

ATS

Applied Technology Services, Inc.

Your Partner in Technology

www.appliedtechnologyservices.com



Surviving a MD State IT Audit

Presented by:

ATS and Presidio

March 2, 2010

Agenda

- Introductions
- Overview of a Maryland State Audit
- Sample Findings
- Audit Planning and Preparation
- Implementing a Security Strategy
- Three Methodologies for Assessment
- Q and A

Background Information

Applied Technology Services teams with Presidio to offer services under the **MEEC IT Security Assessments and Advisory Services** contract, #C200916.

Applied Technology Services

Applied Technology Services (“ATS”) is a local minority and women-owned technology services company serving commercial and government clients throughout the state of Maryland. ATS has a long history working with Maryland State and Local governments to develop solutions and provide services across the enterprise.

Core competencies include:

- Hardware and Software Solution Development and Deployment Services
- Enterprise Maintenance Services through *ATS CareSM*
- Network Security Solutions
- Network Support Services
- Technical Staffing (network engineers, security engineers, web developers, programmers, technicians, help desk support and analysts)

3

Presidio

Security solutions from Presidio Networked Solutions provide protection for critical information assets and ensuring uninterrupted operational integrity.

Systems & network security solutions include:

- Vulnerability assessments
- Risk Assessments
- Web site health checks
- Penetration testing
- Systems security auditing
- Policy and procedure development
- Secure network design and implementation
- Product selection and evaluation
- Incident response
- Managed security services
- Security intelligence services

Types of Audits

The MD State Office of Legislative Audits conducts fiscal and compliance audits of each unit of State Government at least once every three years. The agency performs audits in accordance with State Government Article, Section 2-1221 of the Annotated Code of Maryland.

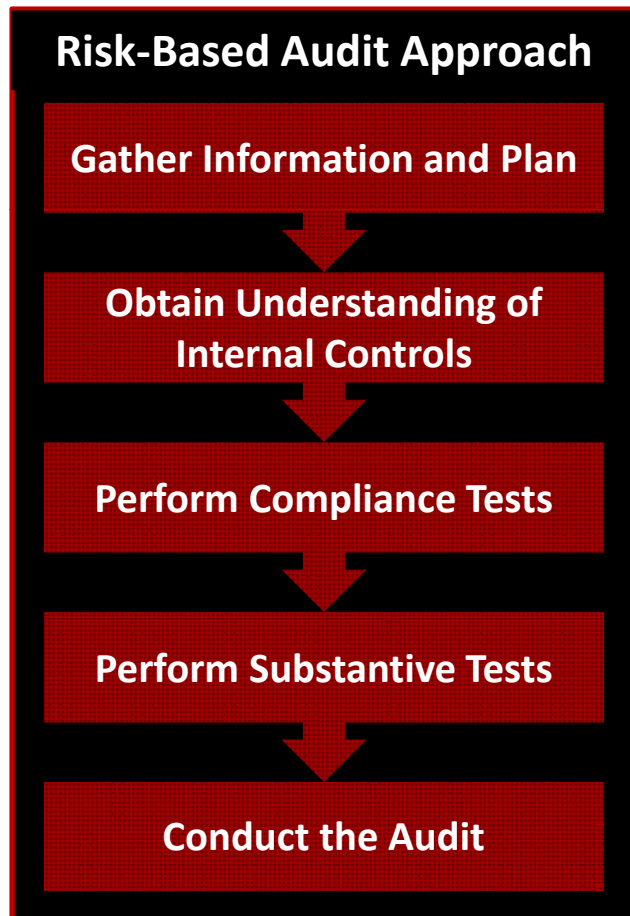
Audit Types

- Fiscal/compliance
- Performance
- Financial management and/or reporting



Note: State Community Colleges must adopt MHEC guidelines in accordance with the Education Article, Section 16-315(a) which requires an independent entity audit financial statements and internal controls. These entities may also have internal auditing procedures required at the local government level.

