Organizational Security Policies, Planning, & Dynamics

Module 3

Module Objectives

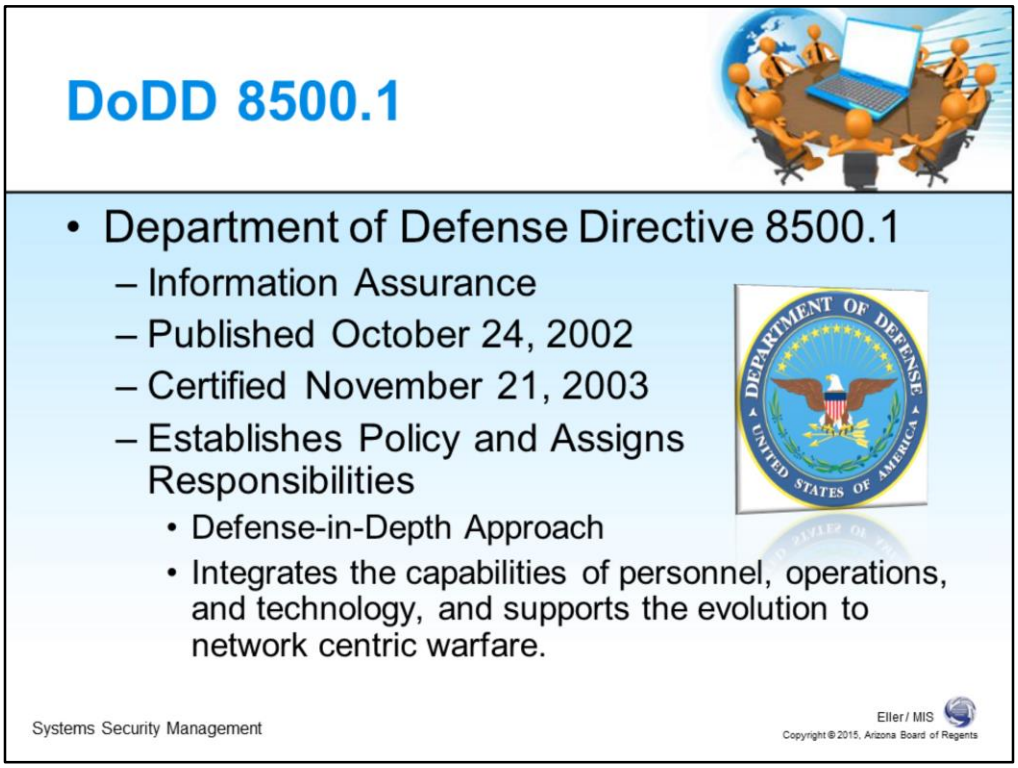
- DoDD 8500.1
- IA Policy
- Security Principles
- The Need for Policies
- Accreditation & Certification
- Assessments
- IA Domains
- Accountability Process/Program
- Operational Considerations & Review
- Mission, Objectives, & Goals
- Systems Testing & Evaluation (ST&E)
- Vulnerability Scanning
- Penetration Testing
- Blue vs. Red
- Next Module…

Systems Security Management

Eller / MIS

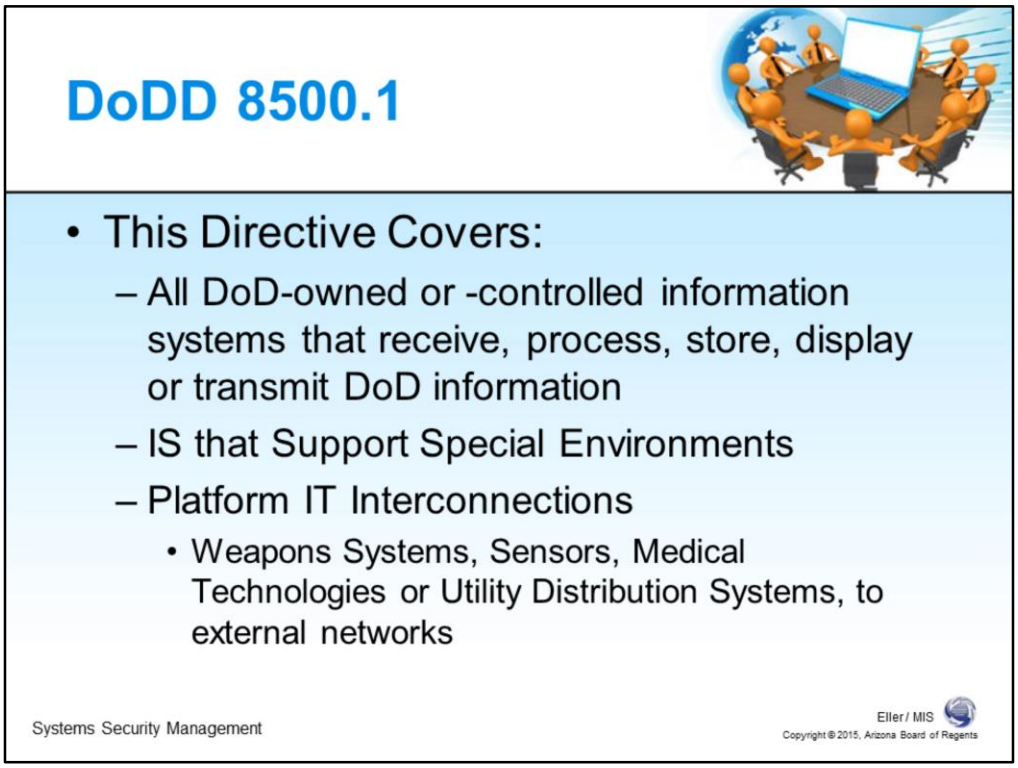
At the end of this module, you should be able to:

- Describe the Department of Defense Directive 8500.1.
- Understand what Information Assurance Policies are and why they are necessary.
- Describe security principles and understand the need for policies.
- Understand the need for accreditation and certification.
- Understand the need for assessments.
- Understand the two Information Assurance domains and why they are important.
- Describe operational considerations and review for adopting IA.
- Understand the need for a mission, objectives, and goals when adopting an IA program.
- Describe systems testing and evaluation.
- Understand what vulnerability scanning is.
- Understand what penetration testing is.
- Describe the concept of blue versus red.



