# Information Systems Audit
# Module V

Mathew A Thomas
Grad. CWA, FCA, MCA, CDM, ISA, CISSP.

# Introduction

- ✓ About the Course
- ✓ About the Module
  - ► Module 5 (25%) 50 Questions
- ✓ About the Material
  - ► Source, Organisation
  - ► Module 5: Chapters 20-26

# About this Presentation

- ✓ Logical Access Controls
  - ► Chapter 20, 21 and 22 26,51
- ✓ Application Controls
  - ► Chapter 23 80
- ✓ Auditing Logical and Application Controls
  - ► Chapter 24 109
- ✓ Physical Access Controls
  - ► Chapter 25 133
- ✓ Environmental Controls
  - ► Chapter 26 156
- ✓ Miscellaneous
  - ► Processor Controls, Real and Virtual, Output Controls

# Information Security

- ISO 17799 Standard on Information Security Management:
  - Defines information security to mean the preservation of confidentiality, integrity and availability of information.
  - Confidentiality
    - Information should be accessible and disclosed only to those who are authorized to have access.
  - Integrity
    - Information should be protected from unauthorised modification.
  - Availability
    - Information should be available as and when required for authorized purposes.

# Primary Objectives

- ✓ Securing resident data
  - Significant volume of data resides in computing equipment and devices.
- ✓ Securing data in transit
  - Much of data is also in transit between computers or between networks, traveling on communication channels, which are susceptible to a wide range of risks.

# Paths of Logical Access

- ✓ Mainframe Terminals
  - ► Access to the mainframe central computer can be obtained through any of the dumb or intelligent terminals connected to the central computer.
- ✓ Console
  - ► One or some terminals connected to the mainframe are configured for privileged access capable of commanding and controlling the functions and operations of the central computer and attached devices.
- ✓ Networked Computer
  - ► Access to a computer or resources on the network can be enabled by simply connecting a computer to the network.

# Paths of Logical Access

- ✓ Client/Server
  - ► The information and processing tends to get distributed across locations and computing equipment on the network, thus raising the concerns of multiple points of access.
- ✓ Networked Devices
  - ► Access to resources on a computer or network can also be achieved through telecommunication devices which provide for access paths such as hubs, switches and routers, point of sale device, wireless equipment.
- ✓ Dial-Up Access
  - ► A computer located at a geographical disparate location can dial up a remote organisational server using public/private telecommunication lines eg. dial up access to an ISP for connecting to the internet.

# Technical Exposures

- Data Leakage
  - Sensitive information contained in computer files may be copied on to a disks or other media, electronically transferred across networks to other locations, transmitted across internet or simply viewed or printed.
- Wire Tapping
  - This is similar to tapping of telephone lines, networking cables or telecommunication lines are tapped by the perpetrator for eavesdropping.
- Scavenging or Dumpster Diving
  - The perpetrator gains access to apparently inconspicuous directories or areas such as recycle bins, temporary files, deleted files, redundant configuration settings.

# Technical Exposures

- Emanation Interception
  - Many of the devices used for computing radiate signals or waves, such as electromagnetic radiation emanated by dot matrix printers, which can be intercepted using simple devices.
- Data Diddling
  - Changing data before or as they are entered into the computer.
  - Common abuse because it requires limited technical knowledge
  - Occurs before computer security can protect data

# Technical Exposures

- Piggybacking
  - The perpetrator waits for the authorised user to log into the system and after the user has gained access to the system, the perpetrator follows or takes over control.
  - Act of following an authorized person through a secured door.
  - Electronically attaching to an authorized telecommunications link to intercept and possibly alter transmissions.
  - Involves intercepting communication between OS and user and modifying them or substituting new messages (RW532)

# Technical Exposures

- Masquerading
  - A perpetrator impersonates as a legitimate user.
  - Send a message to the Systems Administrator into claiming to have lost his password and ask for a new password.
  - Sends a message to all users requiring them disclosing some sensitive information.
- Spoofing
  - The perpetrator replaces the boundary system such as a login/password screen with his look-alike screen, induces the user to login and after the user enters the password, simulates a crash and returns control the original login screen.

# Technical Exposures

- Asynchronous Attacks
  - Occur in multiprocessing environments where data move asynchronously (one character at a time with a start and stop signal) across telecommunications lines. As a result, numerous data transmissions must wait for the line to be free (and flowing in the proper direction) before being transmitted.
  - Data that are waiting are susceptible to unauthorized accesses called asynchronous attacks.
  - These attacks, which are usually very small pinlike insertions into cable, may be committed via hardware and are extremely hard to detect.
- Buffer Overflow
  - Malicious program induces a buffer or stack overflow.
  - Attempt to access the processing routines, instruction or data to reveal sensitive data or sneak in malicious code.
- Trojans
  - Program that appears as authorized or normal but carries a destructive payload.

# Technical Exposures

- Rounding Down
  - Drawing off small amounts of money from a computerized transaction or account and rerouting this amount to the perpetrators account.
  - The term "rounding down" refers to rounding small fractions of a denomination down and transferring these small fractions into the unauthorized account.
  - Since the amounts are so small, they are rarely noticed.
- Salami Technique
  - Slicing of small amounts of money from a computerized transaction or account and is similar to the rounding down technique.
  - Salami technique truncates the last few digits.

# Technical Exposures

- Viruses
  - Malicious program code inserted into other executable code that can self-replicate.
  - Payload may be destructive or benign.
  - A virus may lie dormant for some time until triggered by a certain event or occurrence, such as a date or being copied a pre-specified number of times. (Cf. Bombs)
  - Viruses are not capable of self-actuating.
- Worms
  - Destructive programs that may destroy data or utilize tremendous computer and communication resources.
  - Can run independently and travel from machine to machine across network connections.
  - A worm have its components stationed in various places in a network.
  - Self-actuating and self-sustaining.

# Technical Exposures

- Logic Bombs
  - Similar to viruses, but they do not self-replicate.
  - Their destructive action is programmed to “blow up” on meeting a logical event.
  - Creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific time in the future.
  - Logic bombs are very difficult to detect before they blow up.
  - The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb.
- Trap Doors
  - Exits out of an authorized program that allow insertion of specific logic, such as program interrupts, to permit a review of data during processing.
  - These holes also permit insertion of unauthorized logic.

# Technical Exposures

- Remote Shut Down
  - Initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up lines) to the computer.
  - Only individuals knowing a high-level systems logon-ID can usually initiate the shut-down process.
- Denial of Service (DoS)
  - DoS is an attack that disrupts or completely denies or degrades service to legitimate users, networks, systems, or other resources.
  - The intent of any such attack is usually malicious in nature and often takes little skill because the requisite tools are readily available.
- Distributed Denial of Service (DDoS)
  - Victimize “innocent” computer (also called as zombies) to launch a multi-pronged attack, wherein computers of non-desirous users continuously request for service from a target computer system.
- Social Engineering
  - No technical know-how required.
  - The perpetrator uses social and tactical skills to obtain unauthorized information.

# Viruses

- It was earlier believed that viruses could not infect data files, but recently viruses have been written that infect data files too.  E.g. Macros viruses
- Components:
  - Vector
  - Replicator or Infector
  - Payload
  - Polymorphism Engine
- Controls Over Viruses
  - Policy and Procedure controls
  - Technical Methods
    - Anti-Virus Software

# Policy and Procedure controls

- ✓ Build/Boot from original, clean master copies.
- ✓ Update virus software scanning definitions frequently.
- ✓ Write-protect all diskettes with .EXE or .COM extensions.
- ✓ Have vendors run demonstrations on their machines, not yours.
- ✓ Scan shareware / commercial software disks before use.
- ✓ Field technicians scan their disks on a test machine before they use
- ✓ Network administrator should use workstation and server anti-virus software.
- ✓ Ensure that bridge, router and gateway updates are authentic.
- ✓ Backups are a vital element of anti-virus strategy. This plan should account for scanning selected backup files for virus infection once a virus has been detected.
- ✓ Educate users so they will heed these policies and procedures.
- ✓ Review anti-virus policies and procedures at least once a year.
- ✓ Prepare a virus eradication procedure and identify a contact person.

# Technical Methods

- ✓ Use workstations without floppy disks
- ✓ Use boot virus protection (i.e., firmware-based )
- ✓ Anti-Virus Software
  - Scanners
    - ► look for sequences of bits called signatures that are typical of virus programs.
  - Active Monitors (Heuristic Scanners)
    - ► interpret DOS and BIOS calls, looking for virus-like actions.
  - Integrity Checkers
    - ► compute a binary number on a known virus-free program that is then stored in a database file.
    - ► The checker computers the CRC on the program about to be executed and compares it to the number in the database.

# Computer Crime and its Impact

- Financial Loss
  - Direct, through loss of electronic funds or indirect
- Legal Repercussions
  - Privacy , lawsuits from investors, industry-specific regulatory agencies
- Loss of Credibility or Competitive Edge
  - A security violation can severely damage credibility, resulting in loss of business and prestige.

# Computer Crime and its Impact

- Blackmail/Industrial Espionage
  - A perpetrator can extort money from an organization by threatening to exploit a security breach.
- Sabotage
  - Dislike of the organization or for self-gratification
- Disclosure of Confidential Information
  - Also sensitive or embarrassing Information.

