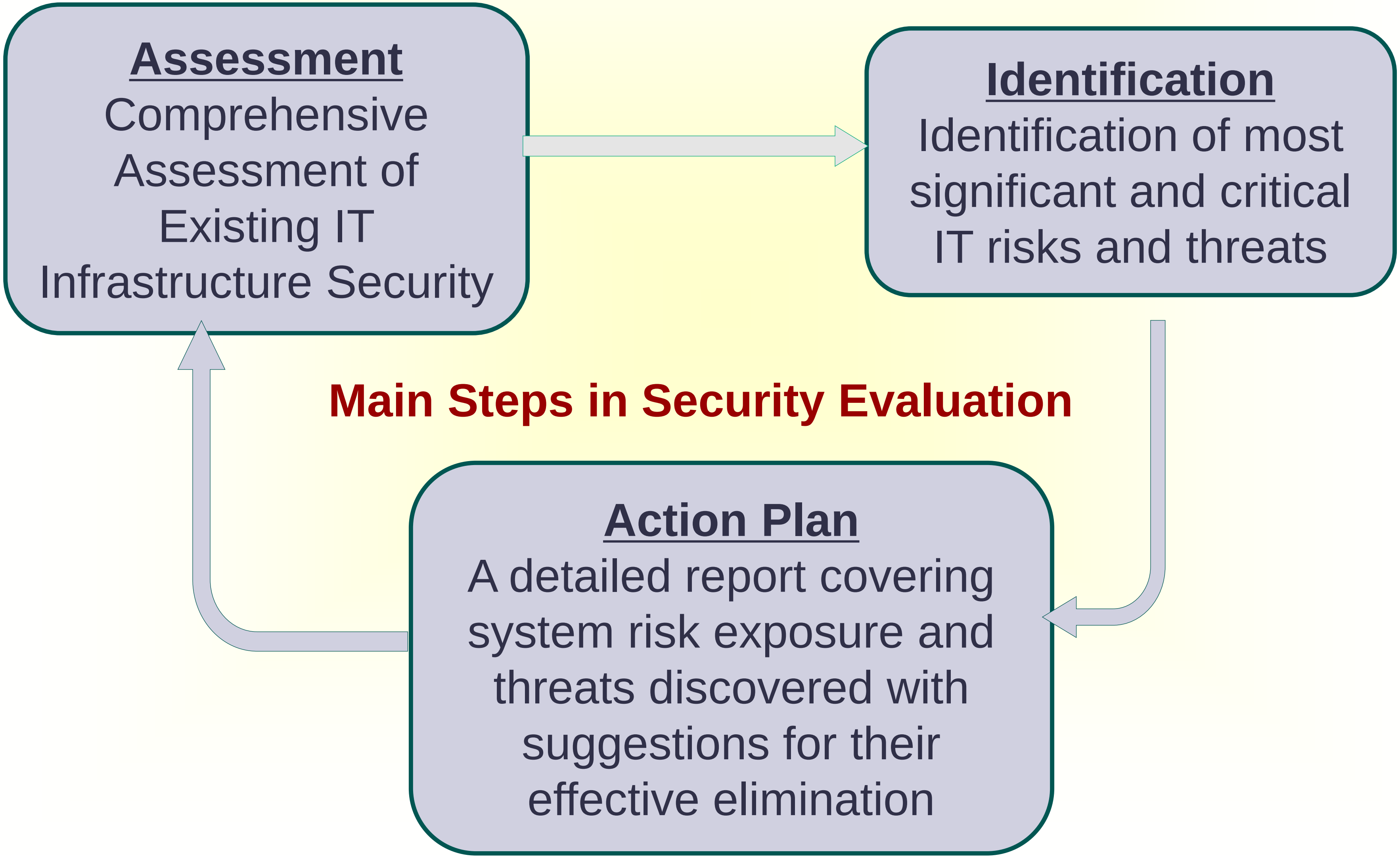
Chapter 7 – Security Evaluation

7.1 Introduction

- The main purpose of a security evaluation is to discover weak points in the architecture of IT infrastructure



Assessment
Comprehensive Assessment of Existing IT Infrastructure Security

Identification
Identification of most significant and critical IT risks and threats

