Introduction to the CISSP Exam

ISC²™

International Information Systems Security Certification Consortium, Inc.

- **Non-profit/tax-exempt**
- **Sole purposes - certification and education**
- **Board of Directors with Executive Committee**

CISSP Applicant Requirements

- **Subscribe to the (ISC)^2 Code of Ethics**
- **Three years of work experience in one or more of the ten test domains:**
  - **Security Management Practices**
  - **Law, Investigation & Ethics**
  - **Physical Security**
  - **Operations Security**
  - **Business Continuity & Disaster Recovery Planning**
  - **Security Architecture & Models**
  - **Access Control Systems & Methodology**
  - **Cryptography**
  - **Telecommunications & Network Security**
  - **Application & Systems Development**

CISSP Examination

- **Format**
  - **250 multiple choice questions**
  - **Up to 6 hours to complete**
- **Scheduling**
  - **Major Information Security Conferences**
  - **CBK Review Seminar Locations**

Self Study - Study Guide

- **Contents**
  - **Description of ten test domains**
  - **List of reference documents**
- **Availability**
  - **Free from web page**
  - **Sample questions from web page**

Overview - Seminar

- One-day “Intro to the CISSP Exam & CBK”
- Eight-day “CBK Review Seminar”
  - Public Sessions announced on Web Page
  - In-house sessions are available

Additional Information

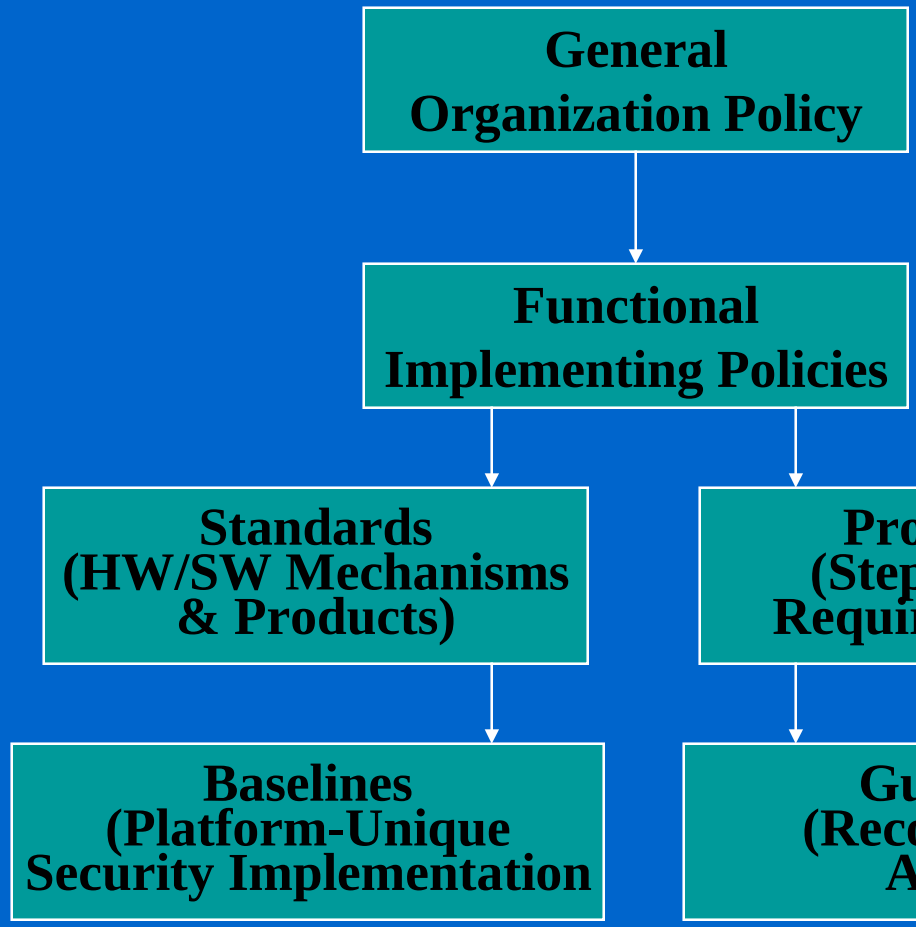
- **Address:**
  - **(ISC)² Inc., 860 Worcester Rd., Suite 101, Framingham, MA 01702**
- **Phone/Fax: Phone: (508) 875-8400, Fax: (508) 875-8450**
- **E-mail: info@isc2.org or isc2office@compuserve.com**
- **Web page: www ISC2.Org**

SECURITY MANAGEMENT PRACTICES

ISC²™

Policies, Standards, Guidelines & Procedures

Policy/Standards/Procedures Hierarchy



Writing Policy

- **Purpose**
- **Set objectives**
- **Fix responsibility**
- **Provide resources**
- **Allocate staff**
- **Implement using standards & guidelines**

British Standard 7799

- Comprehensive guidance on range of controls for implementing information security
- Divided into 10 sections

Information Classification/ Categorization

ISC²™

Classified Data/Information

- **Government information requiring protection against unauthorized disclosure**
- **TOP SECRET/SECRET/CONFIDENTIAL**

Sensitive Data/Information

- Information in military critical technologies list
  - New/high technology
  - Key indicators of operational capabilities
  - Sensitive but unclassified (SUI) designation
- Designated by knowledgeable authority
  - Damage caused if disclosed, altered, lost, or destroyed

Sensitive Business Data

- For official use only–investigative activity
- Financial–integrity of fiscal assets
- Sensitive management–defend against loss or disruption
- Proprietary–competitive edge
- Privileged–conformance with business standards/law
- Private–records about individuals

Classification Objectives

- General
  - Minimize information risks
    - Destruction/modification/disclosure
- Government
  - Avoid unauthorized disclosure
  - Comply with privacy law
- Commercial
  - Maintain competitive edge
  - Protect legal tactics
  - Comply with privacy law

Organization Architecture

ISC²™

Organization forms

- Centralized
- Decentralized
- Placement of IS/IT security function
  - Where significant power & authority exists
    - CIO, Administrative VP, Information Resources VP
    - Necessary to get job done

Roles and Responsibilities

- For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.
- Since every organization will have its own unique needs, it is not possible to provide a generic approach.
- Organizations must assign security related functions in the appropriate manner to nominated employees.