# Violators

- Hackers
  - Persons with computing talent who gain unauthorized access to computers and networks.
- Employees
  - IS Personnel
  - Disgruntled Employees
  - Addicted to substances
  - Having financial problems
- End User
- Part-time and Temporary Personnel

# Violators

- Former Employees
- Interested or Educated Outsiders
  - Competitors, Foreigners
  - Organized criminals
  - Crackers (paid hackers working for a third party)
  - Phreackers (hackers attempting access into the telephone/communication system)
- Terrorists
- Vendors and Consultants
- Accidental Ignorant

# Computer Forensics

- ✓ Computer Crime is hard to detect and prove.
- ✓ No physical marks or trails.
- ✓ Evidence, if any, is usually in electronic form.
- ✓ Evidence in electronic form is capable of undetectable tampering, which makes it untenable in the court of law.

# Computer Forensics

- Computer forensics is a specialized field
  - which deals with the employment of a set of predefined procedures to thoroughly examine a computer system using software and tools to extract and preserve evidence of criminal activity.
- Preservation, identification, extraction and documentation of computer evidence.

# Access Control

Chapter 21

# Objectives of Access Controls

- ✓ Identification of user, including programs and resources
- ✓ Determine whether the user (including programs) has rights of access to the computer resource
- ✓ The type of access that should be allowed and the abilities thereof
- ✓ Restrict the action of users to permitted resources and abilities thereof

# Logical Access Control Considerations

- Identity of User
  - Nature of authority with regard to the actions permitted on the users is based on the identity of the users.
- Roles
  - Access to resources are categorized on the functions or jobs to be performed by employees.
  - Concept of the owner, user and custodian of the information.

# Logical Access Control Considerations

- Location
  - Access to resources may also be required to be restricted by the physical or logical location of the user.
- Constraints
  - Restricted to certain time of the day or certain days.
- Action Privileges
  - Modes of access with regard to data or information.
  - Read, Write/Create,  Delete, Execute.

# Classification of Information Resources

- ✓ Subjects: Authorized users or processes
- ✓ Objects: Information and IS resources.
- ✓ Naming Conventions
  - Granularity of access control
  - Reduces the number of access rules
  - Easy to maintain

# Classification of data

- ✓ By assigning classes or levels of sensitivity to computer files, management can establish guidelines for the level of access controls that should be assigned.
- ✓ Data classification reduces the risk and cost of overprotecting computer resources.

# Classification of data

- ✓ Top Secret
  - ► Compromise can endanger the existence of the organization.
- ✓ Secret
  - ► Strategic to the survival of the organization.
  - ► Disclosure could cause severe damage to the organization.
- ✓ Confidential
  - ► Compromise may cause loss significant loss or damage.
- ✓ Sensitive
  - ► Disclosure may cause serious impact.
- ✓ Unclassified
  - ► Disclosure would not cause any adverse impact
  - ► Freely available to the public.
- ✓ Public, Sensitive, Private and Confidential.

# Classification of Users

- Access Philosophy
  - Access to computerized information should be based on a documented "need-to-know, need-to-do" basis.
- Data Owners, Custodians and Users
- Data Ownership
  - Data ownership refers to the classification of data elements and allocation of responsibility for ensuring that they are kept confidential, complete and accurate.
  - By assigning responsibility for protecting computer data to particular employees, accountability is established.

# Data Owners

- ✓ Are generally managers and directors responsible for using information for running and controlling the business.
- ✓ Responsible for protection of the data resource and accountable for any loss or damage to the data resource
- ✓ Their security responsibilities include authorizing access, ensuring access rules are updated when personnel changes occur and regularly inventorying access rules for the data for which they are responsible.

# Data Custodians

- ✓ These people are responsible for storing and safeguarding the data.
- ✓ Responsible for day to day protection of the data resource, under delegated responsibility from owners.
- ✓ Include IS personnel such as systems analysts and computer operators.

# Data Users

- These people, often referred to as end users, are the actual users of the computerized data.
- Derive their rights of access from the data owners.
- Their levels of access into the computer should be authorized by the data owners and restricted and monitored by the security administrator.

# Access Control Models

- ✓ Mandatory Access Control
  - ► Labeled security, Rule-based.
  - ► Access restrictions are associated with every resource and every user.
  - ► An individual user is given access to a resource only based on his clearance with respect to every resource.
  - ► Defence installations
- ✓ Discretionary Access Control
  - ► Users are given rights to specify delegation of rights to resources allowed to them.
  - ► Popular in commercial organisations

# Access Control Administration

- Responsibilities
  - Creating new users
  - Implementing access controls (Logical and Physical)
  - Modifying user rights
  - Modifying asset classifications
  - Monitoring access violations
  - Reporting access violations
  - Handling Incidents of violation
  - Terminating users

# Security Administrator

- ✓ Security administrators are responsible for providing adequate physical and logical security for IS programs, data and equipment.
- ✓ Information security policy will provide the basic guidelines under which the security administrator will operate.

# Audit Trail

- ✓ Record of all actions on resources by individuals and computing programs and processes.
- ✓ Source of information about
  - ► Violation of access
  - ► Performance of IS components
  - ► Integrity flaws in processes and data
- ✓ Audit Trails are detective controls for
  - ► Fixing accountability
  - ► Enable reconstruction of events
  - ► Intrusion detection
  - ► Analysis of problem and failed events
  - ► Trace history of transaction updates
  - ► Trace usage/consumption of resources

# Audit Trail

- Effective use of audit trails requires
  - Discipline in enabling and preservation of audit trails
  - Periodic/event based review of audit trails
  - Initiating early corrective action based on audit trail information
- Enabling audit trails draws upon computing resources and impacts availability.

# Components of a Security Policy

- ✓ Management Support and Commitment
- ✓ Access Philosophy
- ✓ Statutory Compliance
- ✓ Reviews of Access Authorization
- ✓ Security Awareness
- ✓ Role of the Security Administrator
- ✓ Security Committee

# Management Support and Commitment

- Management must demonstrate a commitment to security.
  - By clearly approving and supporting formal security awareness and training.
- This may require special management level training since security is not necessarily a part of management expertise.

# Access Philosophy

- ✓ Access to computerized information should be based on a documented "need-to-know, need-to-do" basis.

# Statutory Compliance

- The policy should state that compliance is required with all relevant legislation, E.g.
  - Confidentiality of personal information.
  - Specific regulations relating to particular industries, e.g. banking and financial institutions, Medical records, etc.

# Reviews of Access Authorization

- Access controls should be evaluated regularly to ensure they are still effective.
  - Effectiveness of access controls affected by:
    - Personnel and departmental changes
    - Malicious efforts
    - Carelessness
  - Security administrator, with the assistance of the managers, should review access controls.
  - Any access exceeding the "need-to-know, need-to-do" philosophy should be changed accordingly.

# Security Awareness

- All employees, including management, need to be made aware on a regular basis of the importance of security.
  - Mechanisms available for raising security awareness :
    - Distribution of a written security policy
    - Training on a regular basis of employees, users, support staff
    - Non-disclosure statements signed by the employee
    - Use of different media in promulgating security
    - Visible enforcement of security rules
    - Simulate security incidents for improving security procedures
    - Reward employees who report suspicious events
    - Periodic audits

# Security Awareness

- Employee responsibilities for security include:
  - Reading the security policy
  - Keeping logon-Ids and passwords secret.
  - Reporting suspected violations of security to the security administrator
  - Maintaining good physical security by keeping doors locked, safeguarding access keys, not disclosing access door lock combinations and questioning unfamiliar people
  - Conforming to local laws and regulations
  - Adhering to privacy regulations with regard to confidential information (e.g. health, legal, etc.)

# Role of the Security Administrator

- The security administrator is responsible for
  - Implementing, monitoring and enforcing the security rules that management has established and authorized.
- The security administration should not be responsible for updating application data nor be an end user, application programmer, computer operators or data entry clerk. [Separation of Duties].
- In large organization, the security administrator is usually a full time function; in small organizations, someone may perform its function with other non-conflicting responsibilities.

# Security Committee

- Security guidelines, policies and procedures affect the entire organization and such as should have the support and suggestions of
  - end users, executive management security administration, IS personnel and legal counsel.
- Therefore individuals representing various management levels, should meet as a committee to discuss these issues and establish security practices.

# Logical Security Techniques

Chapter 22

# Process of Access Control

- ✓ Identification
- ✓ Authentication
- ✓ Authorization
- ✓ Accounting
- ✓ Authentication Factors:
  - Something the user has
  - Something the user knows/remembers
  - Something the user is

# Logon Ids and Password

- ✓ Two-phase user identification/authentication process
- ✓ Restrict access to computerized information, transactions, programs and system software
- ✓ The computer maintains an internal list of valid logon-Ids and a corresponding set of access rules for each logon-ID.
- ✓ Access rules can usually be specified at the operating system level (controlling access to files) or within individual application systems

# Authorisation Matrix

- Subject
  - Users
- Object
  - Unit of the database
- Access Rights
  - Read Only, Write Only, Update etc.

| | Data 1 | Data 2 | Data 3 | Data 4 |
|---|---|---|---|---|
| User 1 | RO | RW | RO | RO |
| User 2 | RO | D | RW | RW |
| User 3 | W | D | RO | RW |

# Weaknesses of Logon Mechanism

- ✓ Passwords are easily shared. Users often advertently or inadvertently reveal passwords
- ✓ Repeated use of same password.
- ✓ Password is too short or easy to guess.
- ✓ Password is too long or complex to remember.
- ✓ Too many passwords have to be remembered.
- ✓ Passwords can be shared, guessed, spoofed or captured.

# Passwords - Best Practices

- ✓ Easy for the user to remember, but difficult for a perpetrator to guess.
- ✓ Initial password assignment should be done discretely by the security administrator.
- ✓ If the wrong password is entered a predefined number of times, typically three, the logon-ID should be automatically and permanently deactivated.
- ✓ Passwords should be internally one-way encrypted.
- ✓ Passwords should be changed periodically.
- ✓ Passwords must be known only to one individual.