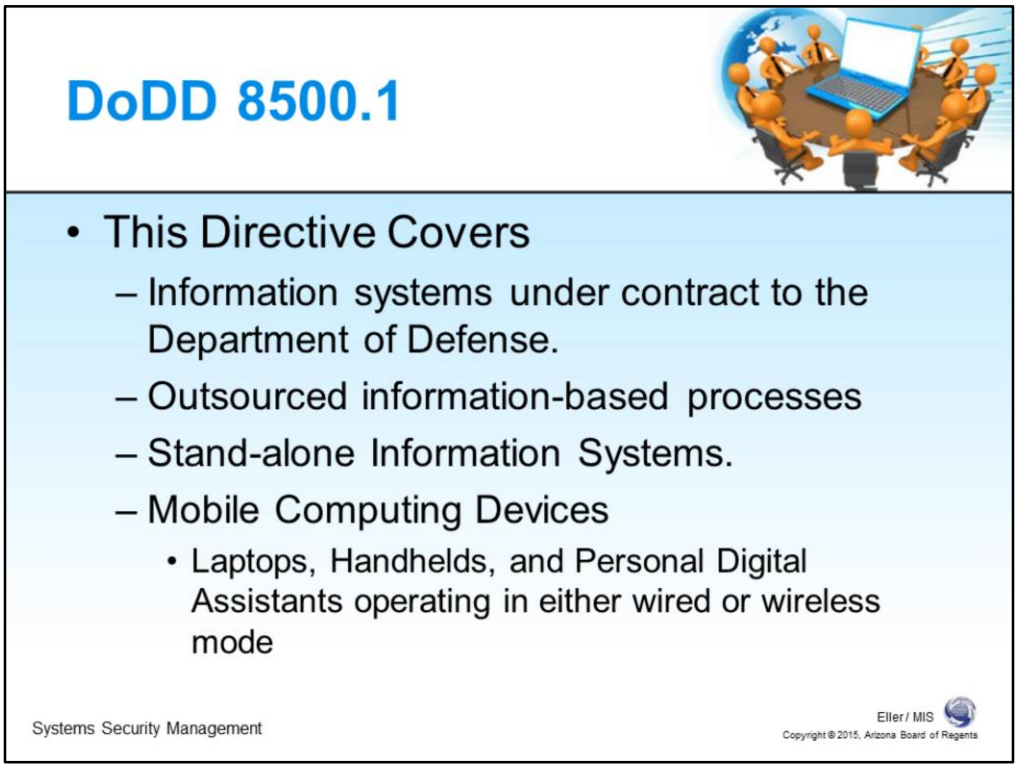
Department of Defense Directive 8500.1

The Department of Defense Directive 8500.1 was created to define the Government's Information Assurance program. DoDD 8500.1 was originally published on October 24, 2002 and certified on November 21, 2003. This directive establishes official government policy for its Information Assurance program and assigns responsibilities to different government agencies. The directive takes a defense-in-depth approach to Information Assurance, integrating the capabilities of personnel, operations, and technology, and supporting the evolution to network centric warfare.



Department of Defense Directive 8500.1 (continued)

DoDD 8500.1 was designed to cover all Department of Defense owned or controlled information systems that receive, process, store, display, or transmit DoD information. The directive also covers information systems that support special environments, such as remote posts, and platform IT interconnections, or platforms that communicate with other networks. This would include weapons systems, sensors, medical technologies, or utility distribution systems.