Responsibilities to consider include:

Executive Management - assigned overall responsibility for the security of information;

Information Systems Security Professionals - responsible for the design, implementation, management, and review of the organization's security policy, standards, measures, practices, and procedures;

Roles and Responsibilities Cont.

- ***Data Owners*** - responsible for determining sensitivity or classification levels of the data as well as maintaining accuracy and integrity of the data resident on the information system;
- ***Process Owners*** - responsible for ensuring that appropriate security, consistent with the organization's security policy, is embedded in their information systems;
- ***Technology providers*** - responsible for assisting with the implementation of information security;
- ***Users*** - responsible for following the procedures set out in the organization's security policy; and
- ***Information Systems Auditors*** - responsible for providing independent assurance to management on the appropriateness of the security objectives, and on whether the security policy, standards, measures, practices, and procedures are appropriate and comply with the organization's security objectives.

Information Security Responsibilities

- **Establish & maintain security program**
  - **Develop/implement policies, procedures & guidelines**
  - **Maintain resource access controls**
  - **Provide guidance on distributed processing & telecommunications security issues**
  - **Conduct security awareness training**
  - **Provide risk analysis services**
  - **Investigate incidents**
- **Provide EDP audit coordination**

Security Management Activities

- Evaluate success of security control activities
- Identify new opportunities/risks
  - Research protection mechanisms
- Recommend control measures
- Interpret security requirements from external sources
- Coordinate security activities

Activities (Cont.)

- Liaison with other functions
- Prepare plans, proposals, schedules, budgets
  - Budget 2%-3% of IS budget
- Represent organization on INFOSEC matters
- Provide administrative support
- Consult on security controls

Information Security Awareness Training Program

ISC²™

Objectives

- Indoctrinate system users & support personnel
- Specify security requirements
  - Mode of operation
  - Access requirements
  - Information handling
  - Reporting procedures
  - Unauthorized actions
  - Periodic reindoctrination
- Effectively relay INFOSEC requirements
- Motivate personnel to comply with requirements

Training Media

- Lectures/presentations
- Movies/videos
- Posters
- Newsletters/bulletins
- Awards
- Electronic notices (i.e., banners, message of day, last access)
- Stickers/coasters/notepads/etc.
- Web page
- Penetration testing activities

Training Topics

- Policies, procedures, standards
- Errors, accidents & omissions
- Physical & environmental hazards
- Penetration test results
- Information warfare
- Malicious code/logic
- Intrusions
- Theft

Risk Analysis

Risk Analysis Purposes

- **Quantify impact of potential threats**
- **Economic balance: impact & countermeasure cost**
- **Identify risks**

Definitions

- **Threat**
- **Exposure**
- **Vulnerability**
- **Countermeasures**
- **Risk**

Quantitative Risk Analysis

- **Definition**
  - **Attempts to assign independently objective numeric values (e.g., monetary values) to the components of the risk assessment & to the assessment of potential losses**
  - **When all elements (asset value, impact, threat frequency, safeguard effectiveness, safeguard costs, uncertainty & probability) are quantified, the process is considered to be fully quantitative**
  - **Purely quantitative risk analysis not possible because quantitative measures must be applied to qualitative elements**

Automated Risk Analysis

- **Objective minimize manual effort**
  - **After database created**
  - **Rerun analysis with different parameters (what ifs?)**
  - **Perform calculations quickly**
    - **Estimate future expected losses**
    - **Determine benefit of security measures**

Risk Analysis Steps

- **Estimate potential losses (Step 1)**
  - **Physical destruction/theft of assets**
  - **Loss of data**
  - **Theft of information**
  - **Indirect theft of assets**
  - **Delayed processing**

Steps (Cont.)

- **Threat analysis (Step 2)**
  - **Probability of occurrence**
    - **Sources of help**
- **Annual loss expectancy (Step 3)**
  - **Combine potential loss & probability**
  - **Magnitude of risk = ALE**
  - **Guide**
    - **Security measures**
    - **Amount to spend**

Remedial Measures Selection

- Alter environment
- Erect barriers
- Improve procedures
- Early detection
- Contingency plans
- Risk assignment
  - Insurance
- Risk acceptance

Qualitative Risk Analysis

- **Definition**
  - **Does not attempt to assign numeric values to components**
  - **Scenario oriented**
  - **Purely qualitative risk analysis is possible**

Sample Questions

Sample Question

- **1. The preliminary steps to security planning include all of the following EXCEPT**

  - **a. establish objectives.**
  - **b. list planning assumptions.**
  - **c. establish a security audit function.**
  - **d. determine alternate courses of action**

Sample Question

- **2. Which of the following represents an ALE calculation?**

  - **a. Gross loss expectancy X loss frequency.**
  - **b. Asset value X loss expectancy.**
  - **c. Total cost of loss + actual replacement value.**
  - **d. Single loss expectancy X annualized rate of occurrence.**

Sample Question

- **3. Why would an information security policy require that communications test equipment be controlled?**