# Passwords - Best Practices

- ✓ Five to eight characters in length.
- ✓ Combination of alpha, numeric, upper and lower case and special characters.
- ✓ Passwords should not be particularly identifiable with the user (such as first name, last name, spouse name, pet's name, etc.)
- ✓ The system should not permit previous password(s) to be used after being changed.
- ✓ Login-Ids not used after a number of days should be deactivated to prevent possible misuse.
- ✓ The system should automatically disconnect a logon session if no activity has occurred for a period of time (one hour). This is often referred to as "time out."

# Attacks on Password Systems

- Brute force
  - Every possible combination of characters is tried out.
- Dictionary attack
- Trojan
  - Use a Trojan to steal access control lists or other information.

# Attacks on Password Systems

- Spoofing Attack
  - Use a Trojan program, which mimics the system's logon screen, gets the logon and password information and returns control to the genuine access control mechanism.
- Piggybacking
  - Wait for an authorized user to log in and leave the terminal unattended.
  - To secure against this attack automatically log out the session after a pre-determined time of inactivity

# Token Based authentication

- Plastic Cards:
  - Identification of the user and can enable authentication
- Memory tokens
    - Contain visible information such as name, identification number, photograph
    - Magnetic strip, which stores static information about the user.
  - Process
    - Swipe his card through a card reader, which reads the information on the magnetic strip and passes onto the computer for verification with stored information to enable access.
    - Where two-factor authentication is adopted, the user is not only required to have his card read by a card reading device but also required to key in a remembered information
  - E.g. Bank ATM Card

# Token Based authentication

- Smart Tokens
  - Contains a small processor chip which enable storing of dynamic information on the card.
  - Loss of such smart cards can have more serious implications.
- Proximity Readers
  - Card is read by the proximity readers which transmits information to the authentication computer, which enable access to the restricted area or system.
  - Access time is faster
  - Either static or processor based

# Token Based authentication

- Challenge Response
  - Attempt  to reduce the disadvantages with passwords.
  - System generates a random challenge string, which the user enters into a token device along with his PIN. Based on the inputs, the token device generates a response that is entered into the workstation.
- One time Passwords
  - Every session initiated by the user with a system requires a unique password.
  - System generates a one time password based on a pass-phrase input.
  - User can use for one time entry to the desired application or IS resource.

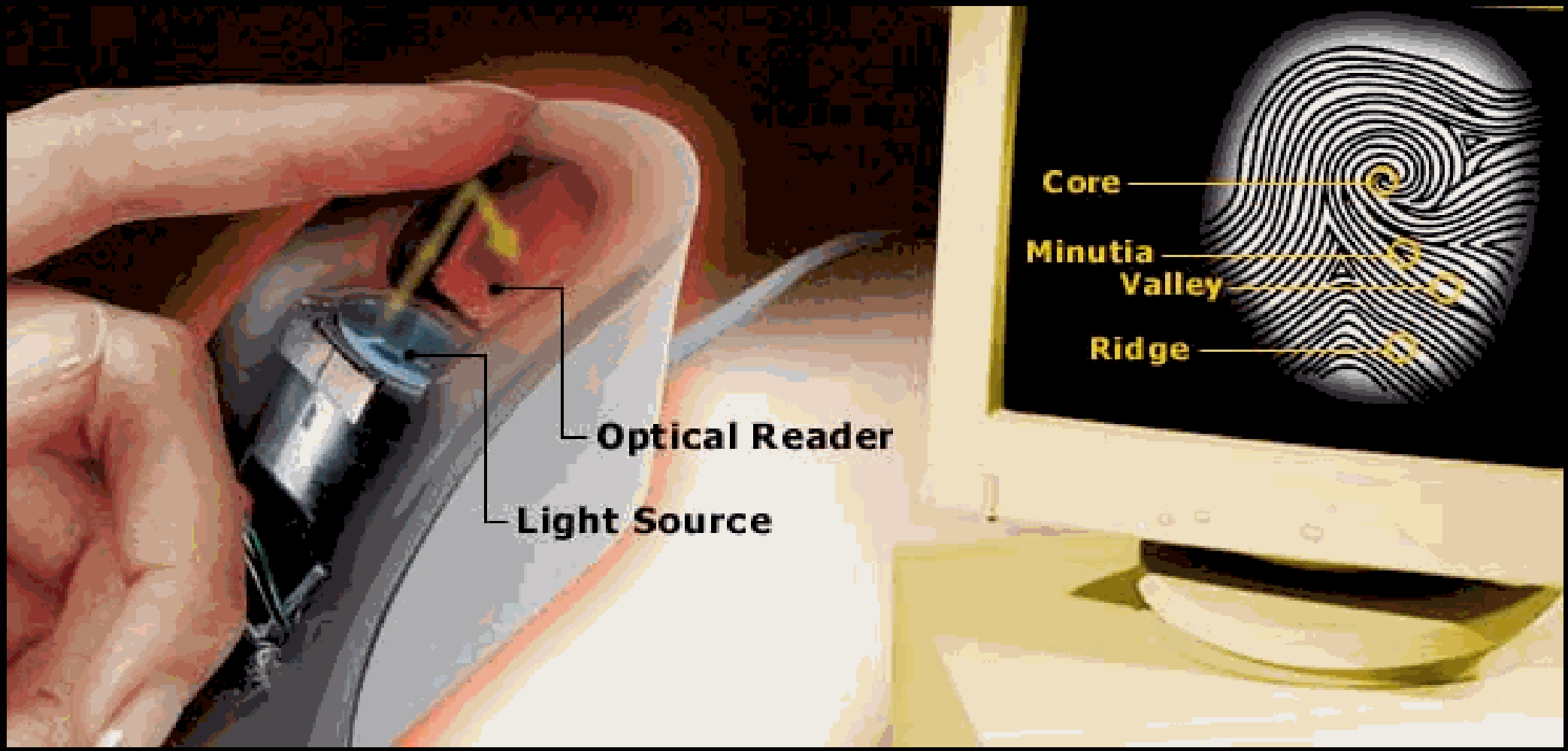
# Single Sign-on

- ✓ User is  required to log into more than one applications.
- ✓ Problem of multiple logon and passwords
- ✓ Transfer all login control to an access control system
- ✓ Single login giving access to multiple applications

# Biometric security

- ✓ Fingerprint
- ✓ Facial Scan
- ✓ Hand Geometry
- ✓ Signature
- ✓ Voice
- ✓ Keystroke Monitoring
- ✓ Iris Scanners
- ✓ Retina Scanners

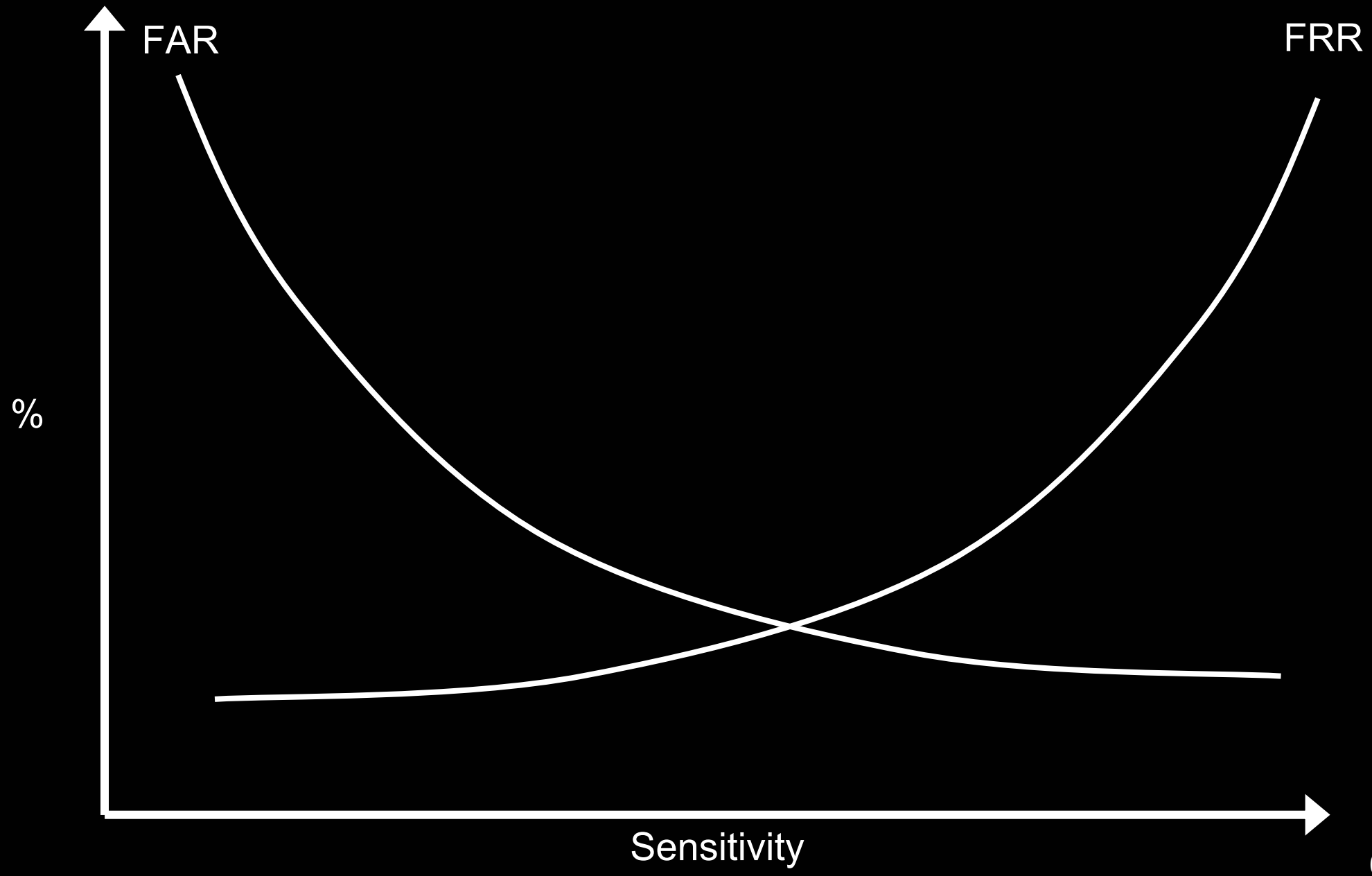
# Fingerprint Scanner



# Biometric security- Metrics

- FRR: False Rejection Rate
  - Wrongfully rejecting a rightful user
- FAR: False Acceptance Rate
  - Wrongfully authenticating an unauthorized user
- Ideal biometric systems requires a low false rejection and false acceptance rate.
- CER: Common Error Rate
  - Crossover Error Rate, is that point where the percentage of false acceptances and false rejects is equal