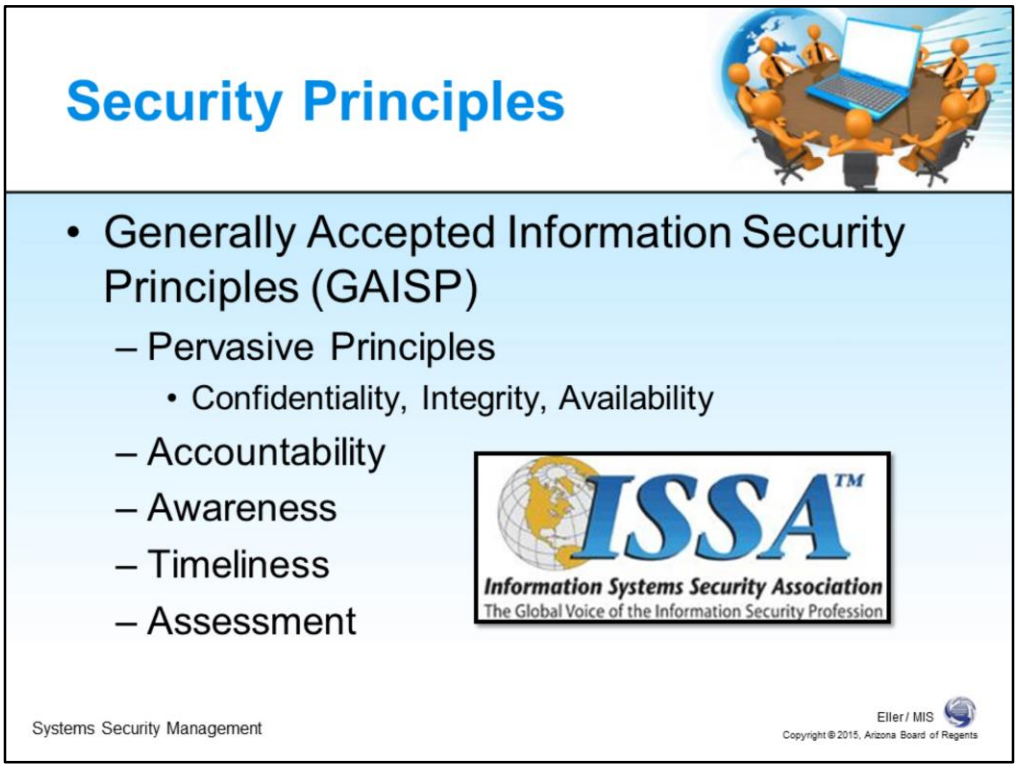


Department of Defense Directive 8500.1 (continued)

DoDD 8500.1 also covers any information systems that are under contract to the Department of Defense, outsourced information-based processes, and stand-alone information systems. In addition, the directive covers all mobile computing devices including laptops, handhelds, and personal digital assistants operating in either wired or wireless modes.

Information Assurance Policy

Information assurance policies are designed to assure confidentiality, integrity, and availability. The U.S. Government adopted an official information assurance policy which also affects defense contractors and other government contracts. In general, IA policies will vary; however all policies should include policy definitions, the creation of information system directives (such as DoDD 8500.1), the creation of roles and responsibilities for carrying out policies, and should define any disciplinary, civil and criminal consequences should any information systems be breached.



Security Principles

The Generally Accepted Information Security Principles, or GAISP, is based on a solid consensus-building process that is central to the success of this approach. Principles at all levels are developed by information security practitioners who fully understand the underlying issues of the documented practices and their application in the real world. Here are some of the pervasive principles:

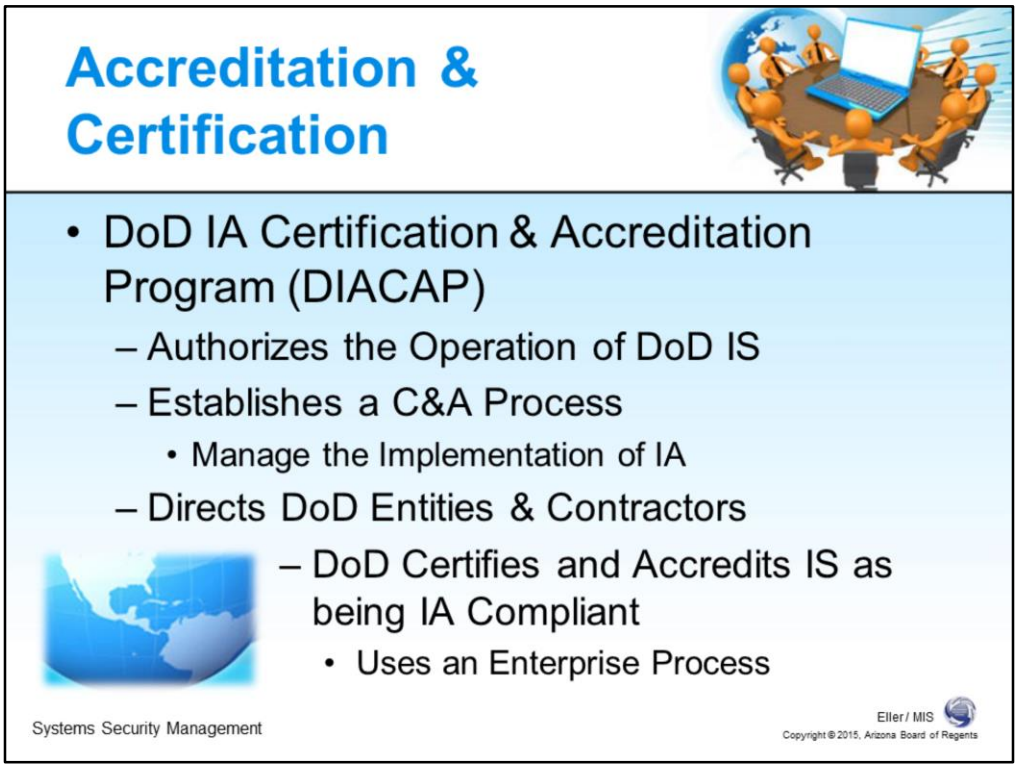
- Computer security supports the mission of the organization
- Computer security is an integral element of sound management
- Computer security should be cost-effective
- Systems owners have security responsibilities outside their own organization
- Computer security responsibilities and accountability should be made explicit
- Computer security requires a comprehensive and integrated approach
- Computer security should be periodically reassessed
- Computer security is constrained by societal factors

Each of the above principles is expected to work closely with the Information Assurance triangle of Confidentiality, Integrity, and Availability. The importance of GAISP involves determining accountability, raising awareness, the timeliness of response to issues, and overall assessment of information systems.