The Audit Process



Typically includes:

- The agencies internal control over its data center(s) and network
- Compliance with applicable State laws, rules and regulations for the computer systems supporting the agency
- An assessment of security controls for routers, firewalls, switches, VPN appliances , wireless network connectivity, critical application access and the use of software vulnerability assessments for critical network servers
- Inquiries of personnel, inspection of documents and records, observation of operations, transaction testing and other audit procedures

Benchmarks and Procedures

- Research from SANS (SysAdmin, Audit, Network, Security) , a cooperative research and education organization
 - The Top 20 Most Critical Internet Security Vulnerabilities
- USM *Guidelines in Response to the State IT Security Policy*
- The Standish Group International, Inc., Chaos 10 (Best Practices)
- Department of General Services' *Inventory Control Manual*
- MSDE Benchmarks
 - IT technical support operations staffing

SANS Top 20 Most Exploited Vulnerabilities

- | | |
|-------------------------------------|---|
| 1. Internet Explorer | 12. Unencrypted Laptops and Removable Media |
| 2. Windows Libraries | 13. DNS Servers |
| 3. Microsoft Office | 14. Backup Software |
| 4. Windows Services | 15. Security, Enterprise, and Directory Management Servers |
| 5. Windows Configuration Weaknesses | 16. VoIP Servers and Phones |
| 6. MAC OS X | 17. Network and Other Devices Common Configuration Weaknesses |
| 7. UNIX Configuration | 18. Excessive Rights and Unauthorized Devices |
| 8. Web Applications | 19. Users (Phishing/Spear Phishing) |
| 9. Database Software | 20. Zero Day Attacks and Prevention Strategies |
| 10. P2P File | |
| 11. Instant Messaging | |



USM Guidelines

- Network Security Standard (Section V)
 - Controls for dial-in access and remote access services
 - Configuration and monitoring of firewalls and network devices
 - Intrusion detection and prevention systems, including automated and manual processes for host-based, network-based or a combination of both and IDS/IPS alert monitoring and escalation
 - Access controls for wireless networks
 - PBX security
 - Disaster recovery plans

Typical Network Vulnerabilities Assessed

Network

- Availability of sensitive network information available on the Internet
- Protection of the internal network
 - Traffic from untrusted third parties, including Internet, students, computer labs and the wireless network
 - Account controls over administrative access to core network devices
 - Rules on firewalls/routers
- Monitoring of critical network devices
 - User and system activity logging and alerts on firewalls
 - Review of security and event logs for core routers and management/ authentication servers
- Protection from wireless network access through the use of encryption

Data

- Restriction and logging/alerts of access to critical system, program and data files
- Comprehensive controls and logging on on production program modifications
- Logging and reporting procedures for security related events
- Control over user accounts and related parameters
- Comprehensive business continuity and disaster recovery plan and procedures, including critical system backup files
- Physical access to critical computing resources

Sample 1 Findings: State University

- **Excessive access** - Students and public have Internet access to internal servers used for the student admissions process and grades
- **Access controls not reviewed** - Employees (3 terminated) have unnecessary administrative read access to core network devices.
- **Controls not tested** – Firewall/routers rules are outdated allowing unauthorized access to network devices.
- **User activity not logged** - The firewall protecting the mainframe was not configured to log all user and system activity or to alert administrators to critical firewall operating conditions and the log was not routinely reviewed
- **Event logs not reviewed** -Event logs for core routers and critical management and authentication servers were not regularly reviewed.
- **Modifications not logged** - Modifications to critical system and production data files were not logged at file-level detail (only libraries were identified)



Sample 2 Findings: State University

- **Control #1 not tested** - Publicly accessible servers were located on the internal network rather than in a separate network zone to minimize security
- **Control #2 not tested** - Firewall rules allowed unnecessary access over numerous ports to many devices in the internal network. Firewall logs stored on firewall, no external logging server.
- **Excessive access** - Employees have unnecessary administrative access, at the network level, to the Internet firewall and a critical core network device
- **Poor controls** - Payroll reports which contained the names, social security numbers, and payroll information for many employees were also stored on a publicly accessible web server.
- **No backups** - Did not periodically back up a critical server and the Internet firewall's configuration
- **No logging** - Logging of critical security-related events was not enabled for an essential application, server, and two critical databases.