# FRR Vs FAR



# Operating Systems logical security

- ✓ Reference monitor is an abstract mechanism that enables enforcing the security policy.
- ✓ The reference monitor mediates all accesses between the subject and objects thus enforcing the security policy via the security kernel.
- ✓ The reference monitor enables segregation of rights of access such as privileged logon and restricts access based on context.

# Relational Database Security

- ✓ Name-Dependent
- ✓ Content Dependent
- ✓ Context Dependent
- ✓ History Dependent

# Name-Dependent Restrictions

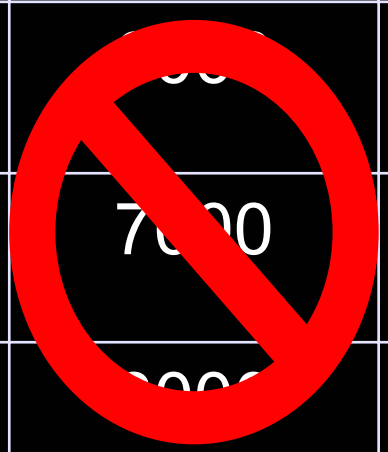
- Users either have access to the named resource or not. Content-Independent .

| Name | Dept | Salary | Address | Rating |
|---|---|---|---|---|
| Satish | Acctg. | 5000 | Delhi | 5 |
| Harish | R&D | 6000 | Goa | 6 |
| Mathew | Prodn. | 7000 | Kochi | 7 |
| Radha | R&D | 8000 | Goa | 8 |

# Content-Dependent Restrictions

- Users permitted or denied access to data depending on its contents

| Name | Dept | Salary | Address | Rating |
|---|---|---|---|---|
| Satish | Acctg. | 5000 | Delhi | 5 |
| Harish | R&D | [redacted] | Goa | 6 |
| Mathew | Prodn. | [redacted] | Kochi | 7 |
| Radha | R&D | [redacted] | Goa | 8 |



# Context-Dependent Restrictions

- Users are permitted or denied access based on the context in which they are seeking access. E.g. Statistical queries

| Name | Dept | Salary | Address | Rating |
|---|---|---|---|---|
| Satish | Acctg. | 5000 | Delhi | 5 |
| Harish | R&D | 21000 | Goa | 6 |
| Mathew | Prodn. | | Kochi | 7 |
| Radha | R&D | | Goa | 8 |

# History-Dependant Restrictions

- ✓ Users are permitted or denied access based on the time series of access and actions they have undertaken

| Name | Dept | Salary | Address |
|---|---|---|---|
| Satish | Acctg. | 5000 | Delhi |
| Harish | R&D | | Goa |
| Mathew | Prodn. | 21000 | Kochi |
| Radha | R&D | | Goa |

R & D
14000

# Network Security

- Terminal security
  - Security feature restricts the number of terminals that can access certain transactions based on the physical/logical address of the terminal.
  - Terminal locks
    - Security feature prevents turning on a computer terminal until a key lock is unlocked by a turn key or card key.
- Dial back procedures
  - Dial-back interrupts the telecommunications dial-up connection to the computer by dialling back the caller to validate user authority.
  - Dial-back can be manual (the computer operator calls back the user) or automatic, (the computer calls back the user using a computerized list of valid phone numbers).
  - Call forwarding can circumvent some dial-back systems.
- Multi-factor authentication

# Network Security

- ✓ Authentication Servers
  - ► Access control is transferred to a centralized or decentralized access authentication servers.
  - ► TACACS (Terminal Access Controller Access Control System)
  - ► RADIUS (Remote Authentication Dial In User Service)
- ✓ Kerberos
  - ► Access is enabled based on a unique encrypted session key generated by interactions between the requesting client, authentication server and then requested server granting a session ticket to the client.
- ✓ Firewalls

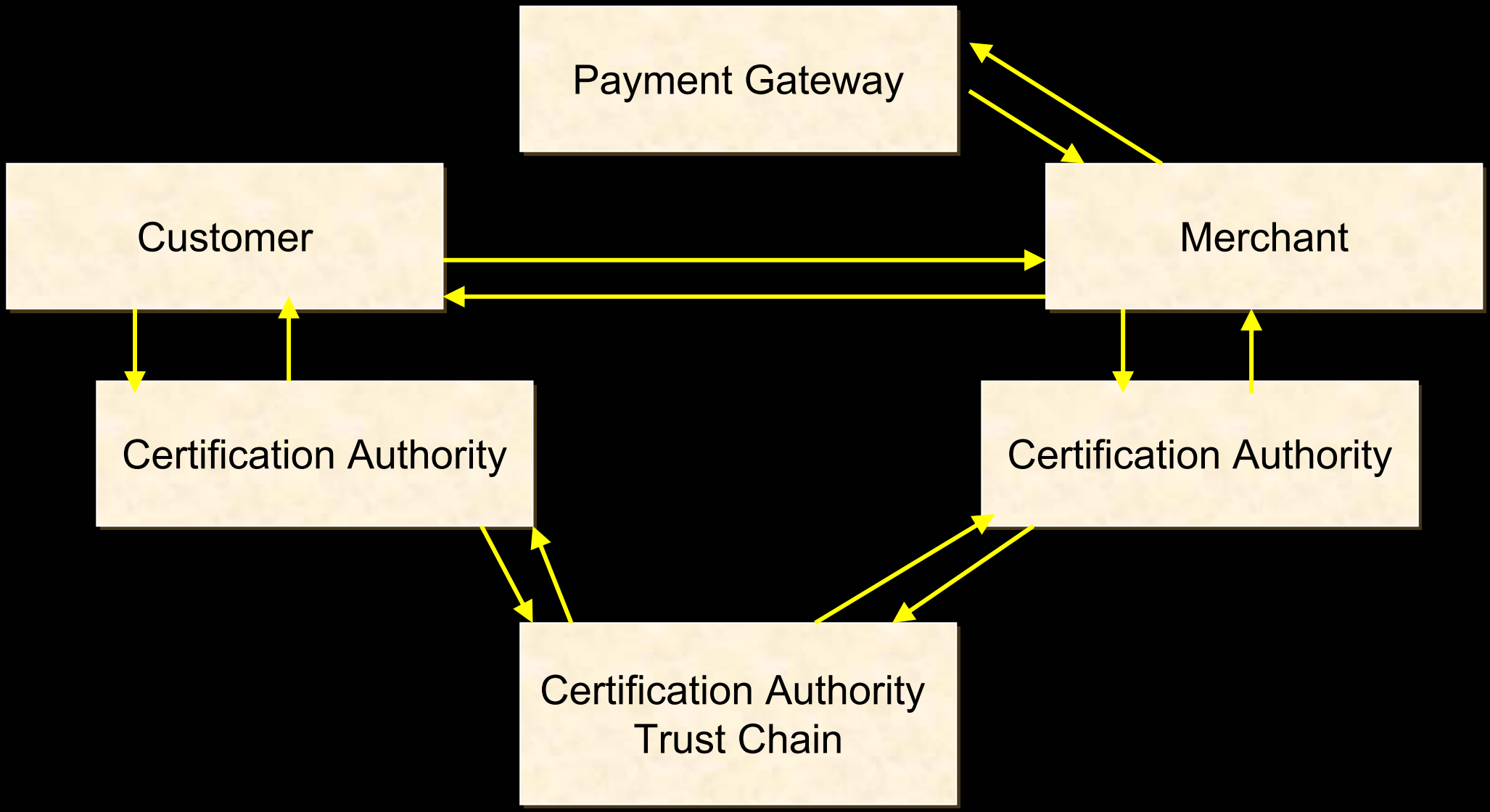
# Network Security

- Intrusion Detection Systems
- Virtual Private Networks (VPNs)
  - VPNs implemented with firewalls create a secure logical tunnel through the unprotected networks connected two or more disparate networks.
  - IPSec, which offers encryption, access control, non repudiation and authentication of packets traveling over unprotected network
- Security Protocols
    - Secure Socket Layer (SSL)
    - Secure Electronic Transaction (SET),
    - Secure Multipurpose Internet Mail Extensions (S/MIME)
    - Pretty Good Privacy (PGP)

