

Class Seven

Topics:

- **Auditors – internal and external**
 - Internal Control
 - The Audit Work Process
 - Information Systems and the Financial Audit
 - Third Party Reviews (SAS 70)
- **Federal Government Standards (classified information)**
 - DoD “Rainbow Book” Concepts
 - The “Orange Book”
 - TCSEC, ITSEC, and the Common Criteria

8/24/2007

Class 7

1

Compliance Auditing

- Outside verification that organizational practices conform to some agreed upon standard
- Practices to be verified may include:
 - Internal control systems designed to:
 - Safeguard assets
 - Assure timeliness & reliability of information
 - Ensure errors and irregularities are discovered & corrected promptly
 - Operational efficiencies
 - Compliance with enterprise standards, procedures and policies
 - Compliance with government regulatory standards

8/24/2007

Class 7

2

Common Types of Compliance Audit

- Regulatory Agencies
- Internal Audit
- Certified Public Accountant
 - Primary concern is with the integrity of financial record keeping
 - Outside CPA audits may be required by law or as a condition of credit
 - Reviews systems relevant to processing significant financial data as expressed in financial statements
 - Risk is defined in terms of the likelihood of material error on financial statements

8/24/2007

Class 7

3

Regulatory Audits

- Determines if the organization is in compliance with external (usually government) laws, regulations, standards, and policies
- Common in financial services industry, especially banking
- May include information system security issues and the reliability of business records
- Often covers other areas:
 - Truth in Lending
 - Non-discrimination
 - Community Reinvestment Act compliance
- Federal Information Security standards – audit involved in TCSEC certification and accreditation process

8/24/2007

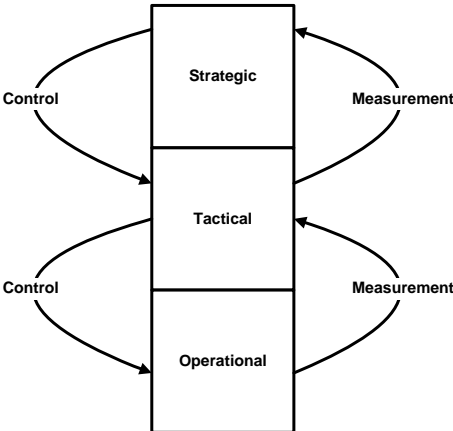
Class 7

4

Internal Audit - Systems of Internal Control

- The rudder or guidance mechanism ensuring the organization is on course
- The management feedback loop, of measurement and corrective actions
- Includes:
 - Accurate recording of performance information
 - Timely provision of information to supervisors and management
 - Specifying appropriate action
- Elements of Internal Control:
 - Management Controls
 - Systems Controls
 - Physical Controls
- Separation of Duties as an internal control:
 - No access to sensitive combinations of capabilities (e.g., to inventory records and to the physical inventory itself)

Internal Audit - Systems of Internal Control



Differences Between Security Administration and Auditing

- Security Administration:
 - Hands-on responsibility for configuration and administration of hardware and system software
 - Data custodian
 - Must make cost/benefit decisions
 - Reports to IT chain of command, often then to a Finance or Operations executive
- Audit:
 - Independent of systems administration
 - Should NOT configure or administer systems
 - Should report to an independent Audit Committee, reporting straight to the Board of Directors
 - Should evaluate risks, may specify alternatives, but usually does not mandate specific measures (unless a compliance audit)
 - Reports findings and recommendations based on risks, but leaves cost/benefit analysis to executives

8/24/2007

Class 7

7

The Audit Work Process

- Define organizational areas
- Rank each area for risk
- Define standards for control compliance
- Establish control objectives and how they are measured
- Develop work program to gather data on the effectiveness of controls
 - Review "General Controls" over the environment
 - If satisfactory, proceed to "Substantive Tests" of compliance of sample transactions
- Derive point of non-compliance, associated risks, and possible corrective action
- Review findings, analysis, and recommendations with each business area for verification
- Present final report to Audit Committee

8/24/2007

Class 7

8

Information Systems and the Financial Audit

- Are financial records properly recorded?
- Do the financial statements reflect accurately the true status of the enterprise?
- Reliance:
 - Are automated systems reliable enough to trust for audit purposes?
 - To what extent must manual reviews of hardcopy records and second party information be performed?
- General Controls Review
- Substantive Testing
- AICPA Standard Audit Statements (SAS)
 - SAS 3 - Requires review of IT environment controls as part of financial audit
 - SAS 55 - Defines the job of the IT control review by an auditor
 - SAS 70 - Review of third party service provider

8/24/2007

Class 7

9

Risk in Financial Audits

- Inherent Risk - risk of material error which internal controls must overcome. A function of the organization, its environment, and how the organization is managed.
- Control Risk - probability that internal controls will not prevent or detect material financial errors on a timely basis.
- Detection Risk - probability that material errors will not only escape internal control systems, but also the effort of external auditors

These all lead to:

- Audit Risk - the risk that financial auditors might accept financial statements as accurate when in fact they contain material misstatements.
- ***So what is a material misstatement?*** The smallest amount of misstatement that would mislead a reasonable person relying on the financial statements for decision making purposes (e.g., an investor, a lender, etc.)

