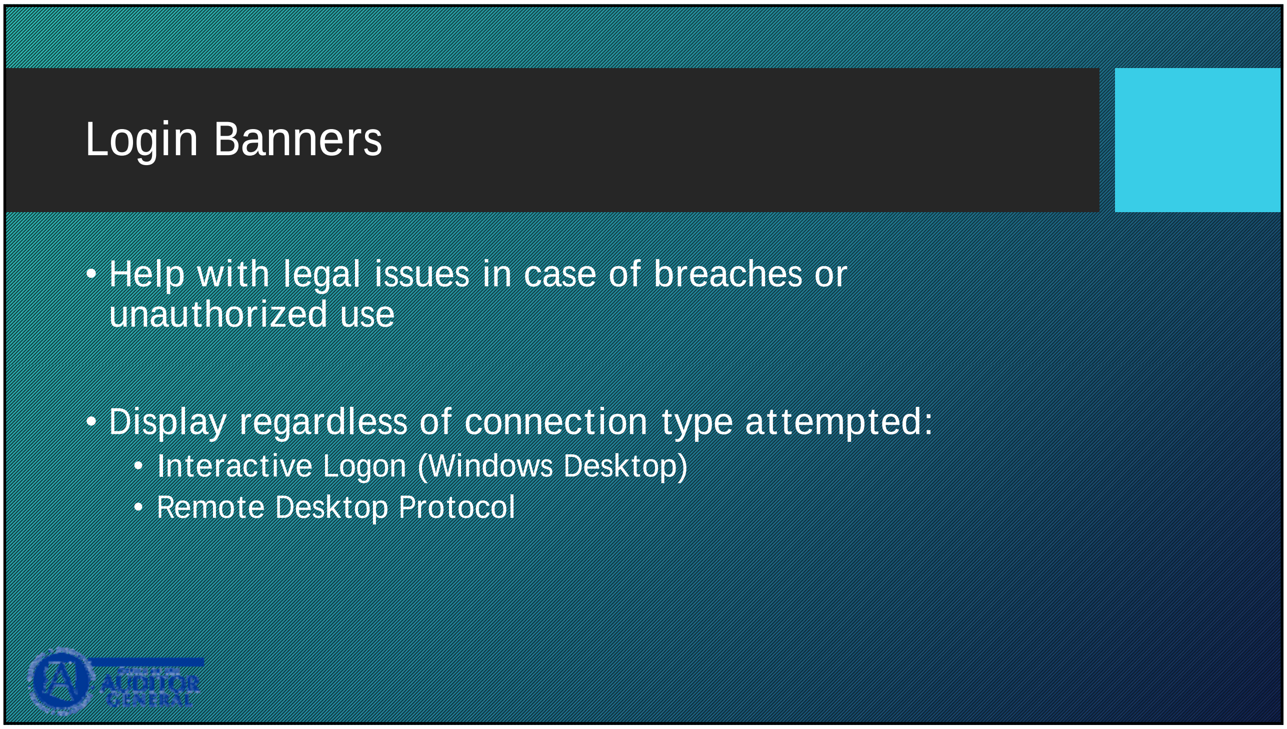
## File Share Controls

**File sharing results in:**

- Large data stores
- Key risk area for controlling access

**Controls are needed to:**

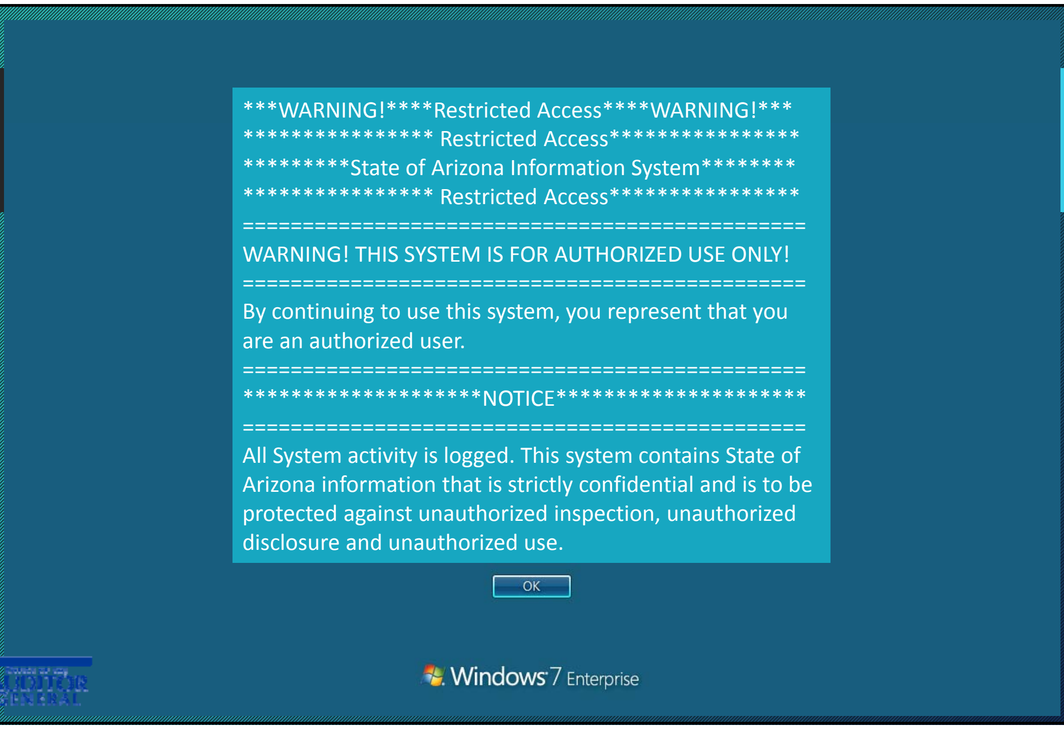
- Strictly manage need based access
- Secure sensitive or confidential data
- Monitor for unauthorized access