The Need for Policies

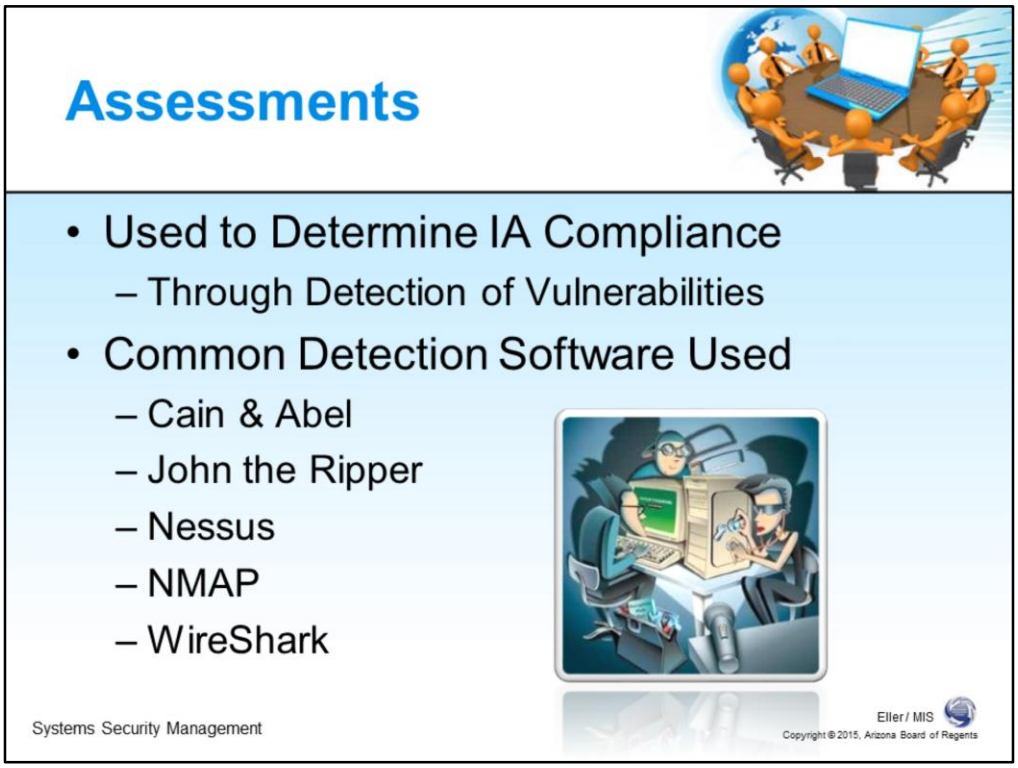
Do organizations have a need for information security policies? The answer to that question is yes. Any organization that makes use of information systems for storing or analyzing any data will absolutely need some sort of information security policy. This is especially true if the organization stores any data of a sensitive nature.

So how then does an organization develop a solid security policy? Well, the start of a security policy should begin with research by a team of people within the organization. Many organizations, especially public organizations such as Universities, publish their security policies online, and this is a great place to start. The team developing the policy should make a list of the different security needs of the organization. This will help focus the team and the policy. Finally, the team should spend some time brainstorming to determine additional information security areas to include in the policy.



Accreditation and Certification

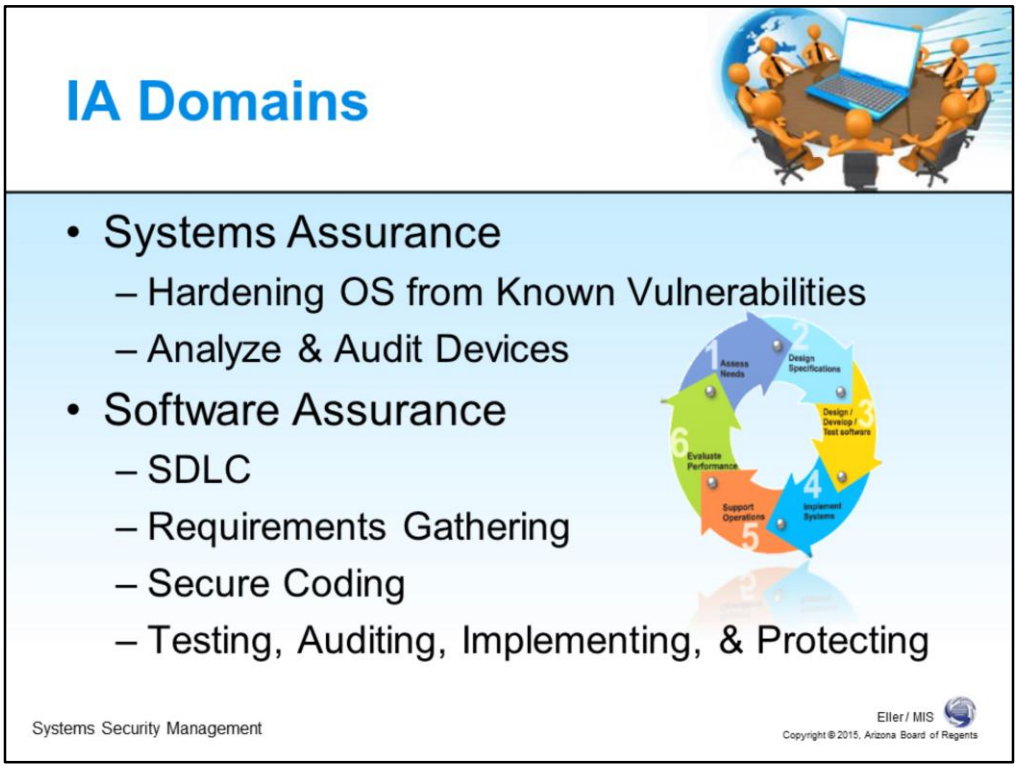
The Department of Defense Information Assurance Certification and Accreditation Program, or DIACAP, authorizes the operation of DoD information systems. The program establishes a certification and accreditation process that helps SysAdmins manage the implementation of IA. DIACAP also directs DoD entities and contractors in the development of a successful IA program. The DoD then certifies and accredits information systems as being Information Assurance compliant using an enterprise-level process.