  - **a. The equipment is susceptible to damage**
  - **b. The equipment can be used to browse information passing on a network**
  - **c. The equipment must always be available for replacement if necessary**
  - **d. The equipment can be used to reconfigure the network multiplexers**

Sample Question

- **4. Step-by-step instructions used to satisfy control requirements is called a**
  - **a. policy**
  - **b. standard**
  - **c. guideline**
  - **d. procedure**

Sample Question

- **5. One purpose of a security awareness program is to modify**
  - **a. employee's attitudes and behaviors.**
  - **b. management's approach.**
  - **c. attitudes of employees with sensitive data.**
  - **d. corporate attitudes about safeguarding data.**

Sample Question

- **6. Which one of the following individuals has PRIMARY responsibility for determining the classification level of information?**
  - **a. Security manager**
  - **b. User**
  - **c. Owner**
  - **d. Auditor**

LAW, INVESTIGATION, AND ETHICS

ISC²™

Law & Crime

Major categories of laws

- **Criminal law**
  - **Individual conduct which violates state or federal laws which are enacted for the protection of the public**

Major Categories of Laws (Cont.)

- **Civil law (tort)**
  - **Wrong against individual or business which results in damage or loss**
  - **No prison time**
  - **Financial restitution**

Intellectual Property Laws

- **Patent**
  - **Grants owner a legally enforceable right to exclude others from practicing the invention covered**
  - **Protects novel, useful and non-obvious inventions**
- **Trademark**
  - **Any word, name, symbol, color, sound, product shape or device or combination of these used to identify goods & distinguish them from those made or sold by others**

Intellectual Property Laws (Cont.)

- **Copyright**
  - **Covers the expression of ideas rather than the ideas themselves - "original works of authorship"**
- **Trade secret**
  - **Proprietary business or technical information which is confidential and protected as long as owner takes certain security actions**

Information Security-related Legal Issues

- **Computer crime laws**
  - **Computer-related crimes and abuses**
  - **Viruses and malicious code**
  - **Software piracy ("software police")**
  - **Internet crossing jurisdiction problems**
  - **Illegal content issues (child pornography)**

Information Security-related Legal Issues (cont.)

- **Other criminal laws (often used by prosecutors more than computer crime laws)**
  - **Wire fraud and mail fraud often used in computer crime cases**
  - **Various economic or financial crime laws, e.g., Embezzlement**

Privacy Laws

- **Privacy laws (European Union principles)**
  - **Data collected fairly and lawfully**
  - **Data only used for the purposes for which collected and only for reasonable time**
  - **Persons entitled to receive a report, on request, on data about them**

Privacy Laws (Cont.)

- Accurate and, where necessary, kept up to date
- One's personal data cannot be disclosed to 3rd parties unless authorized by statute or consent of individual
- Persons have a right to make corrections to their personal data
- Transmission to locations where "equivalent" personal data protection cannot be assured is prohibited

Sources of Liability

- Violations of law
  - Audit reports
- Violations of due care
  - Stockholder suits
- Violations of privacy
  - Employee suits

Elements of Negligence

- **Legally recognized obligation**
  - **Perform to a standard of conduct**
    - **Protect others from unreasonable risks**
- **Failure to conform to required standard**
- **Proximate causation**
- **Resulting injury is actual loss or damage to another**

Management Liability

- Failure to implement recommended precautions = mismanagement
  - Stockholders derivative suit = negligence
- No contingency/disaster recovery plan = negligence
- Failure to use anti-virus detection tools = negligence
- Negligent hiring
  - Failure to conduct background investigation

Investigation

ISC²™

Conducting Investigations

- Logical sequence of events
  - Investigate report
  - Review security/audit policies & procedures
  - Determine crime committed
  - Inform senior management
  - Determine crime status
    - When started/source/operation
    - Level of security needed
  - Identify company elements involved
  - Determine need for law enforcement
  - Protect chain of evidence

Conducting Investigations (cont.)

- Sources of evidence
  - Oral (witnesses)
    - Avoid threats
    - Written statement
  - Written (original documents)
  - Computer generated
  - Visual/audio
    - During event
    - After event

Hearsay Rule

- **Hearsay is 2nd-hand evidence**
  - **Value depends on veracity & competence of source**
  - **All business records considered hearsay**
    - **No first-hand proof of accuracy, reliability, trustworthiness**

Witness Requirements

- Have regular custody of records
- Rely on those records in regular course of business
- Know records prepared in regular course of business
  - Audit trails, if reviewed

Important Investigatory Issues

- **Admissibility of computer evidence**
  - **Admissibility of evidence**
    - **Relevant**
    - **Foundation of admissibility**
    - **Legally permissible**
    - **Evidence identification**
    - **Preservation of evidence**

Enticement vs. Entrapment

- **Enticement**
  - **Intruder lured to selected files**
    - **Cuckoo's Egg**
    - **Presence of downloaded files evidence**
- **Entrapment**
  - **Law enforcement induces a crime by a person who was not previously contemplating the crime**

ETHICS

ISC²™

Basis of and Origin of Computer Ethics

- Common good/interest
- National interest
- Religion
- Individual rights
- Enlightened self interest
- Law
- Professional ethics/practices
- Standards of good practice
- Tradition/culture

Internet Activities Board (IAB) Ethics Viewpoint

- **Ethics & the Internet (RFC No. 1087)**
  - **Access to & use of Internet is a privilege & should be treated as such by all users**

IAB Ethics Viewpoint (cont.)