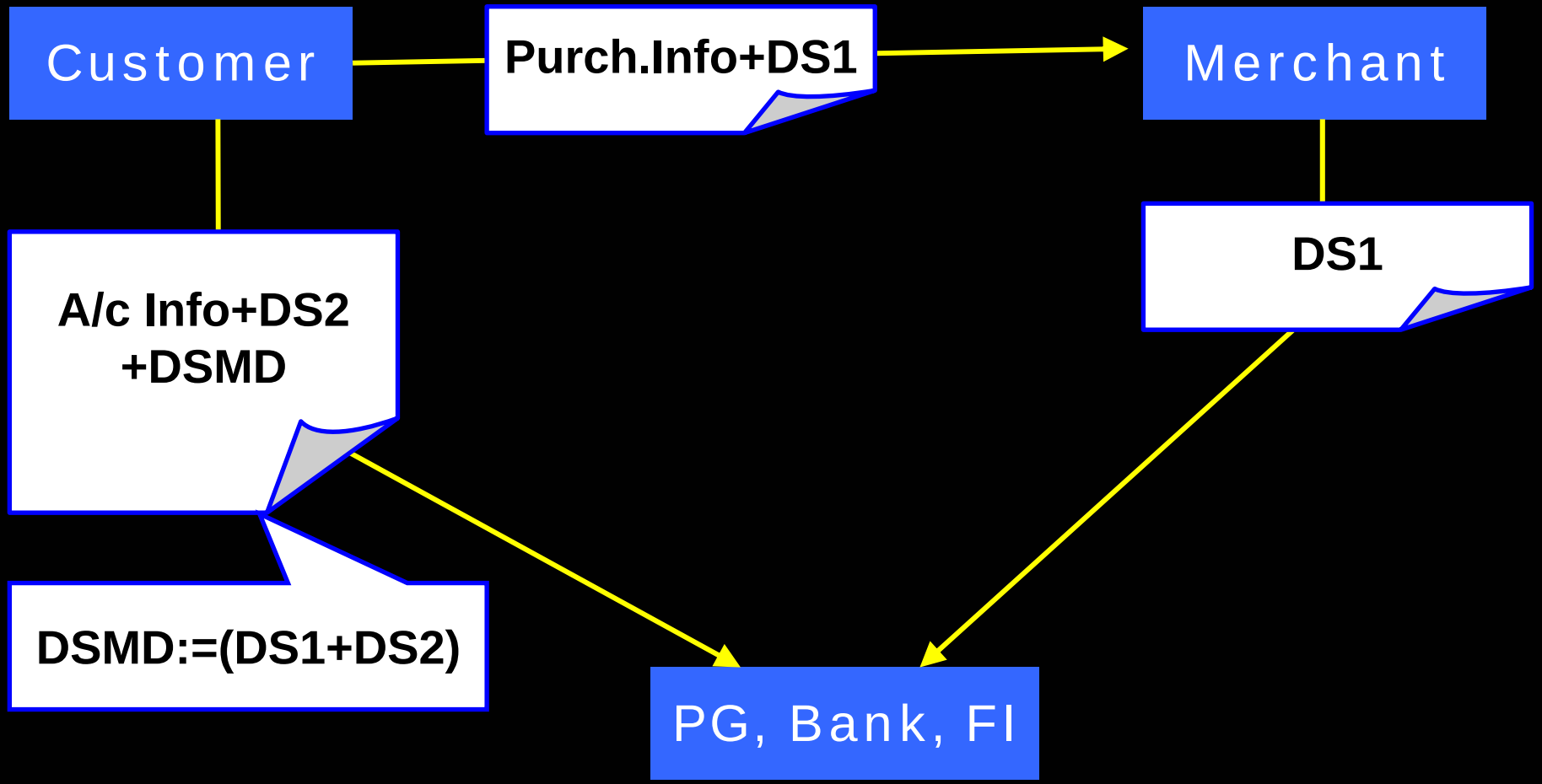
# Secure Socket Layer

- ✓ Developed by Netscape for transmitting private documents via the Internet.
- ✓ SSL works by using a private key to encrypt data that's transferred over the SSL connection.
- ✓ Both Netscape Navigator and Internet Explorer support SSL
- ✓ Web sites use the protocol to obtain confidential user information, such as credit card numbers.
- ✓ By convention, Web pages that require an SSL connection start with https: instead of http.

# SET Credit Card Purchase Model



# SET Dual Signature



# Application Controls

Chapter 23

# Components

- ✓ Boundary Controls
  - Access by authorized users
- ✓ Input Controls
  - Complete, accurate and valid data/Instructions
- ✓ Processing Controls
  - Only authorized processing
  - Integrity of processes and data
- ✓ Datafile controls
  - Consistency, integrity, confidentiality of resident data.
- ✓ Output Controls
  - Consistent and timely outputs

# Boundary Controls Techniques

- ✓ Logon id/password
- ✓ Specified terminals only
- ✓ Encrypt data leaving and entering the application process.
- ✓ Encrypt intermediary data either in input, processing or output stage.
- ✓ Encrypt all exchanges of data/process.

# Input Controls

- ✓ Data Input Methods
- ✓ Source Document Design
- ✓ Data entry screen design
- ✓ Data code controls

# Data Input Methods

- Attribute
  - State of an object (Price, Dimension)
  - Event (Sale, Purchase)
- Devices
  - Keyboard
  - Scanners
  - Mouse
  - Touch screens

# Source Document Design

- Include instructions for completing the form.
- Minimize the amount of handwriting.
- Data to be entered (keyed) should be sequenced so that it can be read like a book, that is, top-to-bottom and left-to-right.
- Capture only variable data
- Do not capture data that can be calculated or stored in computer programs as constants
- Use organization wide consistent business codes for appropriate attributes

# Data entry screen design

- ✓ Caption design
  - Captions consistent
  - Close to data fields.
  - Captions for data fields should be distinctive
  - The caption for each entry field should end with a special symbol
  - Descriptive wording, predefined terms, codes and/or abbreviations
- ✓ Data entry field design
  - Data entry fields should be either to the right of the caption or exactly below it.
  - Provide underscores in fields to indicate when a fixed or maximum length Design should be based on the source document.
  - Small List: Option buttons and check boxes
  - Long list: List boxes
- ✓ Tabbing and skipping
  - Insertion point should move from the first field on the screen to the last without jumping about
  - Incorrect tab order will not only frustrate users, cause user to enter data into the wrong field.
  - Automatic tabbing should be avoided.

# Data entry screen design

- Colour
  - Bright colours should be avoided.
  - Pastel/ soft colours or those that provide good contrast for the fields and captions.
  - Instead of colour, use uppercase and lowercase text to differentiate captions.
- Response time
  - Response time is the interval between entry of data item and the system's indication that it has been stored and is ready for new data.
  - Should be as low as possible and should be reasonably constant.
- Display rate
  - Rate at which characters or images should be displayed. Data entry screens should have a fast display rate. If display rate is slow or inconsistent the data entry is prone to errors.
- Prompting and help facilities
  - Descriptive help should be added wherever possible. Data entry forms should be as self-explanatory as possible but can include help for each field.
  - Further prompting of actions that should be taken by the user will also help if a pop up message is included on placing the cursor on the field.
  - Prompting and help is more required in the case of direct data entry where no source document is involved.

# Data Code Controls

- Types Coding Errors
  - Addition
  - Truncation
  - Transcription
  - Transposition
  - Double transposition

# Data Code Controls

- ✓ Factors affecting Coding Errors
  - Length of the code
    - ► Long codes are error-prone. Use hyphens, slashes, spaces
  - Alphabetic numeric mix
    - ► Grouping of alphabets and numerical separately
  - Choice of characters
    - ► B, I, O, S, V and Z would be confused with 8,1,0,5,U, 2
  - Mixing uppercase/lowercase fonts
    - ► Upper case and lower case should NOT be mixed.
  - Sequence of characters
    - ► Maintain character sequence
- ✓ Check Digits

# Batch Controls

- ✓ Total Monetary Amount
  - Verification that the total monetary value of items processed equals the total monetary value of the batch documents.
- ✓ Total Items
  - Verification that the total number of items included on each document in the batch agrees to the total number of items processed.
- ✓ Hash Totals
  - Verification that a predetermined numeric field existing for all documents in a batch agrees with the total of documents processed.
- ✓ Total Documents
  - Verification that the total number of documents in the batch equals the total number of documents processed.

# Data Validation and Editing

- Sequence Check
- Range Check
- Limit Check
- Missing Data Check
- Duplicate Check
- Programmed Validity Check
- Dependency Check
- Completeness Check
- Reasonableness Check
- Table Look-Ups
- Existence Check

# Data Validation

- Sequence Check
  - The control number follows sequentially and any control numbers out of sequence or duplicated are rejected or noted on an exception report for follow-up purposes.
- Range check
  - Data should be within a predetermined amount. For example, product type codes range from 100 to 250
- Limit check
  - Data should not exceed a predetermined amount. For example, cash payments should not exceed Rs.20,000.

# Data Validation

- Missing Data Check
  - Ensure that key fields are not left blank
- Duplicate Check
  - New transactions are matched to those previously input to ensure that they have not already been entered. Suppliers Invoice Numbers.
- Programmed Validity check
  - Programmed checking of the data validity in accordance with predetermined criteria. For example, marital status is either M or S.

# Data Validation

- Dependency Match(Logical Relationship Check)
  - If a particular condition is true, then one or more additional conditions or data input relationships may be required to be true and consider the input valid. Hire Date > DoB +18.
- Reasonableness Check
  - Input data are matched to predetermined reasonable limits or occurrence rates. For example, a widget manufacturer usually receives orders for no more than 20 widgets. If an order for more than 20 widgets is received, the computer program indicates that the order appears unreasonable.