Assessments

Assessments are used by the Government to determine IA compliance through the detection of vulnerabilities in systems and software. These assessments are completed with the use of freely available tools on the Internet. These tools include:

- **Cain & Abel** – This software is designed to recover and crack passwords from systems. This is a Windows-based utility.
- **John the Ripper** – This software is another password cracking utility for recovering passwords from systems. John the Ripper is Linux-based.
- **Nessus** – This software is used to scan networks systems to identify open network ports and operating system (OS) vulnerabilities. There is a free community version that is limited to home use and for training. If you are interested in scanning more systems or using it for a business, the professional version should be purchased.
- **NMAP** – This software is used to scan networks for network exploration, network inventory, and security auditing.
- **WireShark** – This is a protocol analyzer that gives you insight into the traffic and information going across the wire; the analysis is achieved by putting a network interface card (NIC) into promiscuous mode and capturing all traffic that comes to the card.



Information Assurance Domains

There are two different domains with regard to Information Assurance: Systems Assurance and Software Assurance.

Systems Assurance

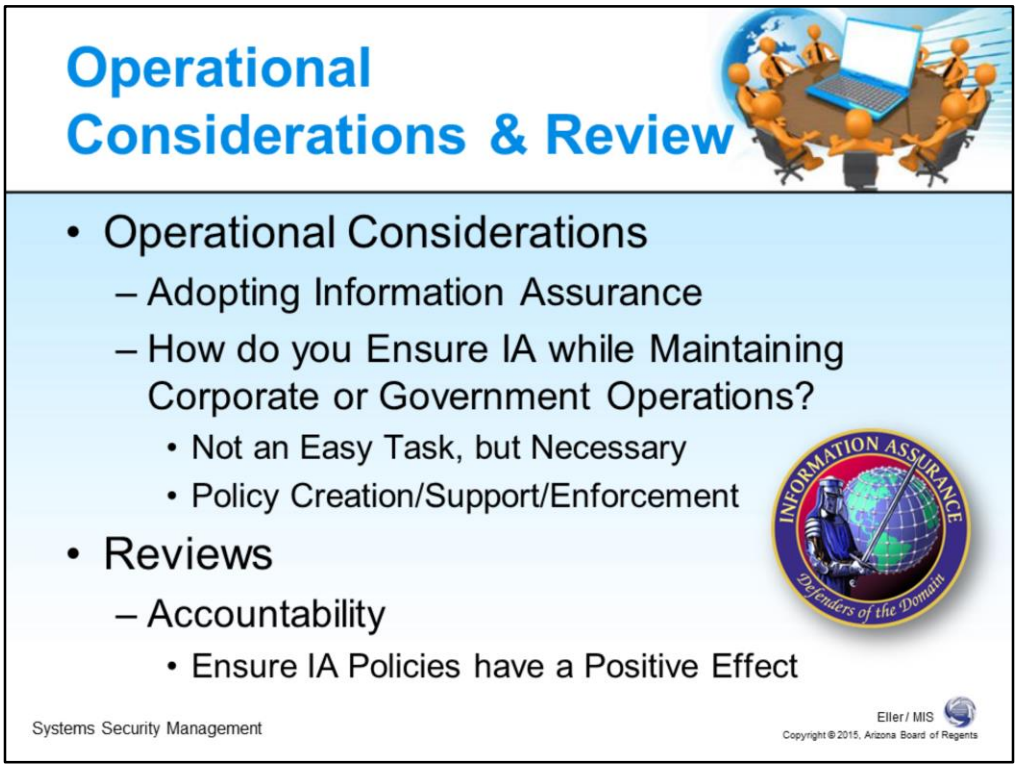
Systems assurance involves working to harden the operating system from known vulnerabilities. This would include installing operating system patches, using firewalls, and setting system access permissions. In order to ensure Systems Assurance the SysAdmin should spend time analyzing and auditing all devices communicating with information systems on the network.

Software Assurance

Software assurance is a different beast altogether. In order to provide software assurance, applications developers need to closely adhere to the software development life cycle (SDLC). This includes spending time gathering requirements, developing the application using secure coding methods, then testing and auditing before implementing and protecting the application.

Accountability Process/Program

Information Assurance requires accountability and accountability requires metrics. In order for an organization to adopt Information Assurance, the organization will need to develop a process or program that will generate metrics that can be tracked. In addition, personnel will need to be trained in Information Assurance techniques and how to use the collected metrics to ensure accountability. Government agencies and contractors that need to adhere to DoDD 8500.1 will need to create an oversight committee in order to ensure Information Assurance.



Operational Considerations and Review

When adopting an Information Assurance program, how do you ensure Information Assurance while maintaining corporate or government operations? In many cases this is not an easy task, but it is possible and necessary. The organization should begin with policy creation as we have discussed here, but that is not the only component to a successful program. A successful IA program needs to have the full support of the organization from the top down. In addition, IA policy needs to be fully enforced. Much of this can be accomplished through technological means; however, some user training will be necessary to ensure full compliance.

Once an IA program is in place, the SysAdmin along with the assistance of management should perform a review of the program in order to not only provide some accountability but also to ensure the IA policies the organization has been enforcing are having a positive effect on information security.