- **Any activity is unethical & unacceptable that purposely:**
  - **Seeks to gain unauthorized access to Internet resources**
  - **Disrupts the intended use of the Internet**
  - **Wastes resources (people, capacity, computer) through such actions**
  - **Destroys the integrity of computer-based information**
  - **Compromises the privacy of users**
  - **Involves negligence in the conduct of Internet-wide experiments**

SAMPLE QUESTIONS

ISC²™

Sample Question

- **1. Under the principle of culpable negligence, executives can be held liable for losses that result from computer system breeches if**
  - **a. the company is not a multi-national company.**
  - **b. they have not exercised due care protecting computing resources.**
  - **c. they have failed to properly insure computer resources against loss.**
  - **d. the company does not prosecute the hacker that caused the breech.**

Sample Question

- **2. Since disks and other magnetic media are only copies of the actual or original evidence, what type of evidence are they are often considered to represent?**

  - **a. Hearsay**
  - **b. Irrelevant**
  - **c. Incomplete**
  - **d. Secondary**

Sample Question

- 3. The deliberate planting of apparent flaws in a system for the purpose of detecting attempted penetrations or confusing an intruder about which flaws to exploit is called

  - a. alteration.
  - b. investigation.
  - c. re-direction.
  - d. enticement.

Sample Question

- **4. Which element must computer evidence have to be admissible in court?**

  - **a. It must be relevant.**
  - **b. It must be annotated.**
  - **c. It must be printed.**
  - **d. It must contain source code.**

Sample Question

- **5. The Internet Activities Board characterizes which of the following as unethical behavior for Internet users?**
  - **a. Writing computer viruses.**
  - **b. Monitoring data traffic.**
  - **c. Wasting computer resources.**
  - **d. Concealing unauthorized accesses.**

PHYSICAL SECURITY

ISC²™

Facility Planning

- "Low visibility"
  - Visually
  - Markings
- Location considerations
  - Adjacent hazards
  - Local crime
  - Natural disasters

Facility Planning (Cont.)

- **Other hazards**
  - **Strikes/job actions**
  - **Air traffic**
  - **Roadways**
  - **Joint tenants**
- **External assistance**
  - **Police**
  - **Fire**
  - **Medical**

General Facility Construction

- Local building construction standards
- IS/IT facility construction standards
  - Floors/walls/ceilings
  - Windows/doors - Main/secondary entrances
- HVACR
- Other

Electrical Power

- Primary power source
  - Dedicated feeder(s) from one or more utility sub-stations or power grids
  - Circuits and distribution panels
  - Transformers/feeder cables
  - Master circuit breakers
  - Voltage monitor/recorder
- Alternate power source
  - Alternate feeder(s)
  - "UPS" (uninterruptible power supply) to provide "clean" power during outage
    - Standby generator, batteries

Electrical Power (cont.)

- **Objective: Clean Power - no voltage fluctuations or interference**
  - **Voltage fluctuations**
    - **Power Loss**
      - **Fault - momentary power out**
      - **Blackout - prolonged loss of power**
    - **Power degradation**
      - **Sag - momentary low voltage**
      - **Brownout - prolonged below normal voltage - which can be planned during overload at the utility company**
    - **Power excess**
      - **Spike - momentary high voltage**
      - **Surge - prolonged high voltage**

Electric Power (cont.)

- **Interference**
  - **Noise - random disturbance interfering with devices**
    - **Electromagnetic interference (EMI)**
      - **Created by difference between 3 wires (hot, neutral, ground)**
      - **Caused by motors, lightning, etc.**
    - **Radio frequency interference (RFI)**
      - **Created by components of electrical system**
      - **Caused by electric cables, fluorescent lighting, truck ignition**
  - **Transient noise - disturbance imposed on power line**

Fire Suppression

- **Fire Classes**
  - **A - Common combustibles**
    - **Suppress with water/soda acid**
  - **B - Liquid**
    - **Suppress with CO_2/soda acid/Halon**
  - **C - Electrical**
    - **Suppress with CO_2/Halon**

Fire Suppression (cont.)

- Combustion elements
  - Fuel
  - Oxygen
  - Temperature
- Suppression methods versus combustion elements
  - Remove fuel/oxygen (CO_2/soda acid)
  - Reduce temperature (water)
  - Interference with chemical reaction (Halon)

Fire Suppression Systems (cont.)

- **Portable extinguishers - to minimize fire damage**
  - **Filled with approved/applicable suppression agent**
  - **Located within 50 feet of any electrical equipment**
  - **At exits**
- **Other considerations**
  - **Clearly mark, with unobstructed view**
  - **Easily reached and operated by average-sized personnel**
  - **Inspected quarterly**

Fire Suppression (cont.)

- **Other considerations concerning fire suppression agents:**
  - **Water - The Fire Protection and Insurance Industries support the use of water as the primary fire extinguishing agent for all business environments, including those dependent on Information Systems!**
  - **CO2 - colorless, odorless, and potentially lethal in that it removes oxygen**
    - **Gas masks give no protection**
    - **Best application is for unattended facilities**
    - **Use built-in delay in manned areas**

Fire Suppression (cont.)

- **Other considerations (cont.):**
  - **Halon (Halongenated extinguishing agent)**
    - **Must be thoroughly mixed with air**
    - **Fastest practical flooding desired**
    - **Montreal protocol (1987) - stopped Halon production as of 01/01/94 due to agent releasing ozone-depleting substances**
    - **Halon 1301 requires expensive pressurized flooding system**
    - **Halon 1211 self-pressurizes (used in portable extinguishers)**
  - **FM-200 - most effective alternative - requires 7% concentration (Halon requires 5%)**

External Boundary Protection

- Fencing & other physical barriers
- Outside lighting
- Intrusion detection
- CCTV
- Patrol Force

External Boundary Protection (cont.)