Sample 3 Findings: Community College

- **Control #1 not tested** - A logging server was accessible at a network level from the untrusted student computer labs within the internal network subjecting the firewall's logs to potential compromise.
- **Event logs not reviewed** - Event logs for firewalls, core routers and critical management/authentication servers were not regularly reviewed.
- **Excessive Access Permissions** - User workstations in the student network segment (including student computer labs) had network level access to most of the administrative network over all ports
- **Password Control Weak** - Credit card, account name and related password were stored in plain text within a computer program file on the student web application server.
- **Excessive Access Permissions** - Employees had system access capabilities that allowed them to modify recorded student grade information even though such capabilities were not necessary for these individuals to perform their job duties.



Sample 4 Findings: School System

- **Passwords vulnerable** – Passwords were set to never expire for many accounts, including high privilege users such as database and network administrators.
- **No logging** - Significant system security-related activities (such as account logons and failed access attempts) for one critical system were not always logged for review
- **Inadequate patching** - As of December 2007, one critical system had not been updated for security related software updates since March 2007, leaving this system vulnerable to security exploits addressed by these updates
- **Poor change management** - Production program changes to critical applications were not adequately documented
- **Physical access inadequate** - Physical access to the computer room was not adequately controlled
- **Poor development strategies** - During implementation of a new financial management system for financial operations and reporting, including general ledger, accounts payable and accounts receivable the entity did not use certain system development best practices to ensure successful project implementation



Audit Findings

- Poor patch management
- Anti-virus software out-of-date
- Controls not checked
- SNMP open on Network
- Default passwords
- Default community strings
- No monitoring
 - No baseline
- Hardware vulnerable
- No logging
- Poor change control
- Applications vulnerable to attack
- No security awareness training
 - Social engineering risk high