Mission, Objectives, and Goals

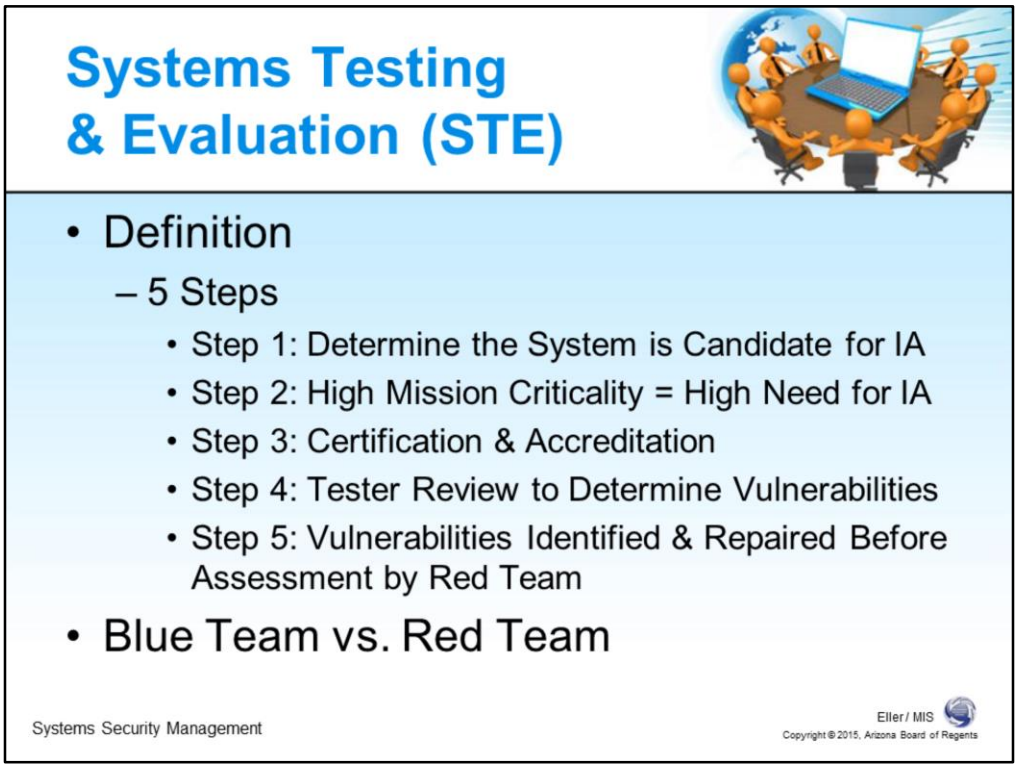
When developing an official Information Assurance program it will be necessary to determine the program's mission, objectives, and goals.

Mission – Why is an IA program necessary?

Objectives – What would creating an IA program do for the organization?

Goals – What would be necessary for the creation of an IA program and how would an IA program benefit the organization?

When combined together, the mission, objectives, and goals fit together to form a complete picture of what an IA program would look like in the organization, just like pieces in a puzzle. They also work to create a framework which can be used to help develop an official organizational IA policy. In addition, they help to highlight the importance of Information Assurance to the organization.



Systems Testing and Evaluation (ST&E)

System Testing and Evaluation is the examination and analysis of the safeguards required to protect an Information System, as they have been applied in an operational environment, to determine the security posture of that system. There are five steps involved with ST&E:

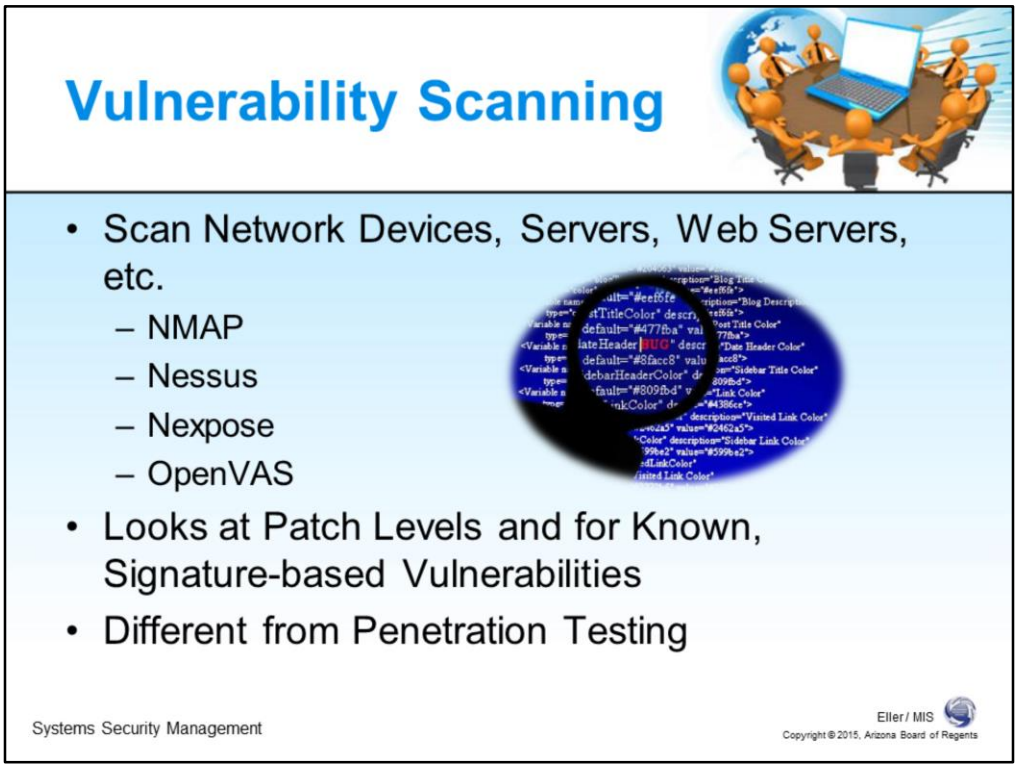
Step 1: Determine the System is a Candidate for Information Assurance
Whenever an Information System is needed by the Government, it will be necessary to determine if the system is a candidate for Information Assurance. In other words, what is the system's purpose and what kind of information will be stored on the system.