- Fencing and other physical barriers
  - Varying heights provide varying levels of protection
    - 3 - 4 ft/1meter (deters casual trespasser)
    - 6 - 7 ft /2meters (too high to climb easily)
    - 8 ft/2.4meters + 3 strands of barbed wire (deter determined intruder)
  - Considerations:
    - Provides crowd control
    - Helps control access to entrances
    - Can be costly
    - May be unacceptably unsightly

External Boundary Protection (cont.)

- Outside lighting examples
  - Floodlights
  - Streetlights
  - Fresnel units
  - Searchlights
- Considerations
  - Security over physical spaces and buildings
  - Safety of personnel
  - Lighting should be used to discourage prowlers & intruders
    - Building critical areas, entrances & parking areas

External Boundary Protection (cont.)

- Intrusion detection/monitoring
  - Optical/light beams
  - Vibration sensors
  - Closed circuit TV
  - Motion detection
    - Infrared
    - Microwave
- Considerations
  - Expensive to install and monitor
  - Requires human response
  - Practical if fence not possible
  - Subject to nuisance alarms
  - Can be penetrated

External Boundary Protection (cont.)

- Closed Circuit television (CCTV) systems
  - Permits one person to monitor large area
  - Should be coupled with alerting function
  - Provision for human response
- Patrol force
  - Can provide flexible security & safety response
  - Good deterrence
  - May be effective for protecting group of buildings
  - Costly
  - Employee vis a vis contractor decision

Personnel Access Controls

- Access control system categories
  - Electric/mechanical latch
  - Universal code/card
  - Group coding
  - Personal identification systems
- Facility
  - Turnstiles
  - Man traps
  - Guards
- Identification
  - Photo ids
  - Magnetic id cards
  - Biometric devices
  - CCTV

Personnel Access Controls (Cont.)

- **Card badge readers**
  - **Magnetic stripe**
  - **Magnetic dot**
  - **Embedded wire**
  - **Proximity**

Personnel Access Controls (Cont.)

- Access control reliability features
  - Tamper alarms
  - Power-fail protection
  - Fail-safe or fail-soft
  - Mechanical-key bypass
  - Default to open or closed
  - Code changes
  - Logging
- Monitoring devices
  - CCTV
  - Motion sensors
  - Guards

Biometric Identification

- Fingerprint
- Palm scan
- Hand geometry
- Voice print
- Retina pattern
- Iris scan
- Facial recognition
- Keystroke dynamics
- Signature dynamics

Biometric Device Considerations

- Resistance to counterfeiting
- Data storage requirements
- Acceptability to users - subject/system contact requirements may be intrusive
  - Enrollment time of 2 minutes per person is standard
  - Average implementation speed & throughput rate is 6-10 seconds
- Reliability & accuracy
  - Three unique biometric characteristics are fingerprint, retina & iris
  - Crossover error rate must be appropriate to the application

Biometric Accuracy Characteristics

- **False reject rate (Type I error)**
  - **Percent of authentic persons rejected as unidentified/unverified**
  - **Also, failure to acquire (sensor not presented with sufficient usable data to make decision)**
- **False accept rate (Type II error)**
  - **Percent of unenrolled/impostors accepted as authentic**
- **Crossover error rate (CER)**
  - **Percent at which false rejection & false acceptance are equal**

Biometric System Performance

System Type	*Response Time*	*Accuracy(CER)*
Palm Scan	**2 - 3 seconds**	**0%**
Hand geometry	**3 - 5 seconds**	**0.1%**
Iris Scan	**2 - 4 seconds**	**0.5%**
Retina Scan	**4 - 7 seconds**	**1.5%**
Fingerprint	**5 -7 seconds**	**5%**
Voice pattern	**10 - 14 seconds**	**8%**
Facial Recognition	**2 seconds**	**TBD**
Signature dynamics	**5 - 10 seconds**	

Personnel Access Controls (cont.)

- **Procedures**
  - **Employee**
  - **Contractor**
  - **Visitor (logs/temp id)**
  - **Service/delivery/maintenance**
  - **Cleaning**
  - **Escorts**

Distributed Processing Impact On Physical Security

- Computers cheaper/smaller/more accessible
  - Located on every desk
  - Connected by networks
  - Difficult to apply physical security measures
    - Other security types more important
- User responsibility increased
  - Laptops
    - File encryption

Sample Questions

ISC²™

Sample Question

- **1. What is a common problem when using vibration detection devices for perimeter control?**
  - **a. They are vulnerable to non-adversarial disturbances.**
  - **b. They can be defeated by electronic means.**
  - **c. Signal amplitude is affected by weather conditions.**
  - **d. They must be buried below the frost line.**

Sample Question

- **2. What physical characteristics does a retinal scan biometric device measure?**
  - **a. The amount of light reaching the retina.**
  - **b. The amount of light reflected by the retina.**
  - **c. The size, curvature, and shape of the retina.**
  - **d. The pattern of blood vessels at the back of the eye.**

Sample Question

- **3. Which of the following measures would be the BEST deterrent to the theft of corporate information from a laptop which was left in a hotel room?**
  - **a. Store all data on disks and lock them in an in-room safe.**
  - **b. Remove the batteries and power supply from the laptop and store them separately from the computer.**
  - **c. Install a cable lock on the laptop when it is unattended.**
  - **d. Encrypt the data on the hard drive.**

Sample Question

- **4. Under what conditions would use of a "Class C" hand-held fire extinguisher be preferable to use of a "Class A" hand-held fire extinguisher?**
  - **a. When the fire is in its incipient stage.**
  - **b. When the fire involves electrical equipment.**
  - **c. When the fire is located in an enclosed area.**
  - **d. When the fire is caused by flammable products.**