## Login Banners

- Help with legal issues in case of breaches or unauthorized use

- Display regardless of connection type attempted:
  - Interactive Logon (Windows Desktop)
  - Remote Desktop Protocol

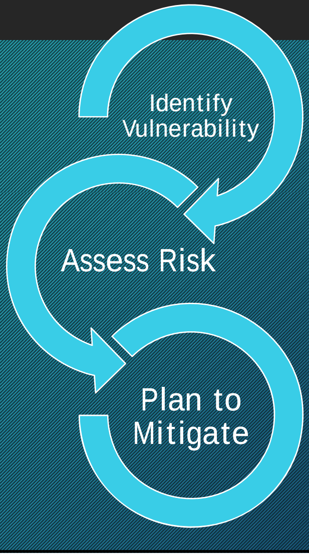


```
***WARNING!****Restricted Access****WARNING!***
**************** Restricted Access****************
*********State of Arizona Information System********
**************** Restricted Access****************
==============================================
WARNING! THIS SYSTEM IS FOR AUTHORIZED USE ONLY!
==============================================
By continuing to use this system, you represent that you
are an authorized user.
==============================================
********************NOTICE*********************
==============================================
All System activity is logged. This system contains State of
Arizona information that is strictly confidential and is to be
protected against unauthorized inspection, unauthorized
disclosure and unauthorized use.
```

## Vulnerability Management

**Assess the security risks in:**

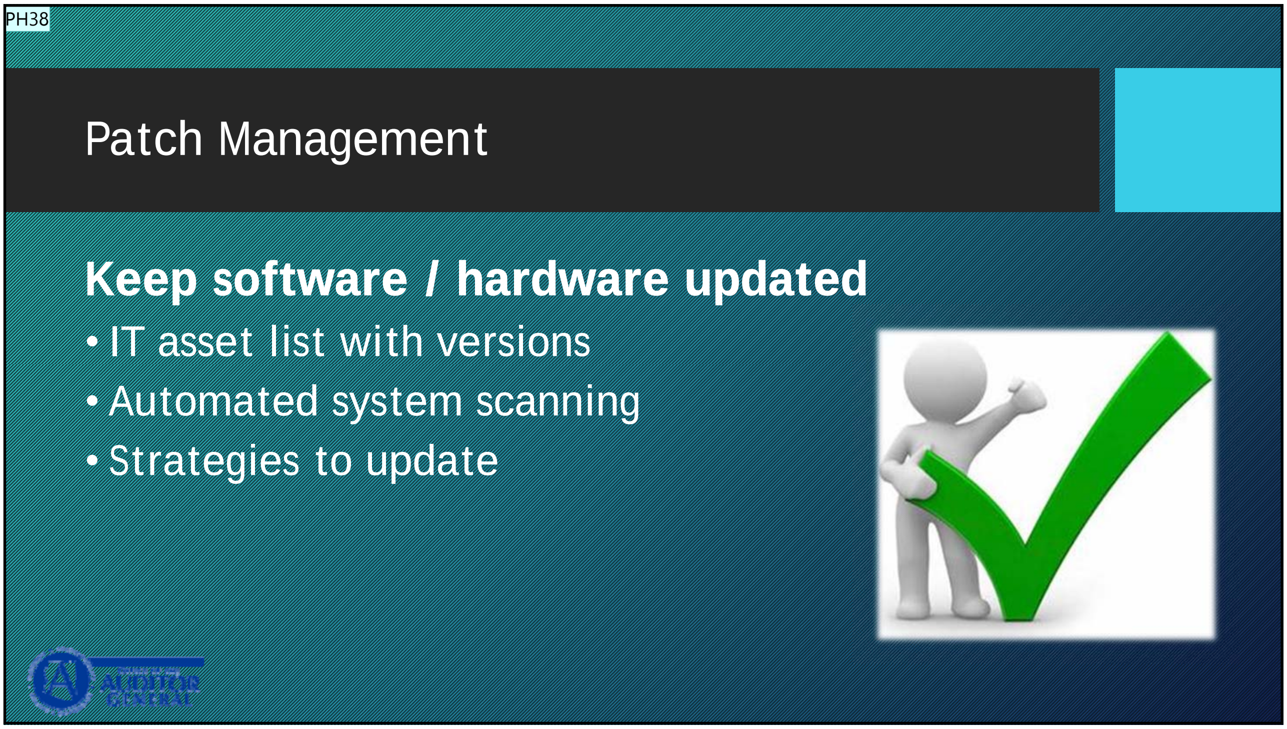
- Software
- Hardware
- Internally-hosted websites



**Determine & document:**

- Known vulnerabilities
- Possible risks
- Action plan to mitigate

Repeat the process!