# Data Validation

- Table Look-ups
  - Input data complies with predetermined criteria maintained in a computerized table of possible values. E.g. Account Codes
- Existence check
  - Data are entered correctly and agree with valid predetermined criteria. Supplier Names
- Completeness Check
  - To ensure that a field contains data and not zeros or blanks.

# Input Error Handling

- Rejecting Only Transactions with Errors
  - Only transactions containing errors would be rejected
- Rejecting the Whole Batch of Transactions
  - Any batch containing errors would be rejected
- Accepting Batch in Suspense
  - Any batches containing errors would not be rejected however, the batch would be posted to suspense pending correction.
- Accepting Batch and Flagging Error Transactions
  - Any batch containing errors would be processed; however, those transactions containing errors would be flagged.

# Instruction input methods

- ✓ Menu Driven Applications
- ✓ Question Answer dialogs
- ✓ Command Languages
- ✓ Direct Manipulation interfaces

# Instruction Input Validation

- Lexical validation
  - Each word entered as a instruction is validated.
- Syntactic validation
  - String of words validated
- Semantic validation
  - Semantic validation reads the set of instructions and verifies if the meaning is correct.
- Example:
    - COMPUTE C = A + B
    - COMPOTE C + A + B

# Processing Controls

- Run-to-Run Totals
  - Run-to-run totals provide the ability to verify data values through the stages of application processing. Run-to-run total verification ensures that data read into the computer was accepted and then applied to the updating process
- Reasonableness verification
- Edit checks
  - An edit check is a program instruction or subroutine that tests for accurate, complete and valid input and updates in an application.
- Field initialization
- Exception reports

# Data File Control Procedures

- ✓ Version usage
- ✓ Internal and External Labeling
- ✓ Data File Security
- ✓ Before and After Image Reporting
- ✓ File Updating and Maintenance Authorization
- ✓ Maintenance Error Reporting and Handling
- ✓ Source Documentation Retention
- ✓ One-For-One Checking
- ✓ Pre-recorded Input
- ✓ Transaction Logs
- ✓ Parity Checking

# Data File Control Procedures

- Version usage
  - It is critical that the proper version of a file, such as date and time of data, be used as well as the correct file in order for the processing to be correct. For example, transactions should be applied to the most current database while restart procedures should use earlier versions.

# Data File Control Procedures

- Internal and External Labelling
  - External labels provide the basis level of assurance that the correct data medium is loaded for processing. Internal labels, including file header records, provide assurance that the proper data file are used and allow for automated checking.
- Data File Security
  - Data file security controls prevent unauthorized access by unauthorized users that many have access to the application to alter data files.

# Data File Control Procedures

- Before and After Image Reporting
  - Computer data on a file prior to and after a transaction is processed can be recorded and reported.
- File Updating and Maintenance Authorization
  - Proper authorization for file updating and maintenance is necessary to ensure that stored data are adequately safeguarded, correct and up-to-date. The additional security may provide levels of authorization in addition to providing an audit trial of file maintenance.

# Data File Control Procedures

- One-For-One Checking
  - Individual documents agree with a detailed listing of documents processed by computer. It is necessary to ensure that all documents have been received for processing.
- Prerecorded Input
  - Certain information fields are preprinted on blank input forms to reduce initial input errors.
- Transaction Logs
  - All transaction input activity is recorded by the computer. A detailed listing including date of input, time of input, user ID and terminal location can then be generated to provide an audit trail.

# Data File Control Procedures

- Parity Checking
  - When programs or vital data are transmitted, additional controls are needed. Transmission errors are controlled primarily by error detecting or correcting codes. Check Parity Checks, Check Digits, CRC, etc.
- Maintenance Error Reporting and Handling
  - Control procedures should be in place to ensure that all error reports are properly reconciled and corrections are submitted on a timely basis. Segregation of Duties.
- Source Documentation Retention
  - Source documentation should be retained for an adequate time period to enable retrieval, reconstruction or verification of data.

# Output Controls

- **Statistical inferences**
  - Positive inference
    - Where a user is able to detect the positive nature or characteristic of a data value. For example, if he is able to find the fact that a senior officer of the company is a consultant and not an employee
  - Negative inference
    - Where a user is able to detect a negative attribute of a data value such as finding out that a senior officer of the company is not a permanent employee but a temporary staff.
  - Exact compromise
    - Users are able to find out the exact value of the data. For example, finding out the personal phone numbers of a senior director of the company, which is available only to Managing Director.
  - Approximate compromise
    - Users are able to find out the approximate salary of an officer based on his grade.

# Batch output controls

- ✓ Storage and logging of sensitive, critical forms
- ✓ Logging of output program executions:
- ✓ Spooling/ Queuing
- ✓ Controls over printing
- ✓ Report distribution and collection controls
- ✓ Retention controls

# Online output controls

- Source controls
  - Source of the output is accurate, complete and consistent.
- Distribution controls
  - Only authorized persons receive the output.
- Communication controls
- Receipt controls
- Retention and deletion controls

# Auditing Logical Access & Application Controls

Chapter 24

# Auditing Logical Access

- ✓ Familiarization with the Information Systems Processing Environment
- ✓ Document the Access Paths
- ✓ Interview Systems Personnel
- ✓ Review Reports from access control software√
- ✓ Review Application Systems Operations Manual
- ✓ Review Written Policies, Procedures and Standards
- ✓ Logical Access Security Policies
- ✓ Formal Security Awareness and Training
- ✓ Documented Authorizations
- ✓ Access Standards

# Familiarization with the IS Environment

- ✓ Obtain a clear understanding of the technical, managerial and security environment of the information systems processing facility.
- ✓ Obtain general understanding of the security risks facing information processing through a review of relevant documentation, inquiry, observation, risk assessment and evaluation techniques.

# Document the Access Paths

- ✓ The terminal should be physically and logically secured.
- ✓ The telecommunications software.
  - Ensure all applications have been defined to the software and that the various optional telecommunication control and processing features used are appropriate and approved by management. Assistance of a system software analyst may be required.
- ✓ The TPS may be the next component in the access path.
  - Key audit issues include ensuring identification/authentication and authorization of the user to gain access to the application.
  - Review internal tables that can reside in the transaction processing software or in separate security software. Access to these should be restricted to the security administrator.
- ✓ Application software then the DBMS.
- ✓ Access Control Software encompasses all the above.

# Interview Systems Personnel

- ✓ Technical experts can be a valuable source of information to the IS Auditor when gaining an understanding of security. To determine who these people are, the IS Auditor should meet with the IS manager and review organizational charts and job descriptions.
- ✓ Key people include the security administrator, network control manager and systems software manager.
- ✓ The IS Auditor should determine whether the security administrator is aware of the logical accesses that must be protected, has the motivation and means to actively monitor logons to account for employee changes and is knowledgeable in how to maintain and monitor access.
- ✓ Interview a sample of end users to assess their awareness of management policies regarding logical security and confidentiality.

# Review Reports from ACS

- ✓ Unsuccessful access attempts should be reported and the ACS should identify the time, terminal, logon and file or data element for which access was attempted.
- ✓ By reviewing a sample of security reports, the IS Auditor can determine if enough information is provided to support an investigation and if the security administrator is performing an effective review of the report.

# Review Operations Manual

- Documentation on the programs that are generally used throughout a data processing installation to support the development, implementation, operations and use of application systems.
- This manual should include information about
  - Platform the application can run on
  - Other applications that can run with the application.

# Review Policies, Procedures and Standards

- ✓ The IS Auditor should review the policies and procedures to determine if they set the tone for proper security and provide a means for assigning responsibility for maintaining a secured computer processing environment.

# Logical Access Security Policies

- ✓ These policies should encourage limiting logical access to a need-to-know basis.

# Formal Security Awareness and Training

- ✓ Security can only be effective if employees know what is expected of them and what their responsibilities are.
- ✓ Promoting security awareness is a preventive control. This can also be a detective measure because it encourages people to identify and report possible security violations.
- ✓ Training should start with the new employee orientation or induction process.
- ✓ To determine the effectiveness of the program, the IS Auditor should interview a sampling of employees to determine their overall awareness.

# Documented Authorizations

- Data access should be identified and authorized in writing.
- The IS Auditor can
  - review a sample of these authorizations to determine if the proper level of written authority was provided.
- If the facility practices data ownership, only the data owners provide written authority.

# Access Standards

- ✓ Access standards should be reviewed by the IS Auditor to ensure that they meet organizational objectives for separating duties, that they prevent fraud or error and that they meet policy requirements for minimizing the risk of unauthorized access.
- ✓ E.g. “all passwords must be at least five character long”

# Security Testing

- ✓ Use of Terminal Cards and Keys
- ✓ Terminal Identification
- ✓ Logon-IDs and Passwords
- ✓ Controls Over Production Resources
- ✓ Logging and Reporting of Computer Access Violations
- ✓ Follow-up Access Violation
- ✓ Dial-Up Access Controls
- ✓ Authorization of Network Changes
- ✓ Identify Methods of Bypassing Security and Compensating Controls
- ✓ Review Access Controls and Password Administration

# Use of Terminal Cards and Keys

- ✓ The IS Auditor can take a sample of these cards or keys and attempt to gain access beyond that which is authorized.
- ✓ IS Auditor will want to know if the security administrator followed up on any unsuccessful attempted violations.

