Classification on the basis of Nature of Information System resources

Environmental Controls:- are controls related to IT environment such as power, air conditioning, Un-Interrupted Power Supply (UPS) smoke detection, fire-extinguishers, dehumidifiers

Environmental Issues and exposure :- mainly due to elements of nature. However with proper controls, exposures can be reduced E.g. Fire, Earthquake, volcano

Classification of the IS Resources from the perspective of environmental exposures and controls

- *Hardware and Media* –Computing equipment, storage media
- *Information System Supporting Infrastructure or Facilities:-*Physical premises like computer rooms, cabins, server rooms
- *Documentation:-*Physical and geographical documentation of computing facilities
- *Supplies:-*Third party maintenance procedures like air conditioning, fire safety. etc.
- *People* :- People are to be made responsible for environmental controls in their environment

Controls for Environmental Exposures

Environmental Exposures	Controls
Fire Damage	• Automatic and Manual Fire alarm placed at strategic locations • Manual fire extinguishers at strategic locations • Fireproof Walls • Fire Exits to be clearly marked • All staff members to be made aware as to how to use the system • Less wood and plastic in computer rooms • Use a gas based fire suppression system • Regular Inspection by fire department
Power Spikes	• Electrical surge protectors built into UPS • UPS Generator-backup power • Voltage Regulators and Circuit Breakers • Emergency Power off Switch
Water Damage	• Water Detectors to be placed under raised floor • Locating Computer room at place other than the basement or ground floor of multi-storeyed building • Other ways – Waterproof ceilings, Proper drainage, Alarms at Strategic points, Water proofing and leakage alarms
Pollution Damage and Others	• Major pollutant in computer installation is dust • Relocation Plans to emphasise on human safety • Redundant power links to be fed into the facility to

	prevent the losses from environmental damages from electric lines • Prohibit eating, drinking and smoking within the information processing facility

Physical Access Controls

Controls designed or related to the physical security of the

- Tangible IS Resources and
- Intangible resources stored on tangible media

Eg: - Access Control doors, Security guards, door alarms, CCTV Monitoring etc.

Results due so accidental or intentional violation of access paths

- Abuse of Data processing resources
- Blackmail
- Embezzlement
- Damage, vandalism or theft to equipments and documents
- Public disclosure of sensitive information
- Unauthorised entry

Possible perpetrators may be **employees** due to

Accidental ignorant-Someone who violates the rules	Addicted to a substance or gambling
Discontented	Experiencing financial or emotional problems
Former employee	Interested or informed outsiders
Notified for their termination	Threatened by disciplinary action or dismissal

Controls for Physical Access Exposures

Physical access controls are designed to protect the organisation from unauthorised access or illegal entry. Some of the more common access control techniques are discussed as follows:-

Locks on doors

- Cipher Locks :- Used in low security situations or when large number of entry and exits must be usable all the time .To enter a person presses a four digit number and door will unlock for a predetermined

Bolting Door Locks :-Special metal key is used to gain entry when the lock is a bolting door lock

Electronic Door Lock:- Magnetic or embedded chip-based plastic card keys may be entered into a reader to gain access in these systems

Biometric Door Locks:- Locks are secure with the individual's unique body features activating them

Advantages of Electronic Door Lock over bolting and combinational keys

- Special Internal code, cards can be made to identify the individual
- Individual access can be restricted through internal code and sensor devices
- Degree of Duplication is reduced
- Card entry can be deactivated of the employee is terminated or the card is lost or stolen

Physical Identification Medium

Personal Identification Numbers (PIN):- A secret number will be assigned to the individual, serves to verify the authenticity of the individual. Visitor has card to be inserted and PIN

*Plastic Cards:-*Cards are used for identification purposes

*Identification Badges:-*With varying colours for the badges, special identification badges can be issued to personnel as well as visitors

Logging on Facilities

Manual Logging:- All visitors to be prompted to sign a visitors log indicating the name, company represented, purpose of visit and person to see

Electronic Logging:-Combination of electronic and biometric security systems. Users logging can be monitored and unsuccessful attempts can be monitored

Other Means of Controlling Physical Access

Video Cameras: - Place at specific locations and monitored by security guards

Security Guards: - Appoint guards added with CCTV

Controlled visitor access: - Responsible employee to escort all visitors

Bonded Personnel:- All service contract personnel like cleaning people to sign a bond

Dead Man Doors:- Pair of doors seen at entrances, First door to close and lock for the second door to operate

LOGICAL ACCESS CONTROLS

Controls relating to logical access to information resources such as operating system controls, application software boundary controls, networking controls, access to database objects, encryption controls, etc.