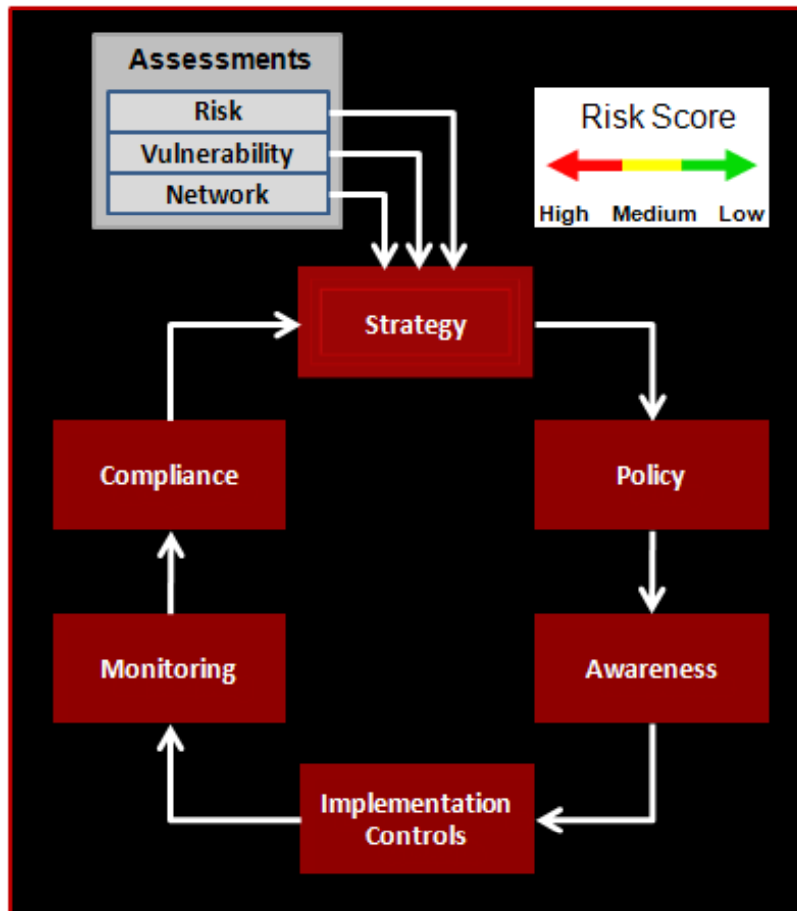
Audit Preparation



- Review your system security policies
- Review security requirement specifications for every user and resource
- Identify and evaluate threat (human factors, natural disasters and infrastructure failure)
- Identify and evaluate vulnerabilities
- Perform security certification (verification of confidentiality, integrity, availability and monitoring)
- Review specifications for ongoing security monitoring for each resource

“By failing to prepare you are preparing to fail.” – Benjamin Franklin

Security Strategy



Strategy – Implement security in all business functions. Presidio uses risk, vulnerability and network assessments to develop customer risk score.

Policy – Establish a framework for the organizational standards.

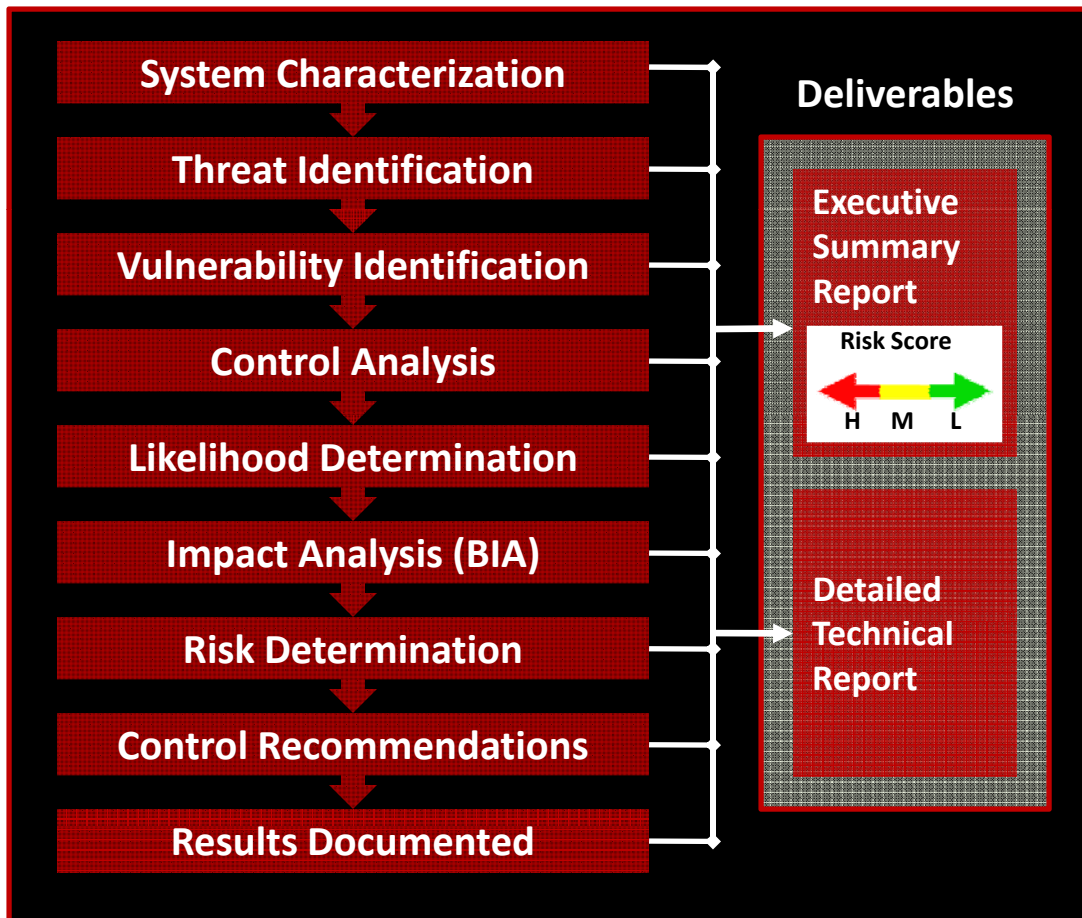
Awareness – Educate those affected by the security policies on their roles and responsibilities. Educate users on social engineering.