# Terminal Identification

- The IS Auditor can work with the network manager to get a listing of terminal addresses and locations. The IS Auditor can then use this list to inventory the terminals, looking for incorrectly logged, missing or additional terminals. The IS Auditor should also select a sample of terminals to ensure they are identified in the network diagram.

# Logon-IDs and Passwords A

- ✓ IS Auditor should attempt to guess the password of a sample of employees' logon-IDs.
- ✓ The IS Auditor should tour end user and programmer work areas looking for passwords taped to the side of terminals, the inside of desk drawers or located in card files.
- ✓ Another source of confidential information is the wastebasket.
- ✓ Users could be asked to give their password to the IS Auditor. However, unless specifically authorized for a particular situation and supported by the security policy, no user should ever disclose his or her password.

# Logon-IDs and Passwords B

- Manual tests:
  - Test periodic change requirements interview a sample of users.
  - Test for disabling or deleting of inactive logon-IDs and passwords. Look for logon-IDs assigned to employees or consultants who are no longer with the company.
  - Test for password syntax.
  - Test for automatic logoff of unattended terminals.
  - Test for automatic deactivation of terminals after unsuccessful access attempts.
  - Test for masking of passwords on terminals.

# Controls Over Production Resources

- Access control should be particularly strong for high level utilities, macro or job control libraries, control libraries and system software parameters. Access to these libraries would provide the ability to bypass other access controls.
- IS Auditor should
  - determine who can access these resources and what can be done with this access.
  - determine if access is on a need-to-know basis.

# Reporting of Computer Access Violations

- ✓ To test for reporting of access violations, the IS Auditor should attempt to access computer transactions or data for which access is not authorized.
- ✓ The attempts should be unsuccessful and should be identified on security reports.
- ✓ This test should be coordinated with the data owner and security administrator to avoid violation of security regulations.

# Follow-up Access Violation

- ✓ The IS Auditor should select a sample of security reports and look for evidence of follow-up and investigation of access violations.

# Dial-Up Access Controls

- ✓ To test for dial-up access authorization, the IS Auditor should dial the computer from a number of authorized and unauthorized telephone lines.
- ✓ If controls are adequate, successful connection will occur with the authorized numbers only.

# Authorization of Network Changes

- Network configuration changes should be authorized in writing by management and implemented in a timely manner.
- The IS Auditor can test this change control by
  - sampling recent change requests, looking for appropriate authorization and matching the request to the actual network device.
  - matching recent network changes, such as new telecommunication line, to added terminals and authorized change requests.

# Methods of Bypassing Security

- This typically includes bypass label processing, special system maintenance logon-Ids, operating system exits, installation utilities and I/O appendages.
- IS Auditor should
  - determine who can access these resources and what can be done with this access.
  - determine if access is on a need-to-basis.

# Review Access Controls and Password Admin.

- ✓ Procedures exist for adding individuals to the list of those authorized to have access to computer resources, changing their access capabilities and deleting them from the list.
- ✓ Passwords syntax, format and change frequency
- ✓ User organizations periodically validate the access capabilities currently provided to individuals in their department.
- ✓ Procedures provide for the suspension of user identification codes (logon-Ids or accounts) or the disabling of terminal, microcomputer or data entry device activity after a particular number of security procedure violations.

# Physical Access Controls

Chapter 25

# Physical Access Exposures

- ✓ Unauthorized entry
- ✓ Damage/theft to equipment or document
- ✓ Copying/viewing of sensitive/copyrighted information
- ✓ Public disclosure of sensitive information
- ✓ Abuse of data processing resources
- ✓ Blackmail
- ✓ Embezzlement

# Possible Perpetrators

- ✓ Employees
  - Disgruntled
  - On strike
  - Threatened by disciplinary action/dismissal
  - Addicted to narcotics/gambling
  - Experiencing financial/emotional problems
  - Notified of their termination
  - Former employees
- ✓ Interested or informed outsiders
- ✓ Accidental ignorant

# Physical Access Control Techniques

- ✓ Bolting Door Locks
- ✓ Combination Door Locks (Cipher Locks)
- ✓ Electronic Door Locks
- ✓ Biometric Door Locks
- ✓ Deadman Doors
- ✓ Compound wall
- ✓ Identification Badges (Photo IDs)
- ✓ Manual Logging
- ✓ Electronic Logging
- ✓ Security Guards
- ✓ Controlled Single Entry Point
- ✓ Controlled Visitor Access
- ✓ Bonded Personnel
- ✓ Alarm System
- ✓ Video Cameras
- ✓ Secured Report/Document Distribution Cart
- ✓ Not Advertising the Location of Sensitive Facilities
- ✓ Computer Terminal Locks

# Physical Access Controls

- ✓ Bolting Door Locks
- ✓ Combination Door Locks (Cipher Locks)
- ✓ Electronic Door Locks
- ✓ Biometric Door Locks
- ✓ Manual Logging
- ✓ Electronic Logging
- ✓ Identification Badges (Photo IDs)
- ✓ Video Cameras
- ✓ Security Guards
- ✓ Controlled Visitor Access
- ✓ Bonded Personnel
- ✓ Deadman Doors
- ✓ Not Advertising the Location of Sensitive Facilities
- ✓ Computer Terminal Locks
- ✓ Controlled Single Entry Point
- ✓ Alarm System
- ✓ Secured Report/Document Distribution Cart

# Bolting Door Locks

- ✓ These locks require the traditional metal key to gain entry.
- ✓ The key should be stamped "Do not duplicate".

# Combination Door Locks (Cipher Locks)

- ✓ Also called Cipher Locks.
- ✓ This system uses a numeric key pad or dial to gain entry.
- ✓ The combination should be changed at regular intervals or whenever an employee with access is transferred, fired or subject to disciplinary action.

# Electronic Door Locks

- This system uses a magnetic or embedded chip-based plastic card key or token entered into a sensor reader to gain access.
- A special code internally stored in the card or token is read by the sensor device that then activates the door locking mechanism.
- Advantages over bolting/combination locks:
  - Cards can be assigned to an identifiable individual.
  - Restrictions can be to door-based or time-based
  - They are difficult to duplicate.
  - Card entry can be easily deactivated in the event an employee is terminated or a card is lost or stolen.

# Biometric Door Locks

- An individual's unique body features, such as voice, retina, fingerprint or signature, activate these locks.
- This system is used in instances when extremely sensitive facilities must be protected, such as in the military.

# Manual Logging

- All visitors should be required to sign a visitor's log indicating their name, company represented, reason for visiting and person to see.
- Logging typically is at the front reception desk and entrance to the computer room.
- Before gaining access, visitors should also be required to provide verification of identification, such as a driver's license, business card or vendor identification tag.

# Electronic Logging

- ✓ Feature of electronic and biometric security systems.
- ✓ All access can be logged, with unsuccessful attempts being highlighted.

# Identification Badges (Photo IDs)

- ✓ Badges should be worn and displayed by all personnel.
- ✓ Visitor badges should be a different color from employee badges for easy identification.
- ✓ Sophisticated photo IDs can also be utilized as electronic card keys.

# Video Cameras

- ✓ Cameras should be located at strategic points and monitored by security guards.
- ✓ Sophisticated video cameras can be activated by motion.
- ✓ The video surveillance recording should be retained for possible future playback.

# Security Guards

- ✓ Guards are very useful if supplemented by video cameras and locked doors. Guards supplied by an external agency should be bonded to protect the organization from loss.

# Controlled Visitor Access

- All visitors should be escorted by a responsible employee.
- Visitors include
  - friends
  - maintenance personnel
  - computer vendors
  - consultants (unless long-term, in which case special guest access may be provided)
  - external auditors

# Bonded Personnel

- ✓ All service contract personnel, such as cleaning people and off-site storage services, should be bonded.
- ✓ This does not improve physical security but limits the financial exposure of the organization.

# Deadman Doors

- This system uses a pair of (two) doors, typically found in entries to facilities such as computer rooms and document stations. For the second door to operate, the first entry door must close and lock, with only one person permitted in the holding area.
- This reduces the risk of piggybacking, when an unauthorized person follows an authorized person through a secured entry.

# Location of Sensitive Facilities

- ✓ Facilities such as computer rooms should not be visible or identifiable from the outside, that is, no windows or directional signs.
- ✓ The building or department directory should discreetly identify only the general location of the information processing facility.

# Computer Terminal Locks

- These lock the device to the desk,
  - prevent the computer from being turned on
  - Disengage keyboard recognition
  - Prevent the use of the computer.

# Controlled Single Entry Point

- ✓ A controlled entry point monitored by a receptionist should be used by all incoming personnel.
- ✓ Multiple entry points increase the risk of unauthorized entry.
- ✓ Unnecessary or unused entry points should be eliminated or deadlocked.

# Alarm System

- ✓ An alarm system should be linked to inactive entry points, motion detectors and the reverse flow of enter or exit only doors.

# Secured Report Distribution Cart

- ✓ Secured Report/Document Distribution Cart - Secured carts, such as mail carts, should be covered and locked and should not be left unattended.

# Auditing Physical Access

- Tour
  - information processing facility (computer room, programmers area, tape library, printer stations and management offices)
  - off-site storage facilities.
- Documents to assist with this effort include
  - emergency evacuation procedures
  - inspection tags (recent inspection?)
  - fire suppression system test results (successful? recently tested?)
  - key lock logs (all keys accounted for and not outstanding to former employees or consultants?)