8/24/2007

Class 7

10

What's a SAS 70?

- Statement of Accounting Standard 'Reports on the Processing of Transactions by Service Organizations'
- Used when one entity obtains services from another entity for:
 - Executing transactions and maintaining associated accountability
 - Recording transaction and processing data
- Type I vs. Type 2
 - Type 1 – review documented policies and procedures
 - Type 2 – review evidence that documented policies and procedures are being followed

8/24/2007

Class 7

11

Compliance Audits - US Federal Standards

- Role of government standards
- Civilian vs. national security
- Commonalities
- Why this matters for the private sector

8/24/2007

Class 7

12

Compliance Audits - US Federal Standards

- Certification - Evaluation of an application to see how well it meets security requirements. A technical evaluation for purposes of accreditation.
- Accreditation - Authorization to operate the application, based on the certification and other criteria.
- Software (or some other component) is **certified**, the entire working environment must be **accredited**, too
- Techniques for certification:
 - Risk Analysis
 - Validation, Verification, and Testing
 - Security Safeguard Evaluation
 - EDP Audit

8/24/2007

Class 7

13

Standards for Government Classified Data

- Clearance/Classification
 - Clearance – the subject's trustworthiness to access classified information
 - Classification – the harm to national security if the information is improperly disclosed
- Modes
 - Given a user based possessing certain clearances, and a mix of information having certain classification levels, how secure must the system be to enforce the security policy, based on the level of risk?
- System assurance and modes
 - Systems will be operated in different environments. Users with different clearances may or may not access the system. The type of assurance is related to how the system is used and by whom

8/24/2007

Class 7

14

Levels, Categories, and Labels

- Level - hierarchical sensitivity classification
- Category - Functional or departmental "need to know"
- Label - the combination of the level and all applicable labels
- Example:

| Labels | Categories | | |
|--------------|------------|---------|--------|
| | NATO | NUCLEAR | Crypto |
| Top Secret | | | |
| Secret | | | |
| Confidential | | | |
| Unclassified | | | |

8/24/2007

Class 7

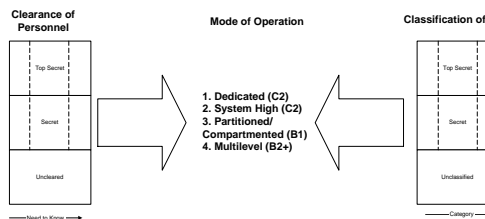
15

Clearances, Classification, and Modes

Clearance Level of authority (or authorization) possessed by the end user. Includes the level and category.

Classification Level of sensitivity of the data. Includes the level and category

Mode Given a community of users (with specified clearances) and data (with specified classifications) what must the security mechanisms look like?



8/24/2007

Class 7

16

Clearances, Classification, and Modes

| Mode | Data | Users | Evaluated to: |
|------------------------------|----------------------------------|---|--|
| Dedicated | Same level & Category | Same Level & Category (all cleared) | C2 (for general system integrity requirements) |
| System High | Same level & Category | Same Level & Different Categories (all cleared) | C2 (to support DAC policy) |
| Partitioned or Compartmented | Same Level, Different Categories | Same Level, Different Categories | B1 |
| Multilevel | Different Levels | Different Levels | B2 and above |

8/24/2007

Class 7

17

This Policy can be expressed mathematically

- A type of set theory fits this well
- A mathematical object called a "Lattice"
- Partial ordering (better than, not better than, can't compare)
- Dominates relationship
- Requires high and low point
- Why bother?
 - Can manipulate very complex classification schemes
 - Can make mathematically provable statements about whether certain properties are true or not

8/24/2007

Class 7

18

The "Dominates" Relationship

- How a lattice is ordered
- Mathematically precise way to describe relationships between user's clearance level and data's classification level
- Label "a" dominates label "b" when "b" is not more important than "a"
- Dominates may be taken to mean:
 - The security level of "a" is greater than or equal to the security level of "b"
 - The security categories of "a" are a superset of the security categories of "b"
- Examples:
 - {top secret, NATO} dominates {top secret}
 - {secret, NATO, Crypto} dominates {unclassified, NATO}
 - {unclassified, Nuclear} dominates {unclassified, Nuclear}

8/24/2007

Class 7

19

TCSEC (sometimes called "Orange Book" criteria)

- Evaluation process is NSA's Trusted Product Evaluation Program (TPEP)
 - TTAP - Newer program, run by NIST not NSA, for B1 & below
- Designed for evaluation of stand-alone systems
- Defines degree of trust - not (in the strictest sense) security
- Does not guarantee security in itself - requires proper configuration and administration of system components
- Fixed set of evaluation categories which combine
 - Functionality (security features)
 - Assurance (proof features are trustworthy)
- **Entire process is being phased out in favor of one based on the international Common Criteria**

8/24/2007

Class 7

20

The Trusted Computing Base (TCB)