Logical access paths are

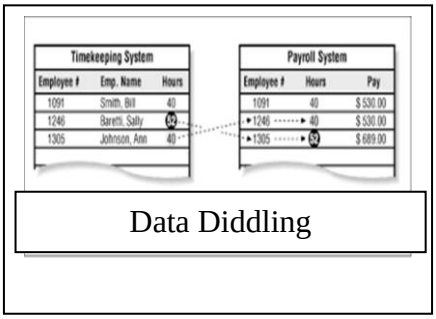
- Online Terminals
- Dial-up Ports
- Telecommunications Network

Logical access issues and exposures

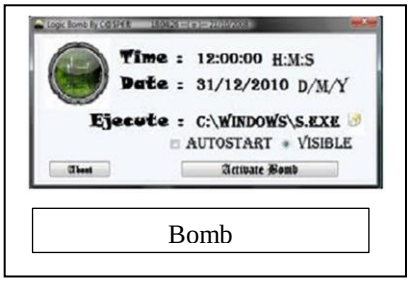
Access control mechanisms to be applied not only to computer operators but also to end user programmers or any authorised users. Intentional or accidental exposures of logical access control encourages technical exposures and computer crimes which are as follows:-

Technical Exposures:- include the following

Data Diddling	Altering the raw data just before a computer processes it and then changing it back once the processing is completed
Bomb	Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met
Trojan Horse	Trojan malware takes its name from the classical story of the Trojan horse, because it imitates the technique to infect computers. A Trojan will hide within seemingly harmless programs, or will try to trick you into installing it.
Worm	A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.
Rounding down	Refers to rounding off a denomination and transferring the same to an authorised account
Salami Technique	In information security, a **salami attack** is a series of minor attacks that together result in a larger attack. An example of salami slicing, also known as penny shaving, is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to the nearest cent in financial transactions. It would be done by always rounding down, and putting the fractions of a cent into another account. The idea is to make the



Data Diddling



Bomb

	change small enough that any single transaction will go undetected.
Trap Doors	Trap doors, also referred to as backdoors, are bits of code embedded in programs by the programmer(s) to quickly gain access at a later time, often during the testing or debugging phase

Computer Crime Exposures

Computer Crime exposures generally result in loss of customers and also embarrassment to management and legal action against the organisations. These are

Financial Loss	Loss of Electronic Funds
Legal Repercussions	Many laws to adhere and organisations will be exposed to lawsuits from investors and insurers if no proper security measures are present
Loss of Credibility or Competitive Edge	Security violation would result in the loss of business and prestige
Blackmail/Industrial Espionage	A Perpetrator can obtain money from organisation by exploiting the security violation
Disclosure of Confidential, Sensitive or embarrassing information	Legal or regulatory actions may happen against the company as a result of the disclosure
Sabotage	People not interested in financial gain but want to spoil the image of the company involve in such activities
Spoofing	Involves forging one's source address and it occurs only from vulnerable systems

Asynchronous attacks

- Numerous data that is getting transmitted must wait for the clearance of the line before the data is being transmitted. Such data is liable for unauthorised access
    - Data Leakage:- Leaking information out of computer from computer reports and tape
    - Subversive threats:- Intruder attempts to violate the integrity of some components in the sub-system
    - Wire Tapping:- Spying on information being transmitted over telecommunication network
    - Piggybacking:-Involves intercepting the communication between the operating system and the user and modifying them or substituting new messages
    - Denial of Service: - is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Logical access violators