# Environmental Controls

Chapter 26

# Environmental Issues and Exposures

- ✓ Fire
- ✓ Natural disasters
  - Earthquake, volcano, hurricane, tornado
- ✓ Power failure
- ✓ Electrical shock
- ✓ Air conditioning failure
- ✓ Equipment failure
- ✓ Water damage/flooding
- ✓ Bomb threat/attack

# Other Environmental Issues

- Is the power supply to the computer properly controlled ?
- Are the HVAC systems for the computer equipment adequate to maintain temperatures within manufacturers' specifications?
- Is the computer equipment protected from the effects of static electricity, using an anti-static rug or anti-static spray?
- Is the computer equipment kept free of dust, smoke and other particulate matter, such as food?
- Is consumption of food, beverage and tobacco products prohibited, by policy around computer equipment?
- Are backup media protected from damage due to temperature extremes, the effects of magnetic fields and water damage?

# Controls for Environmental Exposures I

- ✓ Water Detectors
- ✓ Hand-Held Fire Extinguishers
- ✓ Manual Fire Alarms
- ✓ Smoke Detectors
- ✓ Fire Suppression Systems
  - Water-based systems
    - Wet – Pipe (charged water)
    - Dry – Pipe
  - Halon systems
  - Carbon Dioxide ($CO_2$)

# Controls for Environmental Exposures II

- ✓ Strategically Locating the Computer Room
- ✓ Regular Inspection by Fire Department
- ✓ Fireproof Walls, Floors and Ceilings
- ✓ Electrical Surge Protectors
- ✓ Uninterrupted Power Supply (UPS) / Generator
- ✓ Emergency Power-Off Switch
- ✓ Power Leads from Two Substations
- ✓ Wiring Placed in Electrical Panels and Conduit
- ✓ Prohibition Against Eating, Drinking and Smoking
- ✓ Fire Resistant Office Materials
- ✓ Documented and Tested Emergency Evacuation Plans

# Water Detectors

- ✓ Water detectors should be placed under the raised floor and near drain holes, even if the computer room is on a high floor (remember water leaks).
- ✓ Any unattended equipment storage facilities should also have water detectors.
- ✓ On hearing the alarm, specific individuals should be allocated responsibility for investigating the cause and initiating remedial action.

# Hand-Held Fire Extinguishers

- ✓ Fire extinguishers should be in strategic locations throughout the facility.
- ✓ They should be tagged for inspection and inspected at least annually.

# Manual Fire Alarms

- ✓ Hand-pull fire alarms should be strategically placed throughout the facility.
- ✓ The resulting audible alarm should be linked to a monitored guard station.

# Smoke Detectors

- ✓ Smoke detectors should be above and below the ceiling tiles throughout the facilities and below the raised computer room floor.
- ✓ The detectors should produce an audible alarm when activated and be linked to a monitored station (preferably by the fire department).
- ✓ Smoke detectors should supplement, not replace, fire suppression systems.

# Fire Suppression Systems I

- These systems are designed to automatically activate immediately after detection of high heat typically generated by fire.
- The system should also be inspected and tested annually. Testing intervals should comply with industry and insurance standards and guidelines.
- Ideally, the system should automatically trigger other mechanisms to localize the fire. E.g.
  - Closing fire doors
  - Notifying the fire department
  - Closing off ventilation ducts
  - Shutting down nonessential electrical equipment.

# Fire Suppression Systems II

- Water-based systems
  - Referred to as sprinkler systems. These systems are effective but also are unpopular because they damage equipment and property.
  - The system can be dry pipe or charged (wet pipe)
  - A charged system is more reliable but has the disadvantage of exposing the facility to expensive water damage if the pipes leak or break.
  - Dry pipe systems have the advantage that any failure in the pipe will not result in water leaking into sensitive equipment from above.
- Since water and electricity do not mix, these systems must be combined with an automatic switch to shut down the electricity supply to the area protected.

# Fire Suppression Systems III

- Halon is
  - an inert gas which does no damage to equipment.
  - There should be an audible alarm and brief delay before discharge to permit personnel time to evacuate the area or to override and disconnect the system.
  - Halon adversely effects the ozone layer.
- Carbon Dioxide ($CO_2$) systems
  - Release pressurized carbon dioxide gas into the area protected to replace the oxygen required for combustion.
  - Unlike halon, however, $CO_2$ is unable to sustain human life.
  - Because of this, these systems are usually manually discharged, introducing additional delay

# Strategically Locating the Computer Room

- ✓ Not be located in the basement (Flood Damage)
- ✓ Best location for the computer room to reduce the risk of fire, smoke and water damage is on the 3rd, 4th, 5th or 6th floor.
- ✓ The activity of neighboring organizations should be considered when establishing a computer facility.
- ✓ Locations adjacent to or on the final path to an airport, next to a chemical works where explosive gases may be present, etc. should be avoided.

# Regular Inspection by Fire Department

- ✓ The fire department should inspect the system and facilities annually.
- ✓ Fire department should be notified of the location of the computer room so it can be prepared with equipment appropriate for electrical fires.

# Fireproof Walls, Floors and Ceilings

- ✓ Walls surrounding the information processing facility should contain or block fire from spreading.
- ✓ The surrounding walls should have at least a two-hour fire resistance rating.

# Electrical Surge Protectors

- ✓ These electrical devices reduce the risk of damage to equipment due to power spikes.
- ✓ Voltage regulators measure the incoming electrical current and either increase or decrease the charge to ensure a consistent current.
- ✓ Such protectors are typically built into the uninterruptible power supply (UPS) system.

# Generator and UPS

- ✓ Battery and/or petrol/diesel-driven generator.
- ✓ The system typically cleanses the power to ensure wattage into the computer is consistent.
- ✓ A UPS system can be built into a computer or can be an external piece of equipment.

# Emergency Power-Off Switch

- There may be a need to immediately shut off power to the computer and peripheral devices, such as during a computer room fire or emergency evacuation.
- Two emergency power-off switches should serve this purpose, one in the computer room, the other near, but outside, the computer room.
- The switches should be shielded to prevent accidental activation

# Power Leads from Two Substations

- ✓ Electrical power lines that feed into the facility are exposed to many environmental hazards water, fire, lightning, cutting due to careless digging, ete.
- ✓ To reduce the risk of a power failure due to these events that, for the most part, redundant power lines should feed into the facility.

# Wiring Placed in Electrical Panels and Conduit

- ✓ To reduce the risk of a fire occurring and spreading, wiring should be placed in fire-resistant panels and conduit.
- ✓ This conduit generally lies under the fire-resistant raised computer room floor.

# Prohibition Against Eating, Drinking etc.

- ✓ Food, drink and tobacco use can cause fires, buildup of contaminants or damage to sensitive equipment (especially in the case of liquids).
- ✓ They should be prohibited from the information processing facility.
- ✓ This prohibition should be overt, for example, a sign on the entry door.

# Fire Resistant Office Materials

- ✓ Wastebaskets, curtains, desks, cabinets and other general office materials in the information processing facility should be fire resistant.
- ✓ Cleaning fluids for desktops, console screens and other office furniture/fixtures should not be flammable.

# Emergency Evacuation Plans

- ✓ Evacuation plans should emphasize human safety, but should not leave information processing facilities physically unsecured.
- ✓ Procedures should exist for a controlled shutdown of the computer in an emergency situation, if time permits.

# Auditing Environmental Controls I

- Water and Smoke Detectors
  - Visually verify their presence
- Hand-Held Fire Extinguishers
  - Visually verify their presence and all have been inspected within the last year.
- Fire Suppression Systems
  - Fire suppression systems are expensive to test
  - Review documentation to ensure the system has been inspected and tested within the last year.

# Auditing Environmental Controls II

- Regular Inspection by Fire Department
  - Inquire and obtain a copy of the report, if any
- Fireproof Walls, Floors and Ceilings Surrounding the Computer Room
  - Locate the documentation that identifies the fire rating of the walls surrounding the information processing facility. two-hour fire resistance rating.

# Auditing Environmental Controls III

- ✓ Electrical Surge Protectors
  - Visually observe
- ✓ Power Leads From Two Substations
  - Locate documentation concerning the use and placement of redundant power lines into the information processing facility.
- ✓ Fully Documented and Tested Business Continuity Plan
  - As per Module 6

# Auditing Environmental Controls IV

- ✓ Wiring Places in Electrical Panels and Conduit
  - Visually verify that wiring in the information processing facility is placed in fire-resistant panels and conduct.
- ✓ UPS/Geneator
  - When last tested and review test reports.

# Auditing Environmental Controls V

- Documented and Tested Emergency Evacuation Plans
  - Obtain a copy of the Emergency Evacuation Plan.
  - Determine if it prescribes how to leave the information processing facilities in an organized manner that does not leave the facilities physically unsecured.
  - Interview a sample of IS employees and determine if they are familiar with the documented plan.
  - Verify whether the emergency evacuation plans are posted throughout the facilities.

# Auditing Environmental Controls VI

- Humidity/Temperature Control
  - Visit the IPF on regular intervals and physically determine if temperature and humidity are adequate.
- The testing procedures noted above should also be applied to any off-site storage and processing facilities.

# Micellaneous

# Processing Controls(RW- CH13 )

- ✓ Processor
  - Error Detection and Correction
    - ★ RAM to CPU: Parity
  - Multiple Execution States
    - ★ Supervisor state and Problem State
  - Timer Controls
    - ★ Infinite Loop
  - Component Replication
    - ★ Multicomputer and Multiprocessor
- ✓ Real Memory Controls
  - ★ Parity(Error D&C), Boundary Register(Access Control)
- ✓ Virtual Memory Controls
  - ★ Boundary(Displacement), Address Translation Table

# Thank You

Mathew A Thomas
mat@vsnl.com