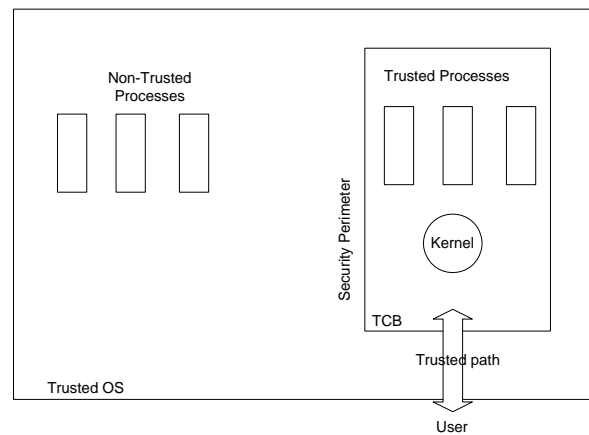
- The scope of a security evaluation – what parts of an operating system’s code must be reviewed
- A TCSEC concept. Common Criteria equivalent is the Security Target
- Definition
 - Part of the system in which one has confidence in expected operation
 - Security kernel may be a part of a TCB
 - Part of the system which supports security and isolates objects which perform protection
 - TCB must be protected from tampering
- Related Concepts:
 - Gateway - a system which manages exchanges across the Security Perimeter
 - Trusted Path - authenticates TCB to the user. Helps prevent password grabbing.
- Smaller is better – easier to prove correct, secure operation

8/24/2007

Class 7

21

The Trusted Computing Base (TCB)



8/24/2007

Class 7

22

TCSEC Certification Levels

| | | | |
|--|----|-----------------------------------|--------------------------|
| ↑ Increasing Assurance (trust) ↓ | D | Uncertified - Minimal Security | ↑ DAC ↓ ↑ MAC ↓ |
| | C | Discretionary Access Control | |
| | C1 | Discretionary Security Protection | |
| | C2 | Controlled Access Protection | |
| | B | Labeled, Mandatory Access Control | |
| | B1 | Labeled Security Protection | |
| | B2 | Structured Protection | |
| | B3 | Security Domains | |
| | A | Verified Design | |
| | A1 | Verified Design | |

8/24/2007

Class 7

23

ITSEC

- ITSEC:
 - Developed by the UK. Later adopted by the European Community
 - Separate assurance and functionality classes (some functionality classes map to TCSEC). Emphasizes effectiveness and correctness as separate criteria.
 - Some functionality classes are designed to map to TCSEC ratings (e.g., F-C2 is TCSEC C2, etc.)
 - Evaluation performed by commercial teams
 - ITSEC is a shorter evaluation process than TCSEC, and evaluates products in something closer to their actual running environment

8/24/2007

Class 7

24

Common Criteria

- **Common Criteria:**
 - Multinational effort to combine best aspects of TCSEC and ITSEC
 - Version 1.0 released January 1996, current version is V2.1
 - Uses both profiles and assurance classes, with the inclusion of Protection Profiles (PP) and Security Target.
- Common Criteria is superceding TCSEC (Orange Book) for US Federal Government security standards
- GASSP explicitly makes reference to Common Criteria
- Common Criteria is an ISO standard

8/24/2007

Class 7

25

Common Criteria Evaluation Concepts

- **Protection Profile (PP):** Set of security requirements for a type of product meeting a customer need. May be defined by user communities, product developers or other interested parties (e.g., agencies regulating a given industry). A proposed PP must undergo evaluation to ensure it is complete, consistent, and technically sound.
- **Security Target (ST):** Requirements and specifications used for evaluation of a specific product. An ST must meet the requirements of the relevant PP.
- **Target of Evaluation (TOE):** Specific product being evaluated
- **Evaluation Assistance Level (EAL):** Degree of assurance (in meeting PP).

8/24/2007

Class 7

26

Common Criteria

- NIST-developed Protection Profiles:
 - CS1 - based on Orange Book C2
 - CS2 - stronger general purpose commercially-oriented PP
 - RBAC - role-based, with privileges based on job functions. Designed to implement separation of duties
 - Traffic Filter Firewall
 - Application Level Firewall

8/24/2007

Class 7

27

Extra Material – Microsoft Baseline Security Analyzer

- A Microsoft utility that does a basic security “compliance audit”, checking
 - Security patches and hotfixes are current
 - Other configuration values meet baseline Microsoft standards
 - Detects “common security misconfigurations”
- Download from: <http://www.microsoft.com/technet/security/tools/mbsahome.msp>
- Before downloading, your browser (I assume IE here) will perform some validation
- Walk through the downloaded installer, selecting all the defaults

8/24/2007

Class 7

28

Extra Material – Microsoft Baseline Security Analyzer



After installation, you will have a Microsoft Baseline Security Analyzer icon on you desktop. Click it to start the application.

8/24/2007

Class 7

29

Extra Material – Microsoft Baseline Security Analyzer



Select the defaults – scan “this computer” and leave all boxes checked.

8/24/2007

Class 7

30