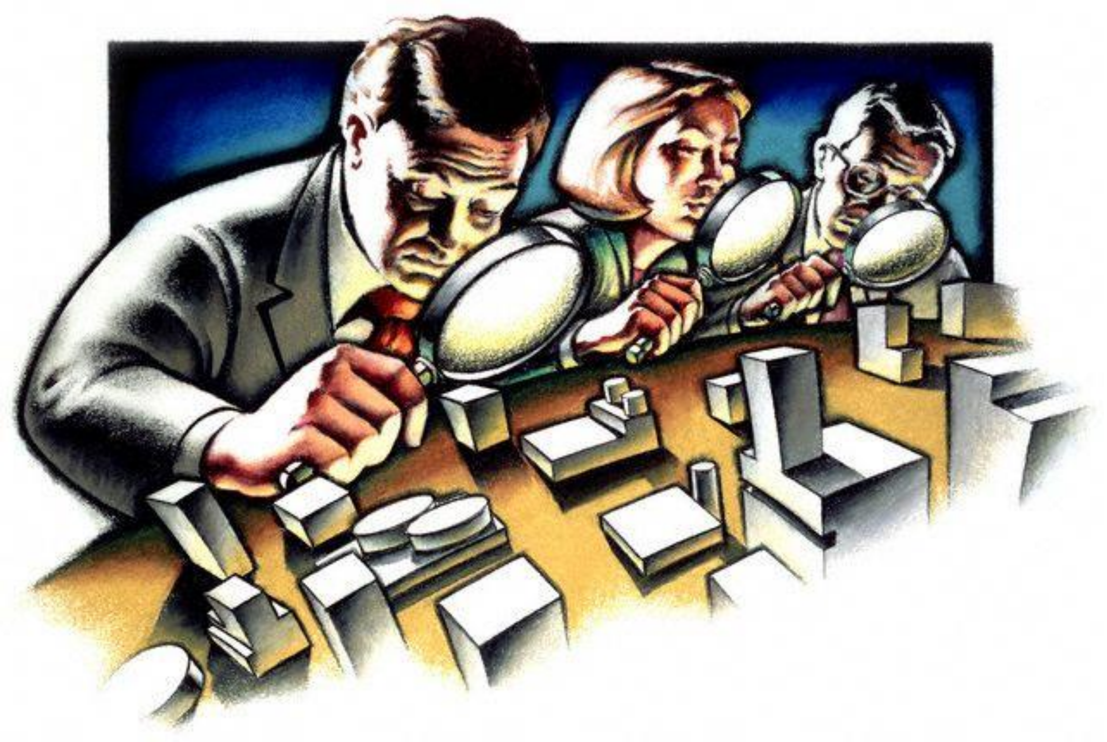
Action Plan
A detailed report covering system risk exposure and threats discovered with suggestions for their effective elimination

Main Steps in Security Evaluation

- Parameters for Security Evaluation
  - Network Architecture and Configuration
  - Firewalls and Routers Configuration
  - System Configuration
  - System Services and Applications Configuration
  - User Authentication and Access Management
  - Updates and Patches Management
  - Antivirus Software Management
  - Confidential Data Handling and Encryption
  - Backup System Management
  - Local Security Policy Review
  - Presence and Qualification of Internal Incident Response Team
  - Physical Security

7.2 Security Assessment Components

- Major security components involved in the assessment process
  1. Network Security
  2. System Security
  3. Application Security
  4. Operational Security
  5. Physical Security



1. Network Security Assessment

- Gather and evaluate network maps, installation procedures, checklists
- Scan networks and networked systems
  - Vulnerability Scanners: Nessus, OpenVAS, Retina, Nipper, SAINT, CoreImpact, etc.
  - Port Scanners: Nmap, Hping, Amap, TCPDump, Metasploit, etc.
  - Application Scanners: whisker, nikto
- Target Selection
  - Key systems (where important information are stored)
  - Exposed systems (where the bad guys play)
  - Gateway systems (intersection of networks)

2. System Security Assessment

- Gather and evaluate software/system inventory information, security standards, checklists, management procedures
- Review configurations with the administrator
- Use a security checklist to evaluate current configuration (Security Checklist example)
- Target Selection
  - Database Systems and File Servers
  - Network Application Servers
  - Desktops

3. Application Security Assessment

- Gather and evaluate application and internal development documents and source code
- Review source code for common programming flaws
- Use code analysis (scanning) tools
  - Fortify, RATS, ITS4, FlawFinder
- It is a skill dependent task and time consuming
- At minimum, evaluate development procedures

4. Operational Security Assessment

- Gather and evaluate procedures and contingency plans
- Evaluate overall security management
- Review backup and disposal procedures
- Examine business continuity and disaster recovery plans
- Look at automated security tasks (virus updates, patches, integrity checks)
- Look at administrator’s security practices

5. Physical Security Assessment

- Gather policy and procedure documents
- Examine facility and take pictures
- Building
  - Life Safety (fire/smoke detection, alarms)
  - Burglar alarms, security guards, police response time
- Security Perimeter
  - Strong doors, locks, visitor areas, sign-in procedures
- Server Rooms
  - Environmental controls and monitoring
  - Sufficient power and HVAC (Heating, Ventilation, and Air Conditioning)
  - Locked cabinets and equipment

- Reporting and Follow-up
  - Once the assessment is complete, a report is needed to inform the client of issues found
  - The report should explain findings in simple terms (remember the audience)
  - Reports should incorporate suggestions on how to overcome vulnerabilities and threats
  - Be available to answer questions and provide explanations