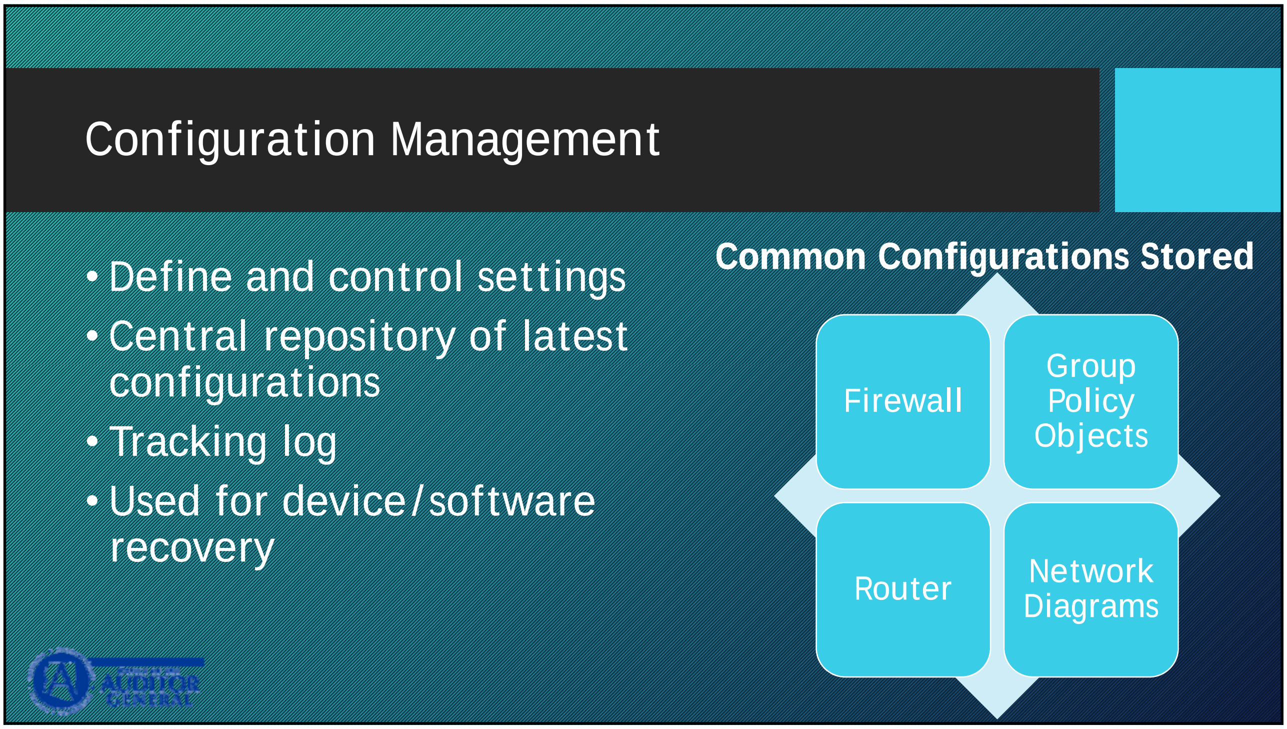


PH38

# Patch Management

**Keep software / hardware updated**

- IT asset list with versions
- Automated system scanning
- Strategies to update



# Configuration Management

- Define and control settings
- Central repository of latest configurations
- Tracking log
- Used for device/software recovery

**Common Configurations Stored**

Firewall

Group Policy Objects

Router

Network Diagrams

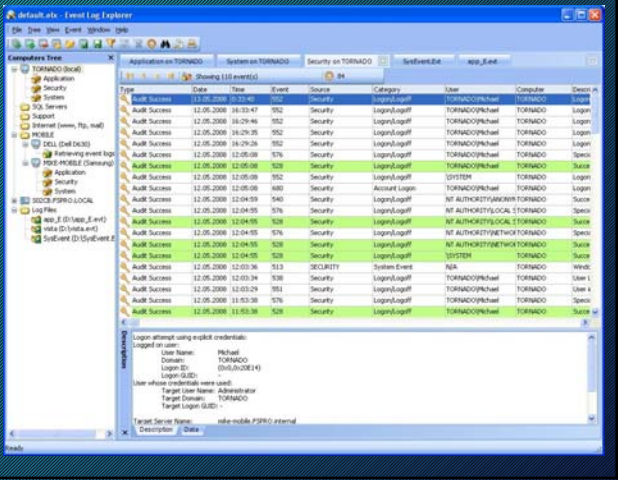
# Logging and Monitoring

**Logging activity**

- Critical and sensitive systems
- Rules based
- Automatically created/stored

**Monitoring logs**

- Regular log monitoring (Proactive)
- Reviewed when things go wrong (Reactive)



