

Security Management

- Managing security
- Assessing security management
- Security and technology

Assessments cover management and technology

- Security is a process not a product:
“Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. “

<http://www.schneier.com/crypto-gram-0005.html>

Management Principles

- Levels of management
 - Strategic
 - Tactical
 - Operational
- Command and control loop
 - Information flows up
 - Control flows down

Class 3

3

Management Principles

- Strategic
 - Fulfilling the organization's purpose
 - Long term, 3 to 5 years and beyond
- Tactical
 - Ensuring strategic goals are met
 - Often organized around annual budget cycle
 - Operations and project management
- Operational
 - Fulfill tactical goals
 - Management of day-to-day processes

Class 3

4

Governance

- How an organization is organized and administered to meet its goals
- Governance is achieved through:
 - The management structure,
 - Assignment of responsibilities and authority,
 - Establishment of policies, standards and procedures,
 - Allocation of resources, monitoring, and accountability.
- Governance is required to ensure that tasks are completed appropriately, that accountability is maintained, and that risk is managed for the entire enterprise.

Class 3

5

Internal Controls

- Processes designed to ensure an organization is properly governed:
 - Operations are effective and efficient
 - Financial reports and other management information is reliable
 - The organization is complying with relevant laws and regulation
- Ensure management directives are properly carried out

Class 3

6

Management Principles

- Tools of management
 - Policies
 - Procedures
 - Standards

Class 3

7

Management Principles

- A security assessment looks at
 - Are there comprehensive, documented information security:
 - Policies
 - Procedures
 - Standards
 - Are these followed consistently throughout the organization?

Class 3

8

Management Principles

- A security assessment looks at the adequacy of management systems governing information security
- Audits tend to look at the management control systems themselves, which rely on properly secured information systems

Class 3

9

Assessment Management Components

- Organizational security policy
- Authority and accountability of senior security executive
- Policies governing relevant security elements
- Documented procedures to implement policies
 - Account management
 - Change management
- Security standards
- Controls to ensure compliance with policies, standards, and procedures

Class 3

10

Assessment Management Components

- Is the security management system complete?
- Does the security management system meet the organization's needs?
- Is their compliance with the dictates of the security management system
- Is the intent of the security management system supported by technical security measures

Security and Technology

Technology and Assessments

- Technology exists to serve an organization's mission, goals, and objectives
- Technology should be configured and operated consistent with an organization's policies and procedures
- A single end user service relies on many different technical components, hence a flaw in any one of them can compromise the service

Class 3

13

Technology and Assessments

- Technical components are inter-related
- Understanding how they are interrelated is required to perform an assessment
- Similar technical components suffer from similar vulnerabilities

Class 3

14

Technology and Assessments

- A simple technical classification:
 - Servers
 - Network
 - Clients (desktops)

Class 3

15

Technology and Assessments

- A more complex technical classification:
 - Servers
 - Application
 - Mail
 - DNS
 - DHCP
 - Network
 - Switches
 - Routers
 - Wireless access points
 - Links
 - Clients (desktops)
 - Windows
 - Apple

Class 3

16

Technology and Assessments

- **A different complex technical classification:**
 - **Servers**
 - Application
 - DBMS
 - Operating System
 - Hardware/physical security
 - **Network**
 - Session Layer
 - Network layer (routed and routing protocols)
 - Data link layer (switches, VLANs and trunks)
 - Physical layer (media)
 - **Clients (desktops)**
 - Application (browser, word processor)
 - Operating system
 - Hardware/physical security

Class 3

17

Technology and Assessments

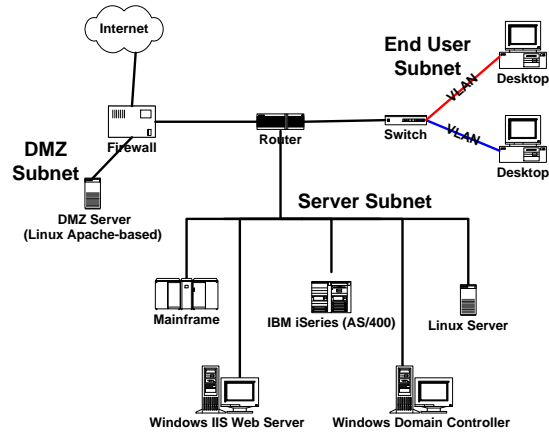
- **How should YOU categorize technology?**
Depends on
 - **Project Scope**
 - **Feasible level of detail**
 - **Risk**
 - **Which devices are most likely to have vulnerabilities**
 - **Which devices carry or store the most important information**
 - **Which devices are the most likely targets for threats**

Class 3

18

A Sample Framework

We will use this for the rest of the class



Class 3

19

Types of Security Assessment

Class 3

20

Assessment types

- Audit
- Security assessment
- Vulnerability Scan
- Penetration test

Class 3

21

Assessment Types

- Audits, security assessments, vulnerability scans, and penetration tests are all ways to analyze risk.
- They emphasize different aspects of risk management, different types of vulnerabilities, and different types of threat.
- Risk can be measured in different ways

Class 3

22

Assessment types

- **FFIEC definitions:**
 - **Audits.** Auditing compares current practices against a set of standards. Industry groups or institution management may create those standards. Institution management is responsible for demonstrating that the standards it adopts are appropriate for the institution.
 - **Assessments.** An assessment is a study to locate security vulnerabilities and identify corrective actions. An assessment differs from an audit by not having a set of standards to test against. It differs from a penetration test by providing the tester with full access to the systems being tested. Assessments may be focused on the security process or the information system. They may also focus on different aspects of the information system, such as one or more hosts or networks.
 - **Penetration Tests.** A penetration test subjects a system to the real-world attacks selected and conducted by the testing personnel. The benefit of a penetration test is that it identifies the extent to which a system can be compromised before the attack is identified and assesses the response mechanism's effectiveness. Because a penetration test seldom is a comprehensive test of the system's security, it should be combined with other monitoring to validate the effectiveness of the security process.

Class 3

23

Assessment types - Scope

- Audit
 - Review information technology management practices
- Security assessment
 - Assess device configuration
- Vulnerability Scan
 - Assess services visible from the network
- Penetration test
 - Attempt to actually gain unauthorized access to a system

Class 3

24

Assessment types - Methods

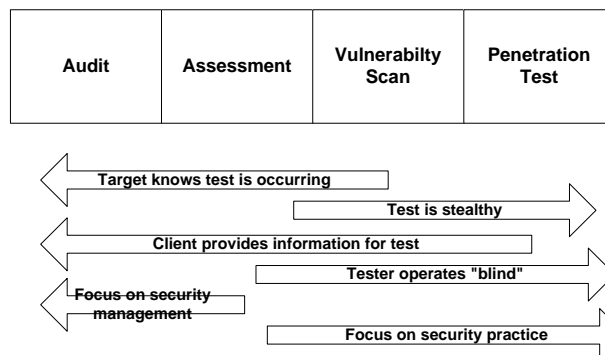
- Audit
 - Interviews, documentation reviews, observe actual operations
- Security assessment
 - Print/download configuration files, use host-based assessment tools
- Vulnerability Scan
 - Network scanning tools
- Penetration test
 - Execute exploits and perform device identity spoofing and social engineering

Class 3

25

Assessment types – Summarized

Note: These are general tendencies



Class 3

26

Audit

- Compliance with:
 - Organizational Policies
 - Regulatory Mandates
 - General principles of organizational governance and control
- In the strict definition, performed by designated internal auditors, public accounting firms, or other specialized parties

Class 3

27

Audit

- An IT audit may involve assessing the quality of information security controls.
- Audits (in the strict sense) are different from other forms of assessment. Their primary focus is governance and internal controls, not security in itself
- There is enough overlap that it is useful to include audits
 - With increased reliance on information systems, you cannot have good internal controls without having reliable, secure information systems

Class 3

28

Security Assessment

- Review of technical and administrative countermeasures
- Technical assessments include review of device configuration to ensure security standards are met
- Focus on technical controls, though may also review security policies and procedures, and review physical security

Class 3

29

Vulnerability Scan

- Automatically scans a network to find possible security vulnerabilities
 - Are there services visible from the network that present possible risks?
 - How much information is given away via accessible network services?
 - Mimics the initial stages of what an attacker might do.
- In between a security assessment and a penetration test in objectives and scope.

Class 3

30

Penetration Test

- Demonstrate feasibility of attacking and compromising a system
- A very narrowly focused attempt to look for security holes in a critical resource, such as a firewall or Web server.
- Often done without the knowledge of technical staff (to better test response to possible intrusion)
- Penetration testers may only be looking at one service on a network resource. They usually operate from outside the firewall with minimal inside information in order to more realistically simulate the means by which a hacker would attack the site.