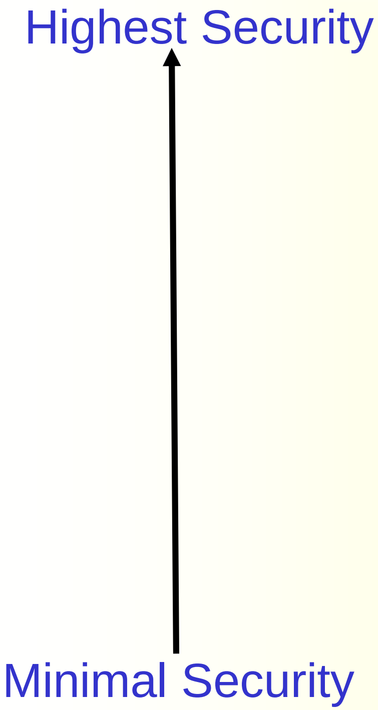
7.3 Methods for Security Evaluation

- TCSEC (1967-1999 by DoD of U.S.)
  - TCSEC (Trusted Computer System Evaluation Criteria) is a standard nicknamed The Orange Book because of its orange cover
    - TCSEC is the first collection of standards used to grade or rate the security of commercial computer products
    - It was modified to Trusted Network Interpretation (TNI) also named The Red Book
  - ITSEC (1991-2001 Europe)
    - European Information Technology Security Evaluation Criteria: as a result of harmonized national criteria by UK, Germany, France, and the Netherlands
  - CC (The Common Criteria) 1998- present
  - Other efforts (COBIT, ISO27K Series)

- The Orange Book
  - Most of the security criteria and standards in product security evaluation have their basis in the TCSEC, the first collection of standards used to grade or rate the security of computer system products
  - The criteria for security evaluation in the Orange Book were developed with three objectives in mind
    - to provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or sensitive information
    - to provide guidance to manufacturers as to what to build into their new, trusted commercial products in order to satisfy trust requirements for sensitive applications
    - to provide a basis for specifying security requirements in acquisition specifications

- The criteria also address two types of requirements
  - specific security feature requirements
  - assurance requirements
- TCSEC defines four security divisions (A, B, C, D) and seven security classes, called ratings (A1, B1, B2, B3, C1, C2, D)
- The four divisions are
  - D - Minimal Protection (Class D)
  - C - Discretional Protection (Classes: C1, C2)
  - B - Mandatory Protection (Classes: B1, B2, B3)
  - A - Verified Protection (Class A1)

- Products in higher security classes provide more security mechanisms and higher assurance through more rigorous analysis



- A1: Verified Protection
- B3: Security Domains
- B2: Structured Protection
- B1: Labeled Security Protection
- C2: Controlled Access Protection
- C1: Discretionary Security Protection
- D: Minimal Protection

Orange Book Security Classes

- The Orange Book was superseded by the Common Criteria as of 2005; but the general topics laid out in it are still key pieces of any security program and/or framework

- Scope and Limitations
  - The TCSEC was written for operating systems and does not translate well to other types of products or to systems
  - Also, the TCSEC focused on the security needs of the U.S. government and military establishments, who funded its development
  - All evaluation classes except C1 and C2 require mandatory access control, which most commercial environments do not use
  - Furthermore, the TCSEC did not address integrity, availability, or other requirements critical to business applications

- Contributions
  - The TCSEC provided a process for security evaluation of commercial products
  - Its existence heightened the awareness of the commercial sector to the needs for computer security
  - As a result, new varieties of products emerged in the 1990s, including virus checkers, firewalls, virtual private networks, IPsec implementations, and cryptographic modules

- The Red Book
  - The National Computer Security Center (NCSC) of the U.S. tried to address the scope problems by providing criteria for other types of products
  - It developed the Trusted Network Interpretation (TNI) of the TCSEC, also referred to as The Red Book, which is a restating of the requirements of the TCSEC in a network context, released in 1987
  - It attempted to address network security issues. Some of the shortfall of the Orange Book that the Red Book tried to address include the distinction between two types of computer networks:
    - Networks of independent components with different jurisdictions and management policies
    - Centralized networks with single accreditation authority and policy

- The ITSEC
  - ITSEC was developed because the Europeans thought that the Orange Book was too rigid
  - ITSEC was meant to provide a framework for security evaluations that would lead to accommodate new future security requirements
  - It puts much more emphasis on integrity and availability
  - The current issue is Version 1.2, published in 1991 followed two years later by its user manual, the IT Security Evaluation Manual (ITSEM), which specifies the methodology to be followed when carrying out ITSEC evaluations

- CC: The Common Criteria (1998-Present)
  - The Common Criteria (CC), sometimes referred to as the Harmonized Criteria, is a multinational successor to the TCSEC and ITSEC that combines the best aspects of ITSEC, TCSEC, CTCPEC (Canadian Criteria), and the U.S. Federal Criteria (FC) into the Common Criteria for Information Technology Security Evaluation
  - CC was designed to be an internationally accepted set of criteria in the form of an ISO (International Standards Organization) standard
- Read about
  - System Security Engineering Capability Maturity Model (SSE-CMM)
  - Backup and its Principles as a Grand Solution to all sorts of Security Problems

That is all I have

Thank you very much for attending and

Good Luck ☺.