| Type | Date | Time | Event | Source | Category | User | Computer | Descri |
|---|---|---|---|---|---|---|---|---|
| Audit Success | 13.05.2008 | 0:33:40 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:33:47 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:46 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:35 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 16:29:26 | 552 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:05:08 | 576 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Speci |
| Audit Success | 12.05.2008 | 12:05:08 | 528 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:05:08 | 552 | Security | Logon/Logoff | \SYSTEM | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:05:08 | 680 | Security | Account Logon | TORNADO\Michael | TORNADO | Logon |
| Audit Success | 12.05.2008 | 12:04:59 | 540 | Security | Logon/Logoff | NT AUTHORITY\ANONYM | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 576 | Security | Logon/Logoff | NT AUTHORITY\LOCAL S | TORNADO | Speci |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | NT AUTHORITY\LOCAL S | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 576 | Security | Logon/Logoff | NT AUTHORITY\NETWOI | TORNADO | Speci |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | NT AUTHORITY\NETWOI | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:04:55 | 528 | Security | Logon/Logoff | \SYSTEM | TORNADO | Succe |
| Audit Success | 12.05.2008 | 12:03:36 | 513 | SECURITY | System Event | N/A | TORNADO | Windc |
| Audit Success | 12.05.2008 | 12:03:34 | 538 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | User L |
| Audit Success | 12.05.2008 | 12:03:29 | 551 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | User i |
| Audit Success | 12.05.2008 | 11:53:38 | 576 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Speci |
| Audit Success | 12.05.2008 | 11:53:38 | 528 | Security | Logon/Logoff | TORNADO\Michael | TORNADO | Succe |

```
Logon attempt using explicit credentials:
Logged on user:
        User Name:          Michael
        Domain:             TORNADO
        Logon ID:           (0x0,0x20E14)
        Logon GUID:         -
User whose credentials were used:
        Target User Name:   Administrator
        Target Domain:      TORNADO
        Target Logon GUID:  -

Target Server Name:         mike-mobile.PSPRO.internal
```

# Web Content Monitoring

## ARS §34-502

Technology protection measures to prevent access to visual depictions that are:

- Obscene content
- Child Pornography
- Content Harmful to Minors

## Other Entities

Monitor Internet Activity for:

- Illegal activities
- Gambling
- Adult Material
- Malicious Content

## Wireless Access Points

- Convenient but can increase security issues
- Properly secured and segmented

| WEP | WPA | WPA2 PSK | WPA2 Enterprise |
|---|---|---|---|
| Weak | | | Strong |

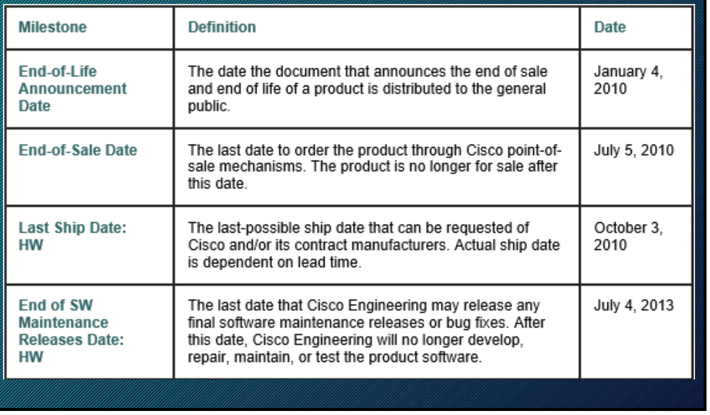
- Guests/non-work functions should not connect directly to the internal network

## End-Of-Life Systems

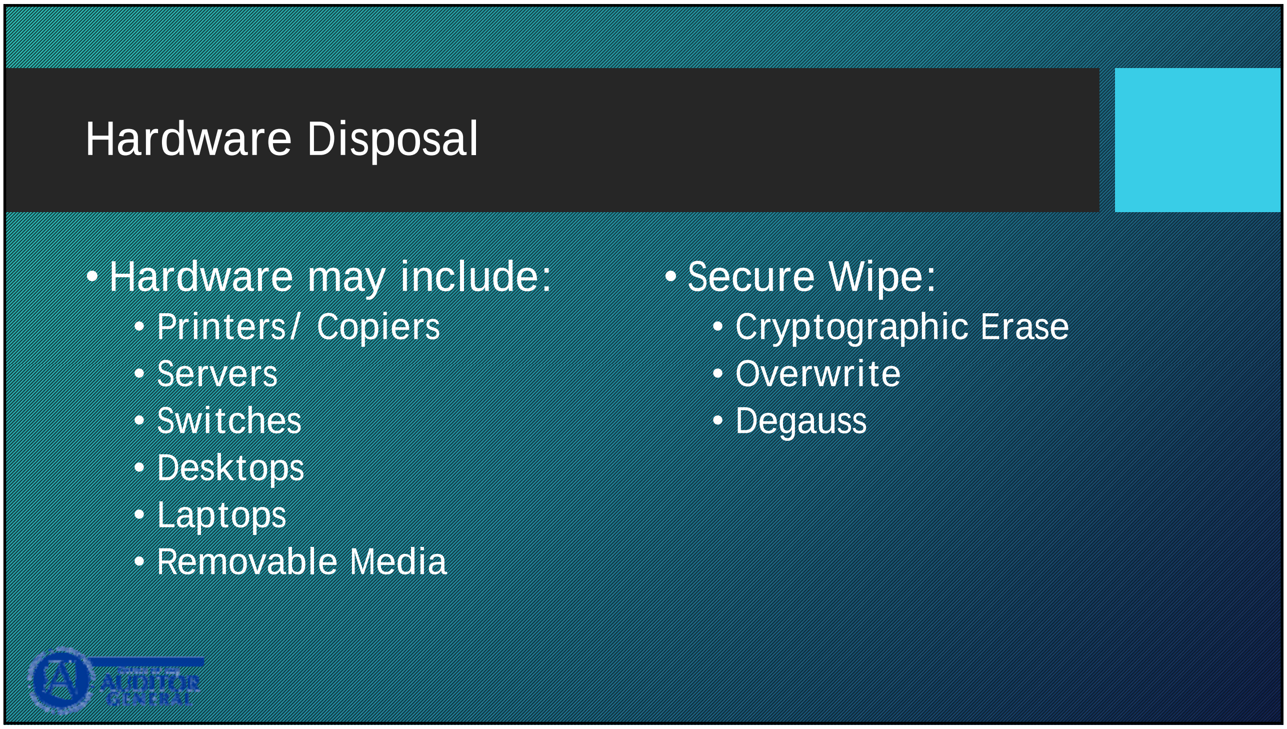
**Unsupported products** = risk of failure & compromise