Step 2: High Mission Criticality = High Need for Information Assurance
Once the information system is determined to be a candidate, the purpose of the information system needs to be determined. If the system is determined to be a highly mission critical system then there is a high need for Information Assurance.

Step 3: Certification and Accreditation
Once a system has been determined to be a candidate for IA and the need has been determined, the system will need to be certified and accredited for Information Assurance by the DoD.

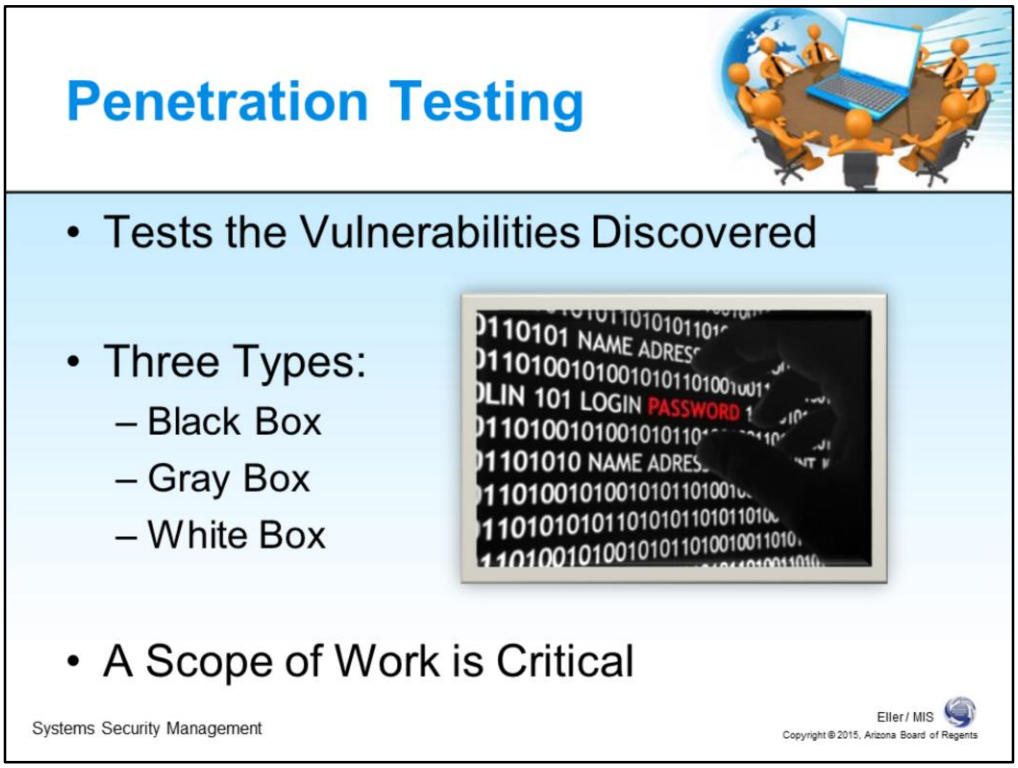
Step 4: Tester Review to Determine Vulnerabilities
After certification, the system needs to undergo a tester review in order to determine if any vulnerabilities exist. This will be covered further in the next slide.

Step 5: Vulnerabilities Identified and Repaired Before Assessment by Red Team
Should the tested review in step 4 reveal any vulnerabilities, they must be repaired and retested in order to ensure the vulnerabilities have been removed. Once this has happened, the information system will be assessed with a penetration test to test the feasibility and threat level of any discovered vulnerabilities.



Vulnerability Scanning

Vulnerability scanning is done by using various free and paid tools to scan your networks and test systems for weaknesses; it is something that should be done on a regular basis to ensure that new vulnerabilities aren't introduced and that systems stay up to date with patches. These tools scan for open and vulnerable ports, look for vulnerabilities based on signatures in their related databases (threats are given severity levels, based on criticality), can test variables on web page forms, and ensure that applications aren't susceptible to things like Cross-Site Scripting, SQL injections, and a host of other, easily overlooked weaknesses. By leveraging some of the scanners' patch management APIs, you can sync your vulnerability scanner to your patch system (Microsoft's WSUS, for example) to ensure that systems stay in compliance with corporate policies. Once the tests are complete, the results are given to the SysAdmins and they attempt to resolve many of the more critical issues before a penetration test is done.