These are people who exploit the physical exposures. They are mainly

Hackers, Employees, IS Personnel, former employee, end users

Logical Access Controls

- **User Access Management:-**
  - **User Registration:-**Information about every user is documented.
  - **Privilege Management**:-Access Privileges to be aligned with job requirements and responsibilities
  - **User Password Management**:-Educating users and making them responsible for their password
  - **Review of user access rights**:-User needs to access information changes with time
- **User Responsibilities**
  - **Password use:-** Mandatory use of strong passwords
  - **Unattended user equipment:-** None of the equipments under responsibility of user remains unprotected
- **Network Access Control**
  - **Policy on the use of network services:-**Selection of the appropriate services and approval to access them should be a part of the policy
  - **Enforced path:-** Specify the exact path for connecting the networks
  - **Segregation of Networks:-** Sensitive information network to be isolated from the internet usage service
  - **Network connection and routing control:-** Traffic between networks to be restricted
  - **Security of Network Services:-**Authentication and Authorisation policy should be implemented across the organisation's network
  - **Firewall:-**Organisations connected to internet and intranet have to implement a firewall to check intrusion
  - **Encryption:-** Conversion of data into secret code for storage in databases and transmission over networks
  - **Call Back Devices :-** it is a system used for protecting a computer network, in which a user calls into a computer, which checks the person's username and password, ends the call, and then calls back the number connected with that username and password.
  - **Recording of Transaction Log:-**All incoming and outgoing requests to be recorded in a transaction log
- **Operating System Access Control**
  - **Automated Terminal identification:-** A particular session could be initiated only from a particular terminal

  - **Terminal Log in Procedure:**-Entering the correct user id and password will provide the access to the user and entering incorrect information, after specific attempts, should lock the user from the system
  - **Access token:**- In case the login attempt is successful, Operating System creates an access token that contains key information about the user including the user id and password
  - **Access Control List:**- List contains information that defines the access privileges of all valid users
  - **Discretionary access control:**- System administrator determines who is to be provided what access and maintains access control list
  - **User identification and authentication:**- Depending on the risks, more measures like Biometric authentication and cryptographic means like Digital Certificates to be employed
  - **Password Management System:**- Operating system to enforce the selection of good passwords
  - **Use of system utilities:**- These help to manage critical functions of the operating system
  - **Duress alarm to safeguard users:**- Users are forced to execute instructions under threat, then the system must provide a means to alert the authorities
  - **Terminal time out:**- Log out the user if it is inactive for a certain period
  - **Limitation of connection time:**- Define the time slot. Not allow transactions before or after this time
- **Application and Monitoring the System Access Control**
  - **Information Access Restriction:-** User is allowed to access only information which he is authorised to access – Read, write and execute
  - **Sensitive system isolation:**-Considering Criticality, it may be even necessary to run system in isolation
  - **Event Logging:**- Maintain logs for all events. All incoming and outgoing requests along with attempted access to be recorded in transaction log
  - **Monitor system use:**-Constant monitoring of systems is essential
  - **Clock synchronisation:**- Event logs play an important role and therefore synchronising the time clock across the network as per standard time is mandatory
- **Mobile Computing**
  - **Theft of** Data carried on the disk drives of portable computers is a high risk factor

CLASSIFICATION ON THE BASIS OF AUDIT FUNCTIONS

- **Managerial Controls**
- **Application Controls**

Managerial Controls

Controls over the managerial controls- to be performed to ensure the development, implementation, operation and maintenance of information systems in a planned and controlled manner. Controls at this level include

Top Management:- Information system function us well managed

*Information System Managem*ent:- Planning and control of the information system activities

System Development Management:- responsible for the design, implementation and maintenance of application systems

Programming Management:- Programming new system, maintain old system and providing support software

Data Administration:- Addressing Planning and control issues in relation to the use of the organisation data

Quality Assurance Management:- Ensuring information system development, implementation, operation and maintenance confirm to established quality standards

Security Administration:- Responsible for access controls and physical security

Operations Management: - Planning and control of the day to day operations of information systems

Application Controls

Objective of these controls is to ensure that the data remains complete, accurate and valid during its input, update and storage

Categories of Controls

Boundary:- Comprises the components establishing interface between user and the system

*Input:-*Components capturing, preparing and entering commands and data into system

*Communication:-*Transmit data among subsystems

Processing:- Components that perform decision making, computation and classification

*Database:-*Components that define, add, access, modify and delete data in the system

Output:- Components that retrieve and present data to the users of the system