Plan ahead- Know:

- When its coming
- How to replace hardware/software
- What tests new products need
- Operations won't be adversely affected



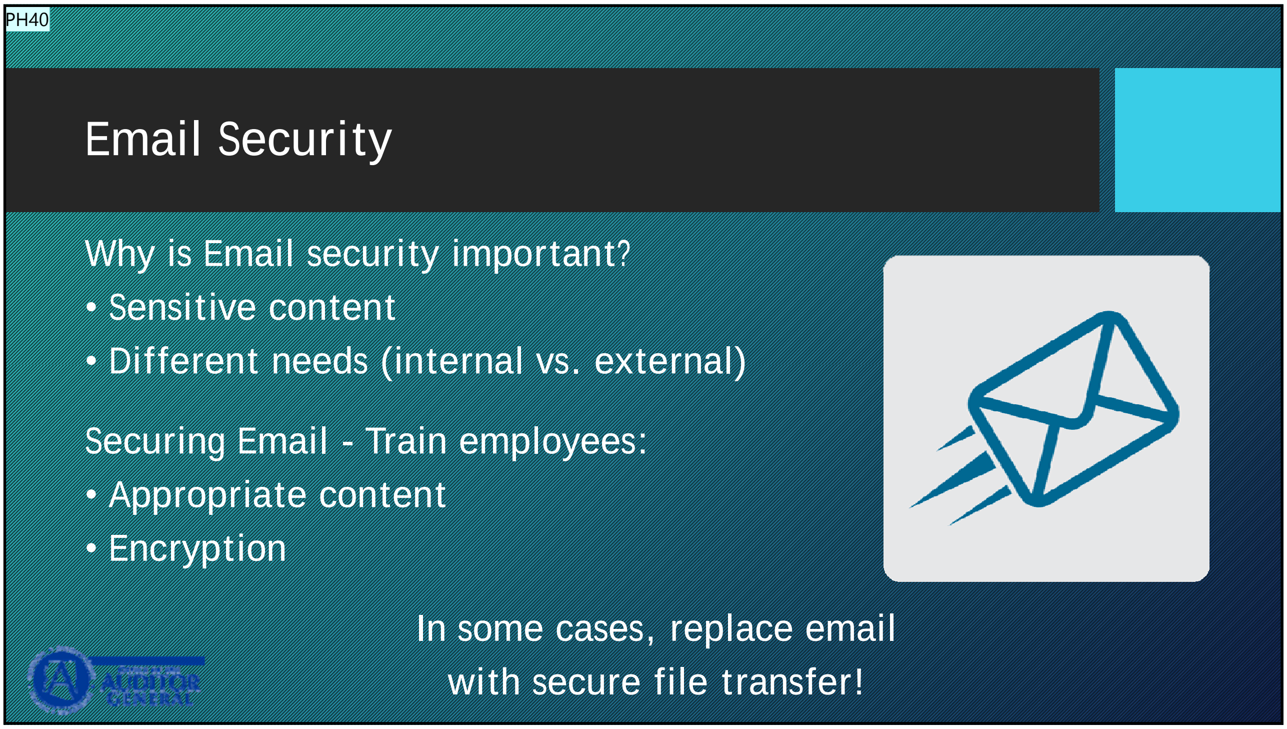
| Milestone | Definition | Date |
|---|---|---|
| End-of-Life Announcement Date | The date the document that announces the end of sale and end of life of a product is distributed to the general public. | January 4, 2010 |
| End-of-Sale Date | The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date. | July 5, 2010 |
| Last Ship Date: HW | The last-possible ship date that can be requested of Cisco and/or its contract manufacturers. Actual ship date is dependent on lead time. | October 3, 2010 |
| End of SW Maintenance Releases Date: HW | The last date that Cisco Engineering may release any final software maintenance releases or bug fixes. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software. | July 4, 2013 |



## Hardware Disposal

- Hardware may include:
  - Printers/ Copiers
  - Servers
  - Switches
  - Desktops
  - Laptops
  - Removable Media
- Secure Wipe:
  - Cryptographic Erase
  - Overwrite
  - Degauss

PH40



## Email Security

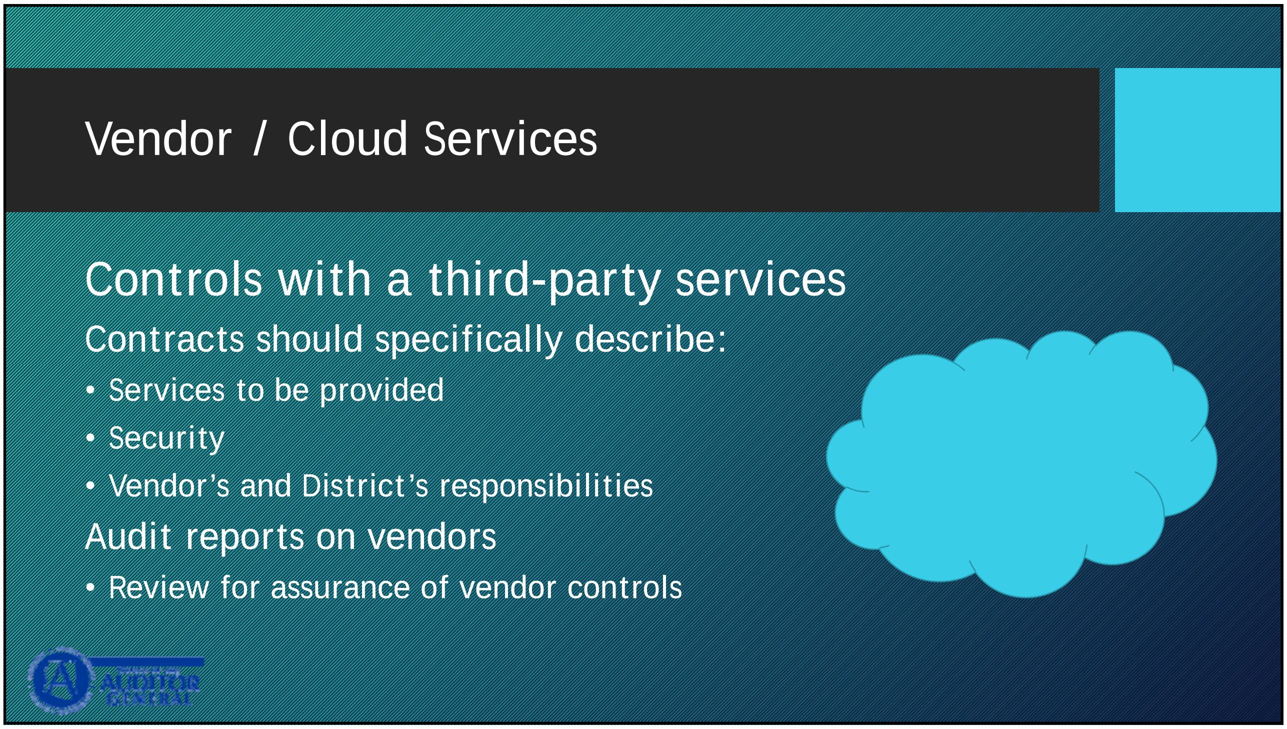
Why is Email security important?

- Sensitive content
- Different needs (internal vs. external)

Securing Email - Train employees:

- Appropriate content
- Encryption

In some cases, replace email with secure file transfer!



## Vendor / Cloud Services

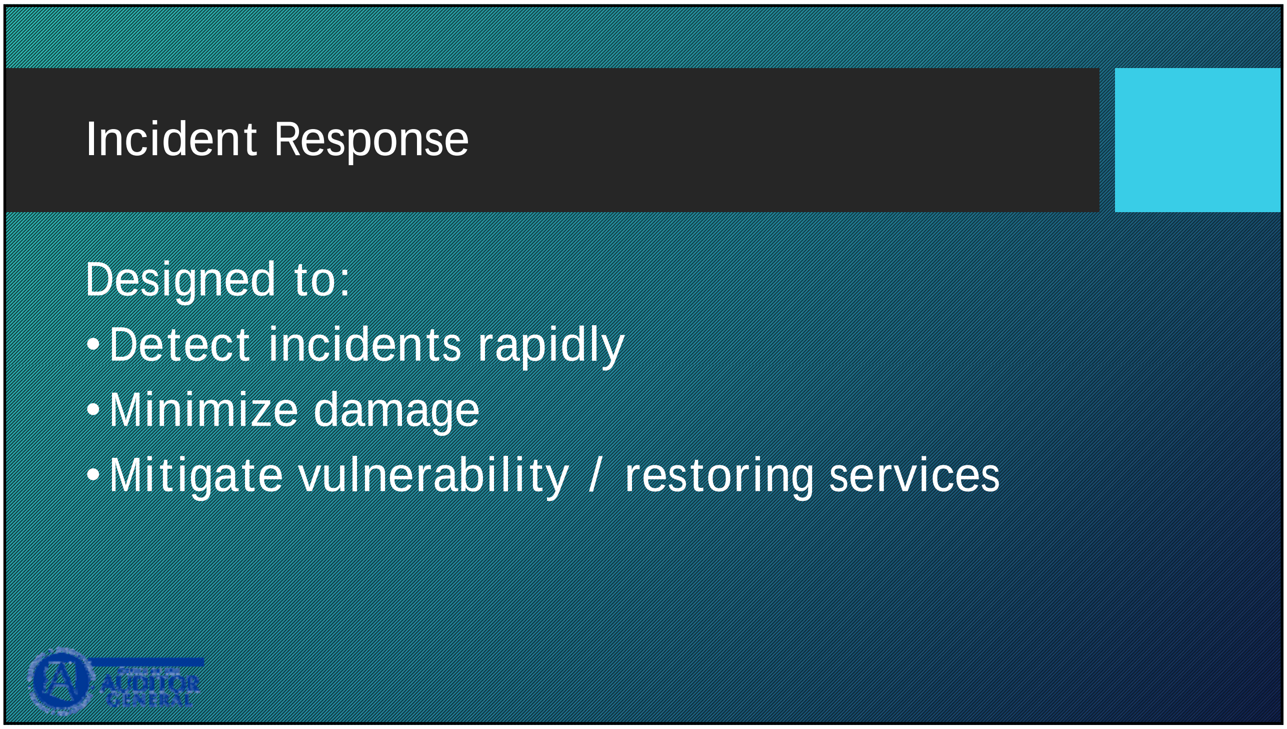
Controls with a third-party services

Contracts should specifically describe:

- Services to be provided
- Security
- Vendor's and District's responsibilities

Audit reports on vendors

- Review for assurance of vendor controls



## Incident Response

Designed to:

- Detect incidents rapidly
- Minimize damage
- Mitigate vulnerability / restoring services

CC37 EA57 CC39 EA60

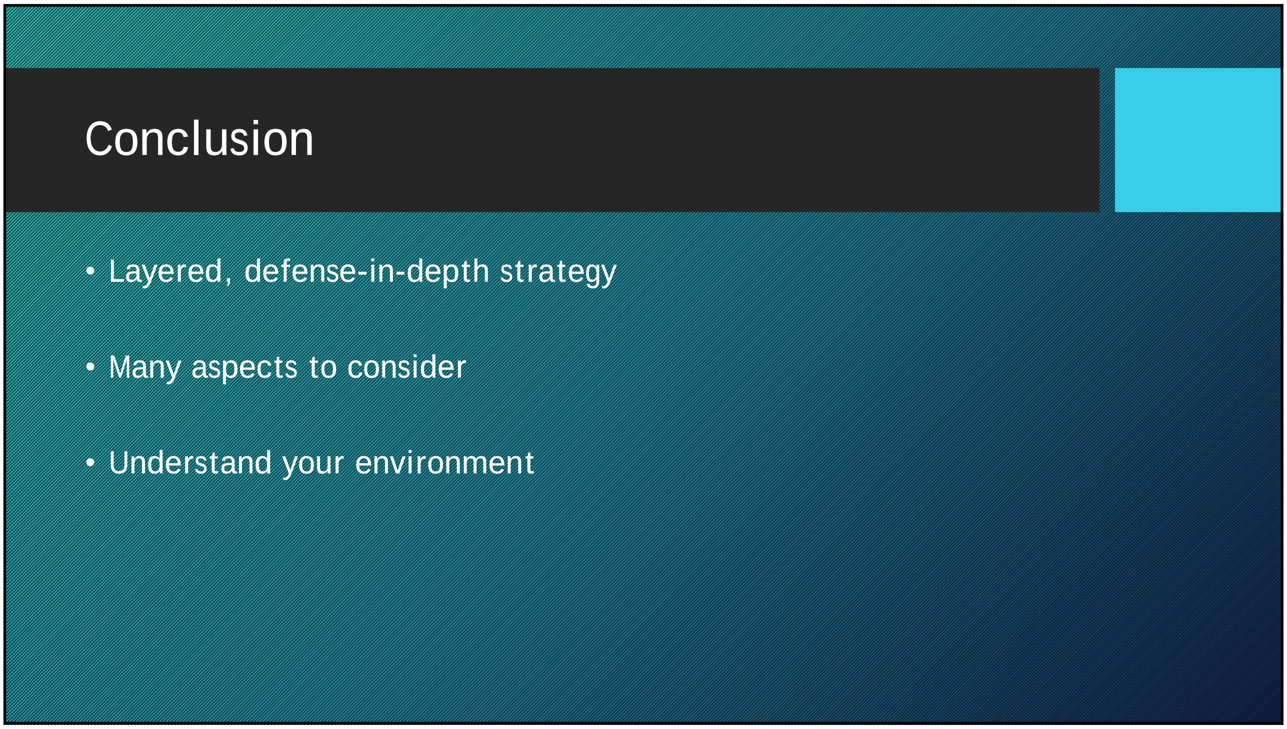
## Bring Your Own Device (BYOD)

- Separating Business vs. Personal data
- Limiting access
- Securing/removing data
- Requiring device controls
  - Anti-Virus
  - Encryption
  - screen locks
  - separate boot
  - VPN software

CC40 GM66

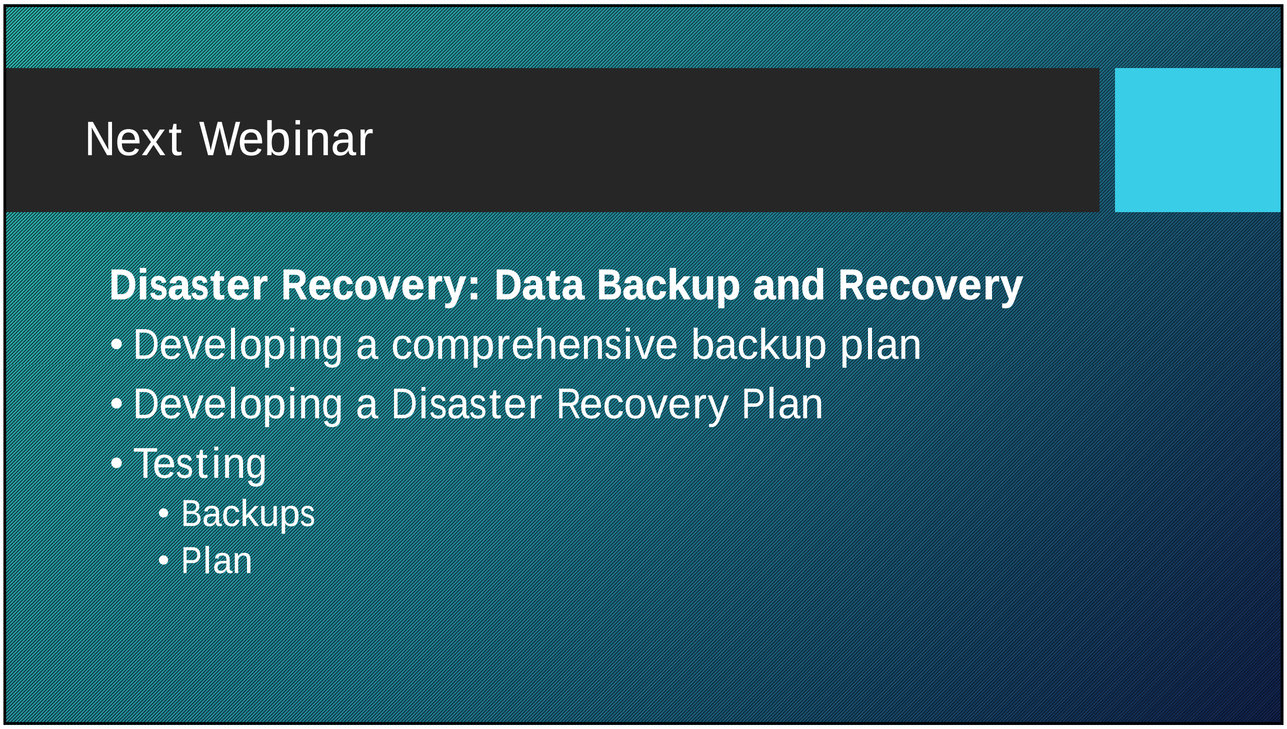
## Advanced Class Topics

- Network Segregation
- Secure Baseline Configurations
- Server Hardening
- Active Directory Security Considerations
- Website Security
- Data Loss Prevention



## Conclusion

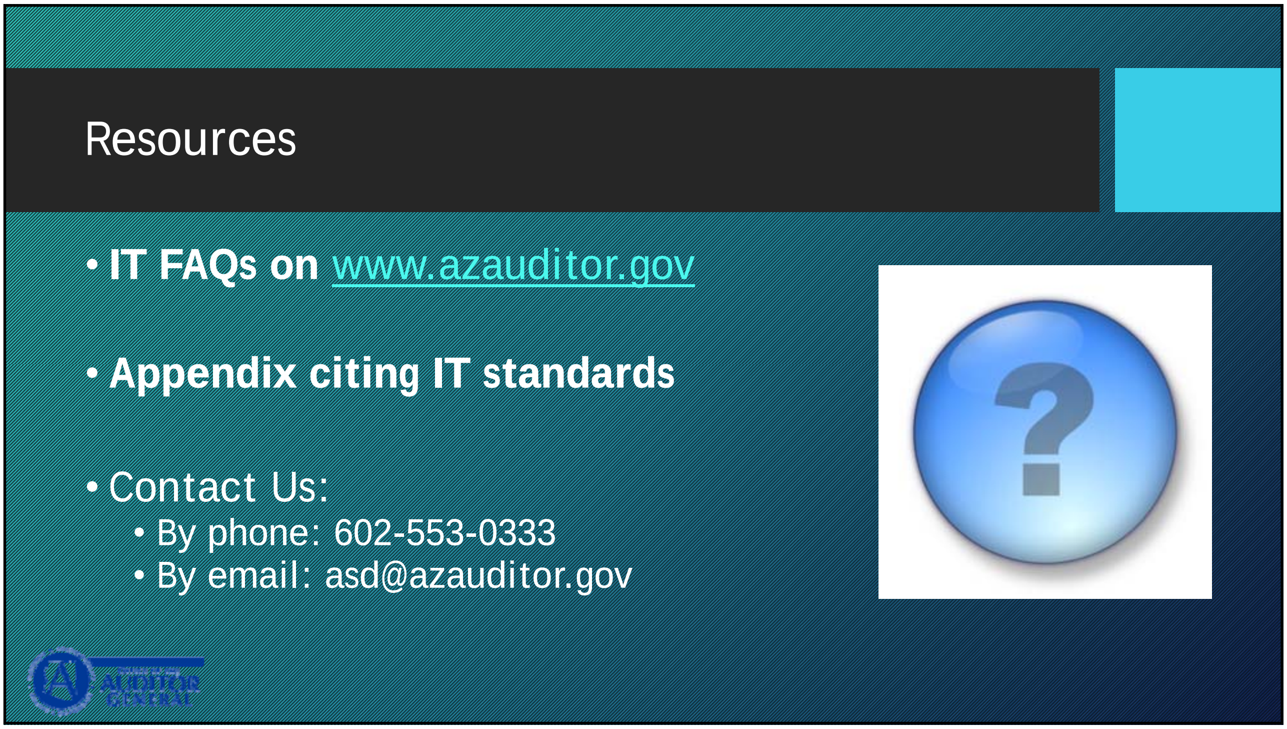
- Layered, defense-in-depth strategy
- Many aspects to consider
- Understand your environment



## Next Webinar

**Disaster Recovery: Data Backup and Recovery**

- Developing a comprehensive backup plan
- Developing a Disaster Recovery Plan
- Testing
  - Backups
  - Plan



## Resources

- **IT FAQs on** www.azauditor.gov

- **Appendix citing IT standards**

- Contact Us:
  - By phone: 602-553-0333
  - By email: asd@azauditor.gov