Implementation – Provide protection, detection and respond controls to protect information.

Monitoring – Monitor and detect policy violations and other security vulnerabilities.

Compliance – Track all security issues.

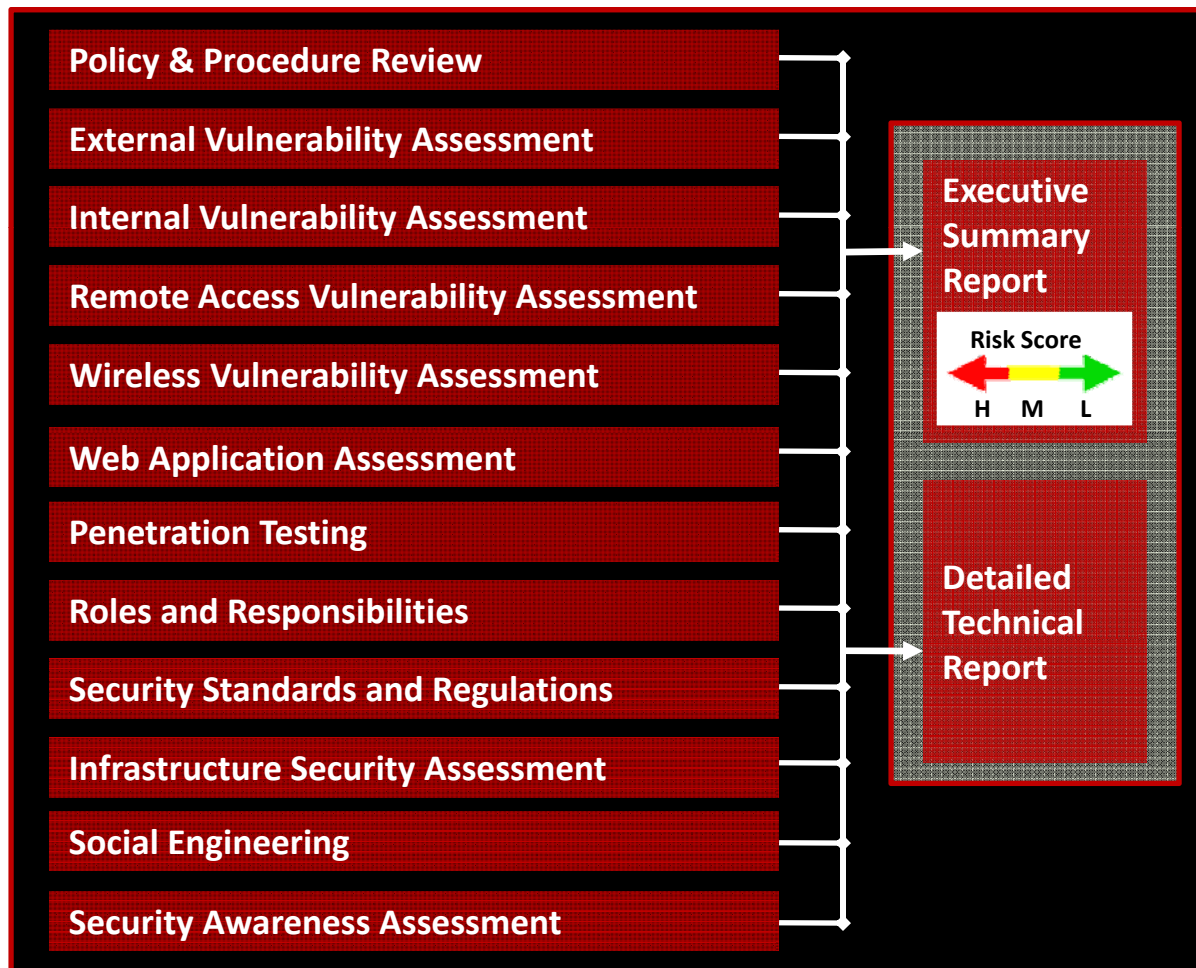
Risk Assessment Methodology



Risk Defined - Risk can be defined as the possibility or probability of an event occurring that will have an impact on an environment.