Sample Question

- **5. To be in compliance with the Montreal Protocol, which of the following options can be taken to refill a Halon flooding system in the event that Halon is fully discharged in the computer room?**
  - **a. Order an immediate refill with Halon 1201 from the manufacturer.**
  - **b. Contact a Halon recycling bank to make arrangements for a refill.**
  - **c. Order a different chlorofluorocarbon compound from the manufacturer.**
  - **d. Order an immediate refill with Halon 1301 from the manufacturer.**

OPERATIONS SECURITY

Operational Security Issue

- **Described in risk analysis**
  - **Threat**
  - **Vulnerability**
  - **Asset**

Definitions

- **Operations security**
  - **Controls over HW, media, & operators with access**
  - **Protects against asset threats**
  - **Baseline or selective mechanisms**
- **Operator**
  - **Supports system operation from operator's console**
    - **Monitors execution of system**
    - **Controls flow of jobs**
    - **Mounts I/O volumes**

Network Administrator Privileges

- **Server startup & shutdown**
  - **File system(s)**
  - **Data base(s)**
  - **Application(s)**
- **Reset**
  - **Time/date**
  - **Operating system log(s)**

Violation Analysis

- Types of violations
  - Repetitive mistakes
  - Individuals exceeding their authority
  - Too many people with unrestricted access
- Where occurring
- Patterns indicating serious intrusion attempts
  - Hackers/disgruntled employees
- Profile based anomaly detection
- Clipping level
  - Establishes baseline violation count to ignore normal user errors

Operator Privileges

- Initial program load
  - Program starts OS controlled from console
    - Operator could load wrong program
- Bypass label processing
- Rename/re-label resources
- Reset
  - Time/date
  - Passwords
- Reassign ports/lines

Potential Abuses

- **Fraud**
  - **Rejected transactions example**
    - **Erroneous transaction entered & rejected**
    - **Perpetrator handles rejects**
    - **Replaces with apparently valid transaction but "pay to" account changed**
- **Interference with operation**
  - **Denial of service**
  - **Production delays**

Potential Abuses (Cont.)

- **Conversion to personal use**
  - **Computing time**
  - **Vendor software**
- **Unauthorized access/disclosure**
  - **Off-hours**
- **Audit trail/system log corruption**

Types of Controls

- Physical access
- Separation of responsibility
  - Force collusion with person in different category
  - Input/output controls
- Instruction/training
- Supervision
- Hardware/area locks
- System/audit logs
- Other (compensating)

Hardware/Software Asset Management

- Hardware
  - Configuration
  - Inventory
  - Fault tolerance
    - Protect against design reliability threats
- Software inventory
  - Operating
  - Backups
    - Operational
    - Off-site
    - Generations

Problem Management

- **Control process**
  - **Reports,tracks, resolves problems affecting services**
    - **Objectives**
    - **Types of problems**
- **System update requires corresponding problem management entry for authorization**

Change Control Management

- Authorizes changes to production systems
  - New applications
  - Modify existing applications
  - Remove old applications
- Uses input from problem management to initiate changes
- Security function can block a change
  - Adversely affects security of applications/data
- Should be extended to include network hardware & servers

Secure System Operation

- **Separation of duties**
  - **System administrator/operator functions**
    - **Installing system software**
    - **Starting up & shutting down system**
    - **Adding & removing users**
    - **Performing backup & recovery**
    - **Mounting disks & tapes**
    - **Handling printers**

Separation of Duties (Cont.)

- Security administrator functions
  - User-oriented activities
    - Setting user clearances
    - Setting initial password
    - Setting other security characteristics for new users
    - Changing security profiles for existing users
  - Setting/changing file sensitivity labels
  - Setting security characteristics of devices & communications channels
  - Reviewing audit data

Separation of Duties (Cont.)

- **Network administrator function**
  - **All system administrator/operator tasks**
  - **All security administrator tasks**
  - **Combination of functions creates greater security risks**
    - **Compromise: trust but verify**

Rotation of Duties

- **Interrupt opportunity to create collusion to subvert operation for fraudulent purposes**
  - **Implementation difficult in organizations with small staffs & inadequate training programs**
- **Provides opportunity to re-justify/reassign privileges**

Trusted Facility Management

- System must support separate operator & administrator roles (B2)
- System must clearly identify functions of security administrator to perform security-related functions (B3 & A1)

Trusted Recovery

- Ensure security not breached during system crash or if system failure occurs (B3 & A1)
- Activities
  - Preparing for system failure
  - Recovering system
- Control
  - Backup all system-critical files regularly
- System problems requiring recover or halt & reboot
  - Crash or power failure
  - Missing resource
  - Inconsistent database
  - System compromise

Trusted Recovery Procedures

- **Before allowing user access**
  - **Reboot system**
    - **Get running in single-user mode**
  - **Recover all file systems active at time of failure**
  - **Restore missing/damaged files & databases**
    - **From most recent backup**
  - **Check security-critical files**

SAMPLE QUESTIONS

ISC²™

Sample Question

- **1. Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?**
  - **a. Limiting the local access of operations personnel**
  - **b. Job rotation of operations personnel**
  - **c. Management monitoring of audit logs**
  - **d. Enforcing regular password changes**

Sample Question

- 2. An electrical device (AC or DC) which can generate coercive magnetic force for the purpose of reducing magnetic flux density to zero on storage media or other magnetic media is called

  - a. a magnetic field.
  - b. a degausser.
  - c. magnetic remanence.
  - d. magnetic saturation.