Penetration Testing

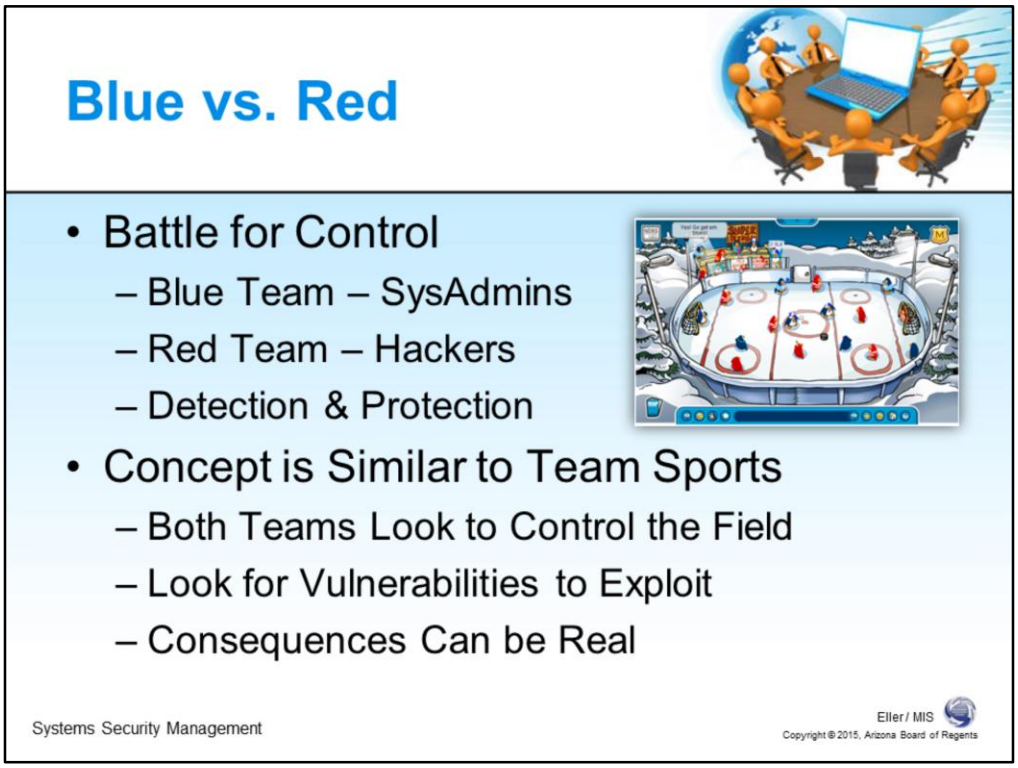
Penetration testing differs from vulnerability assessments in that it actually verifies that the discovered vulnerability is exploitable and is indeed a threat to the organization. A theoretical vulnerability is fine if no one is able to exploit it; by doing a pen test, an organization is determining the level of threat to systems and the network. There are three types of pen tests: black box, gray box, and white box.

Black Box testing is usually conducted by outsourcing to a professional security company, rather than internal security teams. The outsourced company is given almost no information about the network and systems/applications that are being used - oftentimes they only have a company name, or are simply given an IP range to attack - this is to simulate an external threat.

Gray Box testing is conducted with limited knowledge of the networks and systems that need to be tested. This usually starts off as Black Box testing for a highly secured environment and it's determined that a little knowledge is required to make a more thorough analysis; again this is usually conducted by an outsourced company.

White Box testing is usually conducted by an internal "Red Team", with full knowledge of the network, the systems, and the applications being used; this type of testing models an attack by an internal threat - maybe a disgruntled employee or contractor with permissions on the network. White Box testing is by far the most common type of testing done; often this is conducted in a Blue vs. Red "Capture the Flag" scenario.

Regardless of the type of penetration test carried out, a scope of work is critical to have been completed before testing begins. This lays out the requirements of testing, where the hackers dare not tread, and covers Rules of Engagement such as: social engineering limits and expectations, what to do in case a system is damaged, instructions for a "get out of jail free" situation in the event that physical pen tests are conducted and a tester is caught by security, and several other aspects related to the testing. This is necessary to ensure that both sides are aware of limitations and boundaries for conducting the tests.



Blue vs. Red

Blue versus Red is a system penetration test that is designed to be a battle for control of a network. The Blue team is comprised of System Administrators while the Red team is comprised of hackers. The goal of the "game" is detection and protection: detecting the hackers attempts to compromise the network and protecting the network from being hacked.

The concept of Blue versus Red is similar to team sports, where both teams are looking to control the field by looking for vulnerabilities to exploit in the network. The catch is that the consequences for failure can be real. By looking for real-world means and methods for breaching a network, the Red team is highlighting security areas where the Blue team is lacking.

Next Module…

- SA & IS Roles
- Information Sensitivity & Classification
- Data Ownership
- Copyrights
- Digital Millennium Copyright Act
- Piracy
- Hiring & Termination
- Internal Controls
- Separation of Duties
- Lost or Stolen Equipment
- Law Enforcement Interaction

Systems Security Management

Eller / MIS

In the next module we will continue the discussion of organizational security as it involves personnel and legal considerations, including:

- SA & IS Roles
- Information Sensitivity & Classification
- Data Ownership
- Copyrights
- Digital Millennium Copyright Act
- Piracy
- Hiring & Termination
- Internal Controls
- Separation of Duties
- Lost or Stolen Equipment
- Law Enforcement Interaction

References

Information Assurance Policy. (2006, February 1). State of Maryland. Retrieved from http://www.dhmh.state.md.us/policies/summary.htm.

GAISP v3.0. (2004). *Information Systems Security Association*. Retrieved from http://all.net/books/standards/GAISP-v30.pdf.

IT 3.48: Information Assurance Assessment. (2007). *Air Support Operations Center*. Retrieved from http://www.cwid.js.mil/public/CWID07FR/htmlfiles/348ia.html.

Jogelkar, A. N. (2008). Achieving Information Assurance Through Operational Test and Evaluation. *International Test and Evaluation Association*. Retrieved from http://www.itea.org/files/2008/2008%20Journal%20Files/June%202008/jite-29-02-175.pdf.

Liles, S. (2005, June 24). Information Assurance Domains & Defining Software Assurance. *Selil*. Retrieved from http://selil.com/?p=57.

U.S. Department of Defense. (2002, October 24). DoD Directive 8500.1: Information Assurance. Retrieved from https://acc.dau.mil/CommunityBrowser.aspx?id=37475.

U.S. Department of Defense. (2007, November 28). DoD Instruction 8510.01: DIACAP. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf.