MIS 131: Information Systems Administration

Part V: IT Security

Section A: Controls

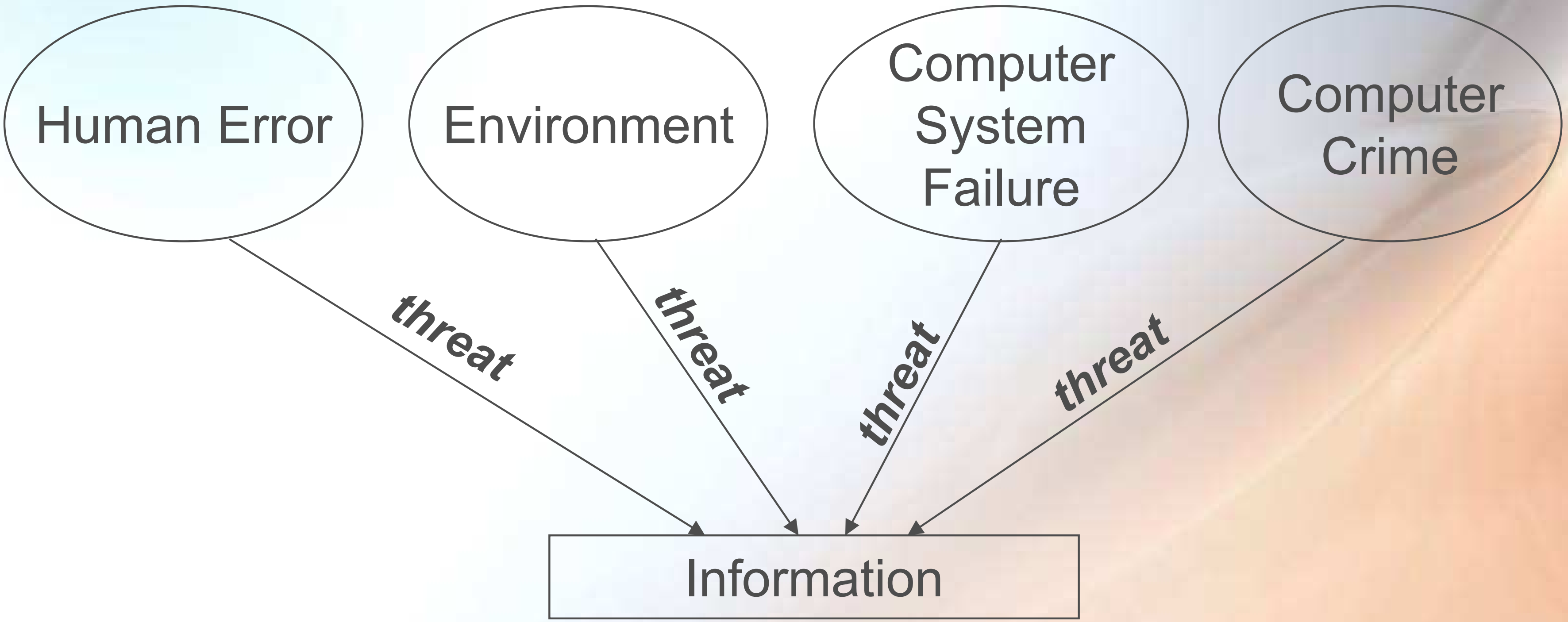
The Importance of Security

- The main purpose of computer operations is to ensure that the organization is provided with information that is
  - Accurate
  - Timely
  - Relevant
  - Reliable
  - Sufficient

The Importance of Security

- However, the achievement of those objectives are hampered by numerous threats such as
  - System failure
  - Poor system design
  - Insufficient and/or inaccurate data
  - Tampering of data (data diddling)
  - Viruses, worms, Trojan horses
  - Hackers and crackers
  - Fire, smoke, earthquake
  - Fraud (e.g. embezzlement)
  - Internal/external sabotage
- In short: “Acts of God and Acts of Man”

The Importance of Security



Human Error

Environment

Computer System Failure

Computer Crime

threat

threat

threat

threat

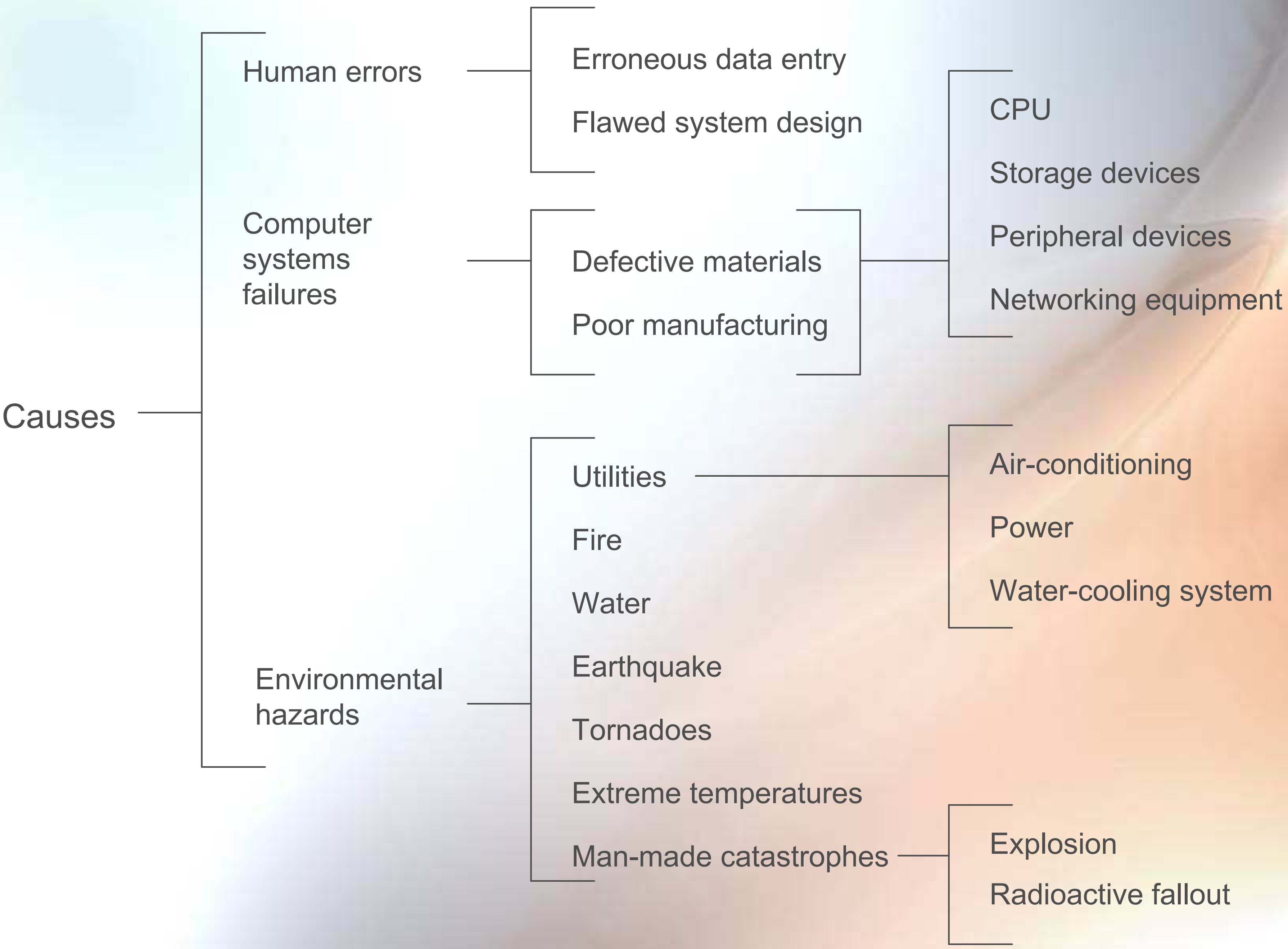
Information

- Hence, IT security is *essential* to counter the above threats

Types of Threats

- Unintentional
  - Human errors: contribute to vast majority (about 55%) of security-related problems
  - Environmental hazards
  - Computer systems failures
- Intentional
  - Computer crimes