Sample Question

- **3. What is the most secure way to dispose of information on a CD-ROM?**
  - **a. Sanitizing**
  - **b. Physical damage**
  - **c. Degaussing**
  - **d. Physical destruction**

Sample Question

- **4. Fault tolerance countermeasures are designed to combat threats to**

  - **a. an uninterruptible power supply.**
  - **b. backup and retention capability.**
  - **c. design reliability.**
  - **d. data integrity.**

Sample Question

- **5. In what way can violation clipping levels assist in violation tracking and analysis?**
  - **a. Clipping levels set a baseline for normal user errors, and violations exceeding that threshold will be recorded for analysis of why the violations occurred.**
  - **b. Clipping levels enable a security administrator to customize the audit trail to record only those violations which are deemed to be security relevant.**
  - **c. Clipping levels enable the security administrator to customize the audit trail to record only actions for users with access to usercodes with a privileged status.**
  - **d. Clipping levels enable a security administrator to view all reductions in security levels which have been made to usercodes which have incurred violations.**

BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY PLANNING

ISC²™

Disaster Definition

- **A sudden, unplanned calamitous event that brings about great damage or loss. Any event that creates an inability on the organization's part to provide critical business functions for some predetermined period of time.**

(source: *Disaster Recovery Journal*, 7-9/90)

Recovery Planning Definition

- **The advance planning and preparations which are necessary to minimize loss and ensure continuity of the critical business functions of an organization.**

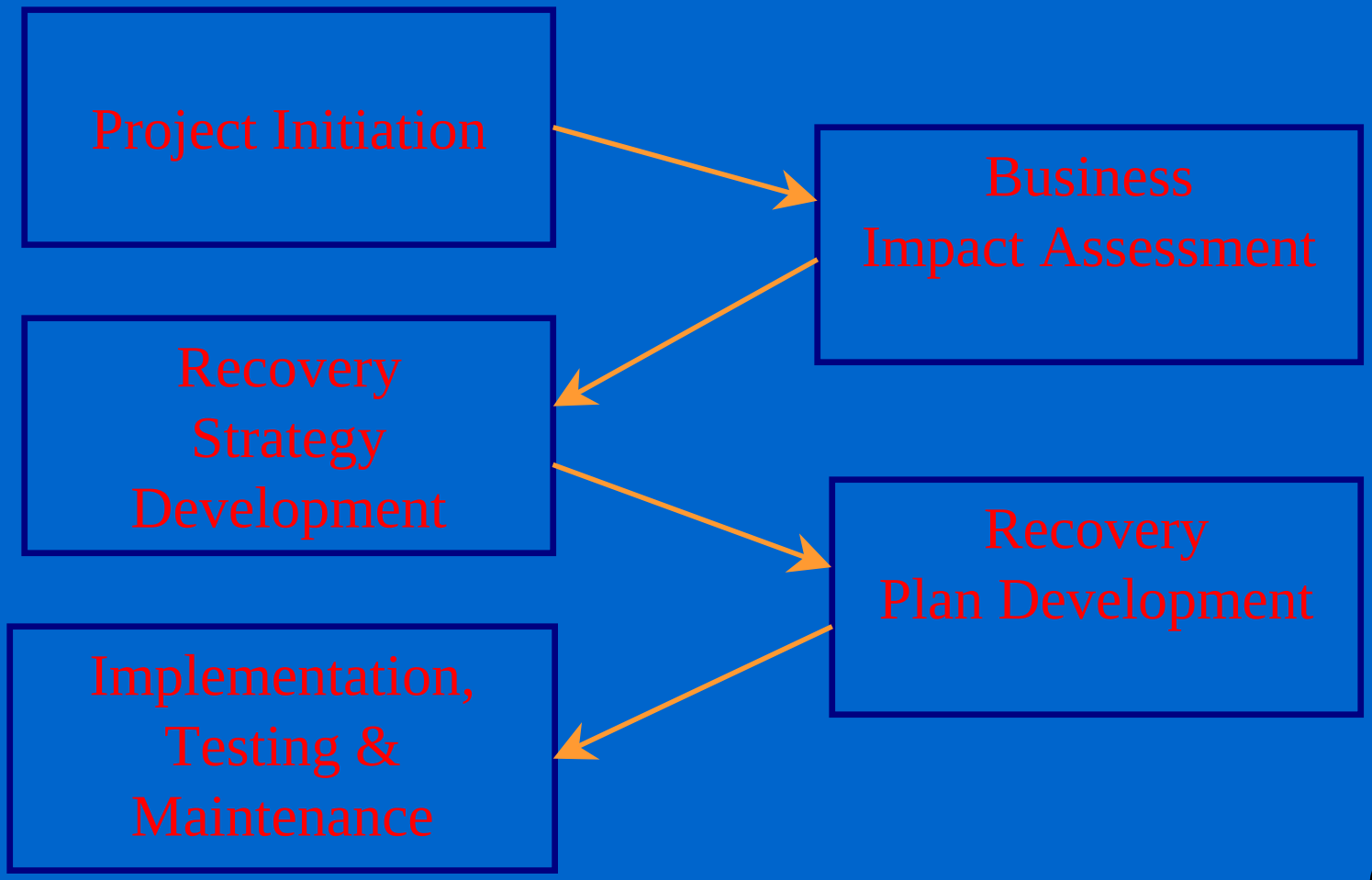
BCP vis-à-vis DRP

- **Business continuity planning**
  - **Ensures continuity of critical business functions**
  - **Facilitates rapid recovery measures to reduce overall impact of disaster**
- **Disaster recovery planning**
  - **Procedures for emergency response, extended backup operations & post-disaster recovery when computer installation suffers loss of computer resources & physical facilities**