Risk can be measured in terms of **impact** and **likelihood**. The greater the impact or likelihood leads to greater risk. This can be used in context when assessing the technology or business risks associated with computer systems.

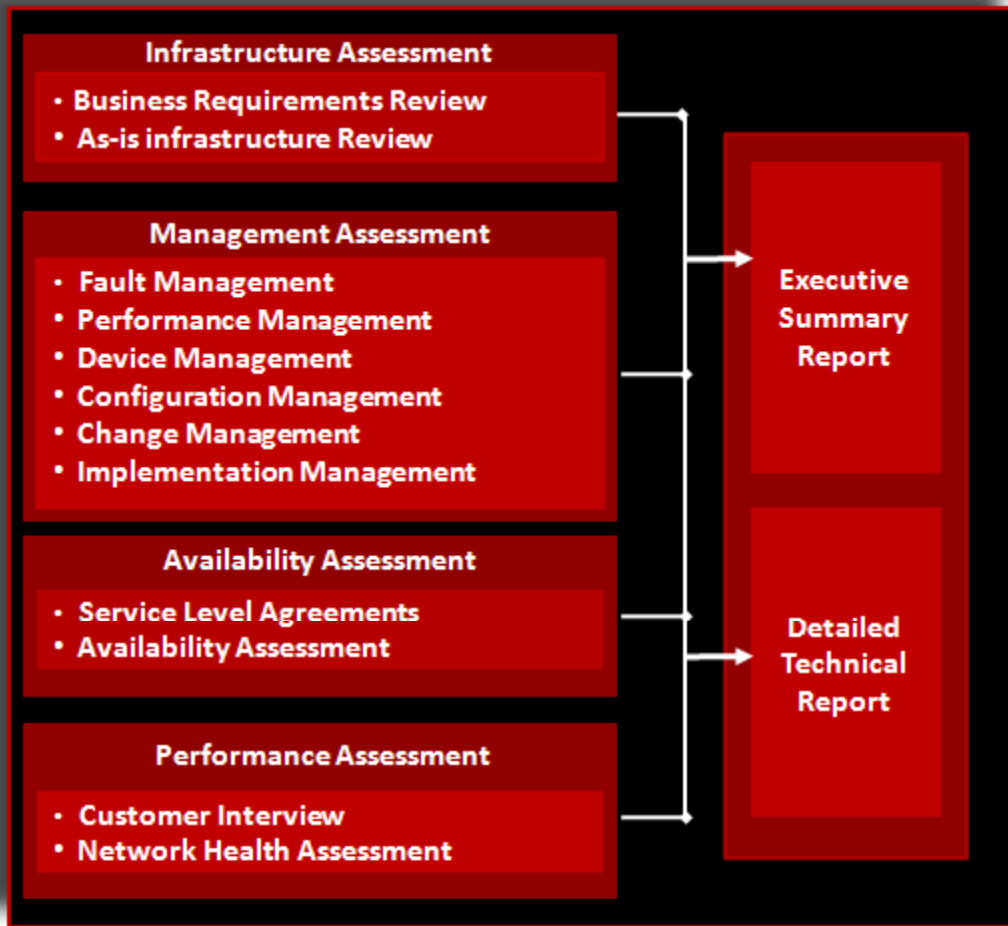
Vulnerability Assessment Methodology



Identify vulnerabilities that could allow malicious users to gain access to customer's trusted networks and systems.

Vulnerability Assessments assist in improving the overall security posture by recommending actions to mitigate the identified vulnerabilities.

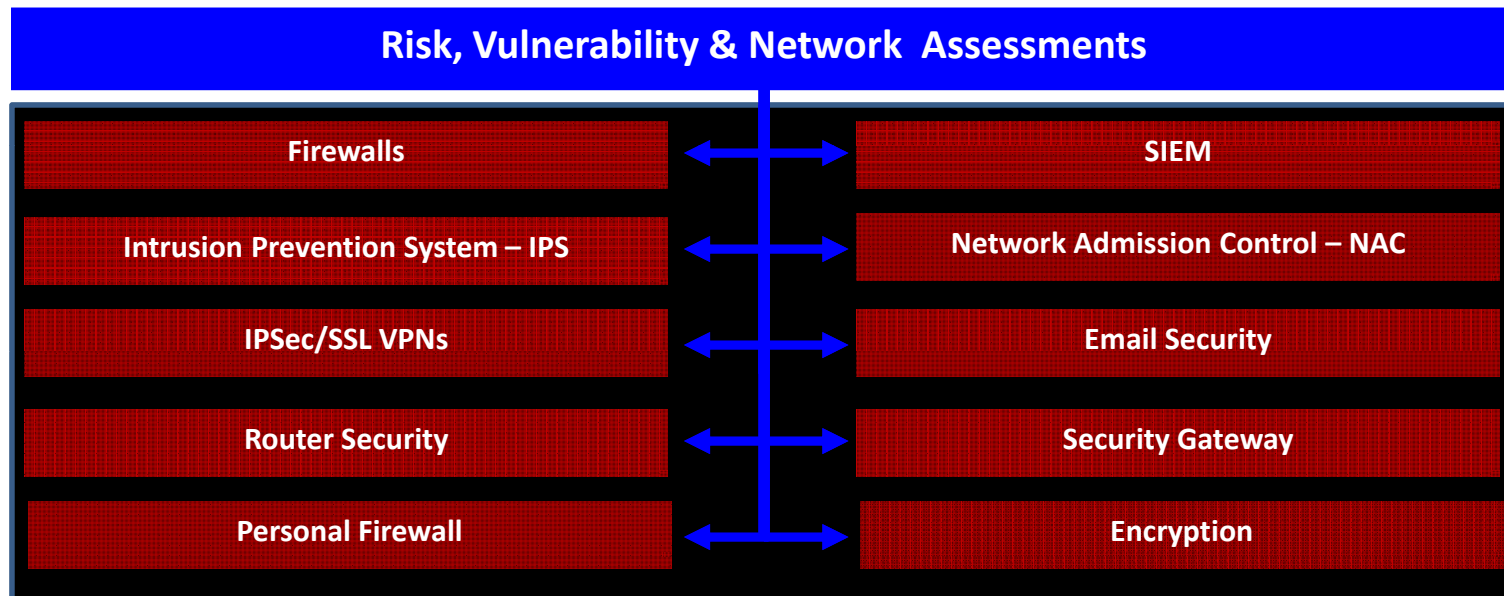
Network Assessment Methodology



Presidio will identify vulnerabilities in the network infrastructure that could potentially impact “availability”.

Presidio’s network assessment will review business requirements, management controls, service level agreements, network availability and network health.

Controls



In Summary

- Prepare early!
- Document your security strategy, policies and procedures
- Assess your risks and vulnerabilities at regular intervals (recommended annually)

Executive Roundtable Invitation

- **ATS and Presidio are offering the first six (6) webinar registrants an opportunity to attend for an informal roundtable on Security Strategy**
- The session will be limited to six (6) individuals to facilitate discussion with all
- Registration is available on a first-come first-serve basis so please register early to save your spot
- Dates/times/location will be scheduled with the registered individuals
- Email daniellem@appliedtechnologyservices.com to participate



Applied Technology Services, Inc.

Your Partner in Technology

www.appliedtechnologyservices.com

Contact Info

Danielle Marchese

Applied Technology Services, President

(410) 900-4321

daniellem@appliedtechnologyservices.com



Applied Technology Services, Inc.

Joe Leonard

Presidio, Security Practice Manager

(301)313-2158

jleonard@presidio.com



PRESIDIO

Be Secure in the Knowledge

Questions?