DRP Objectives

- Protect organization if all or a part of its computer services become unusable
- Provide a sense of security
- Minimize risk of delays
- Guarantee reliability of standby systems
- Provide a standard for testing the plan
- Minimize decision-making during a disaster

Generic Recovery Planning Methodology



Vulnerability Assessment Goals

- Understand economic & operational impact of disruption
- Determine recovery time-frame for critical applications
  - Business functions
  - Network services
- Identify most appropriate recovery strategy
- Cost-justify recovery planning
- Bring contingency planning into normal business decision-making process

Vulnerability Assessment Process

- **Identify essential business functions**
- **Conduct loss impact analysis**
  - **Financial**
  - **Operational**
- **Summarize & recommend recovery priorities**

Identifying Essential Business Functions

- **Loss criteria**
  - **Direct dollar losses**
  - **Added operational expense**
  - **Poor business decisions**
  - **Violation of contract agreements**
  - **Violation of regulatory requirements**
  - **Loss of competitive advantage**
  - **Loss of public confidence**

Business Units (Cont.)

- Timeliness criteria
  - How quickly will losses mount?
  - Is criticality due to periodic (i.e., End of quarter) processing?
- Contingency plans may not be required if lengthy interruption acceptable
- Composite time-loss curves will show total impact

System Backup Alternatives

- Reciprocal/mutual aid agreements
- Subscription services
  - Hot site
  - Warm site
  - Cold site
- Multiple centers
- Service bureaus
- Other data center backup alternatives
  - Rolling hot sites
  - Prefabricated buildings
- Distributed systems backup options

Distributed Systems Backup Options

- In-house systems replacement
- Stockpiling critical components
- Hot site/hot replacement subscriptions
- Vendor replacement
- Combinations

Recovery Plan Components

- Safety
- Continuity of management & emergency powers
- Identification of critical functions
- Emergency response
- Recovery of critical functions
- Salvage & repair
- Restoration of normal operations

Regular Drills & Testing

- No demonstrated capability until plan tested
- Tests exercise all components of plans
- Tests & drills prepare personnel to carry out emergency duties
- Regular test schedule alerts management to changes affecting recovery capabilities

Plan Testing

- **Testing types**
  - **Structured walk-through**
  - **Checklist**
  - **Simulation**
  - **Parallel**
  - **Full-interruption**

Why Plans Get Out of Date

- Environmental changes
- Changes in hardware, software, other critical equipment
- Reorganizations
- Personnel lose interest or forget
- Personnel turnover
- Cumbersome plans not easily updated

Importance of Prevention

- Risk management program
- Physical security
- Information security
- Emergency response procedures & training
- Insurance coverage
- Mitigate the emergency - avoid activating DRP

Off-Site Storage Facility Checklist

- Physical layout
  - Trip from loading dock to private storage areas
    - Efficient, secure, timely?
- Fire resistant construction?
- Fire detection, suppression & alarm connections to the local fire department?
- Temperature & humidity monitoring & control?
- Security access control systems tied into local police dept?
- Backup power for security access, fire & environmental sys?

Off-Site Checklist (Cont.)

- Can records be accessed within your recovery time frame?
  - Any unacceptable delays due to weekends, holidays or location?
- Avoidance of special environmental hazards
  - Periodic flooding, earthquakes, severe power fluctuations, etc?
- Availability of bonded transport services?
- Storage for media other than tapes
  - Hard copy, supplies, diskettes, etc?

Data & Applications Backup Alternatives

- Electronic vaulting
  - Bulk transfer of backup data
- Remote journaling
  - Transmission of journal/transaction log data to off-site location
    - IMS, CICS, IDMS, CPCS, other DBMSes
- Database shadowing
  - Using remotely journaled data
    - Includes staging database restore & roll-forward process
- Standby services
  - Operating critical applications at the remote site

Sample Questions

Sample Question

- **1. For which areas of the enterprise are business continuity plans required?**
  - **a. All areas of the enterprise.**
  - **b. The financial and information processing areas of the enterprise.**
  - **c. The operating areas of the enterprise.**
  - **d. The marketing, finance, and information processing areas.**

Sample Question

- **2. Which of the following will a Business Impact Analysis NOT identify?**
  - **a. Areas that would suffer the greatest financial or operational loss in the event of a disaster.**
  - **b. Systems critical to the survival of the enterprise.**
  - **c. The names of individuals to be contacted during a disaster.**
  - **d. The outage time that can be tolerated by the enterprise as a result of a disaster.**

Sample Question

- **3. What is a hot-site facility?**
  - **a. A site with pre-installed computers, raised flooring, air conditioning, telecommunications and networking equipment, and UPS.**
  - **b. A site in which space is reserved with pre-installed wiring and raised floors.**
  - **c. A site with raised flooring, air conditioning, telecommunications, and networking equipment, and UPS.**
  - **d. A site with ready made work space with telecommunications equipment, LANs, PCs, and terminals for work groups.**

Sample Question

- **4. Which of the following best describes remote journaling?**
  - **a. Send hourly tapes containing transactions off-site.**
  - **b. Send daily tapes containing transactions off-site.**
  - **c. Real-time capture of transactions to multiple storage devices.**
  - **d. The electronic forwarding of transactions to an off-site facility.**

Sample Question

- **5. Emergency actions are taken at the incipient stage of a disaster with the objectives of preventing injuries or loss of life and of**
  - **a. determining the extent of property damage.**
  - **b. protecting evidence.**
  - **c. preventing looting and further damage.**
  - **d. mitigating the damage to avoid the need for recovery.**