Unintentional Threats to Security



- Causes
  - Human errors
    - Erroneous data entry
    - Flawed system design
  - Computer systems failures
    - Defective materials
    - Poor manufacturing
      - CPU
      - Storage devices
      - Peripheral devices
      - Networking equipment
  - Environmental hazards
    - Utilities
      - Air-conditioning
      - Power
      - Water-cooling system
    - Fire
    - Water
    - Earthquake
    - Tornadoes
    - Extreme temperatures
    - Man-made catastrophes
      - Explosion
      - Radioactive fallout

Intentional Threat = Computer Crime

- Computer as *target* of the crime
  - Example: The actual hardware may be stolen or destroyed
- Computer as *medium* or *tool* of attack
  - Example: Computer may be used to embezzle money
- Computer can be used to *intimidate* or *deceive*
  - Example: Stockbroker stole money by convincing clients of a software which will increase ROI by 60% per month

Defense Strategy and Its Objectives

- Selection of a specific defense strategy depends on objective of defense and perceived cost-benefit
- Major objectives
  - Prevention and deterrence
  - Detection
  - Limitation of damage
  - Recovery
  - Correction
  - Awareness and compliance

Controls

- Provide means of protecting IT
- Integrated during systems development
- Implemented once system is in operation
- Meant to protect all components of the system
  - Hardware
  - Software
  - Data
  - Network

The Challenge of Controls

To balance

- the need of the organization for information to assist in decision making

with

- the need to protect this information to ensure that it meet the organization's requirements

Characteristics of Good Controls

- Complete
- Effective
- Timely

Major Categories of Controls

- General controls
  - Established to protect the system regardless of the specific application
- Application controls
  - Safeguards intended to protect specific applications

Categories of General Controls

- Physical controls
  - Protection of computer facilities and resources
- Access controls
  - Restriction of unauthorized user access to a portion of a computer system or the entire system
- Data security controls
  - Protection of data from intentional or accidental disclosure or from unauthorized modification or destruction

Categories of General Controls

- Communications and network controls
  - Protection of network components due to the internet and proliferation of e-commerce
- Administrative controls
  - Deal with issuing guidelines and monitoring compliance with the guidelines

Physical Controls

- Prevention of physical damage due to natural and unnatural disasters such as
  - Earthquakes
  - Floods
  - Fire
  - Physical attack on the computer

Example of Physical Controls

- Against fire
  - Sprinkler system
  - Use of gas-based fire suppressants
- Against power outages
  - Use of uninterruptible power supply (UPS) preferably intelligent ones for servers
- Against lightning and other induced currents
  - Lightning rods
  - Surge protection for both power and network cables
  - Metal conduits for UTP cables especially those close to fluorescent lighting units and those located outside

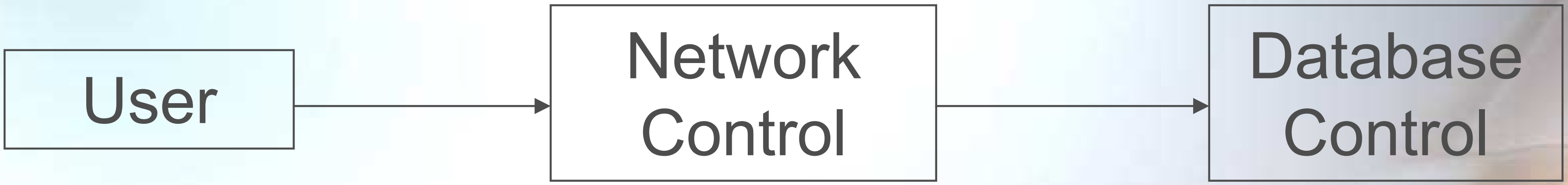
Access Controls

- Physical access to a terminal
  - Use of coded key entry, swipe card, biometric controls
- Logical access to the system
  - Firewalls
    - Allows only authorized traffic into the network
  - Network
    - Require network log-in (log-in name and passwords)
    - Password aging - password expires after some time
    - Password rotation - password must be replaced a number of times before re-using
    - Log-in control - account disabled after a number of consecutive unsuccessful log-ins
  - Database system log-in

Access Controls

- Access to specific system privileges
  - Based on user’s ID, limit which data can be accessed
  - Limit what can be done with data – read, update, delete, insert

A Two-Level Logical Access Model



- log-in
- password aging
- password rotation
- password control

- verifies user
- identifies network resources that user can access

- verifies user
- identify data that user can access
- identify what user can do

An Illustration of Access Controls

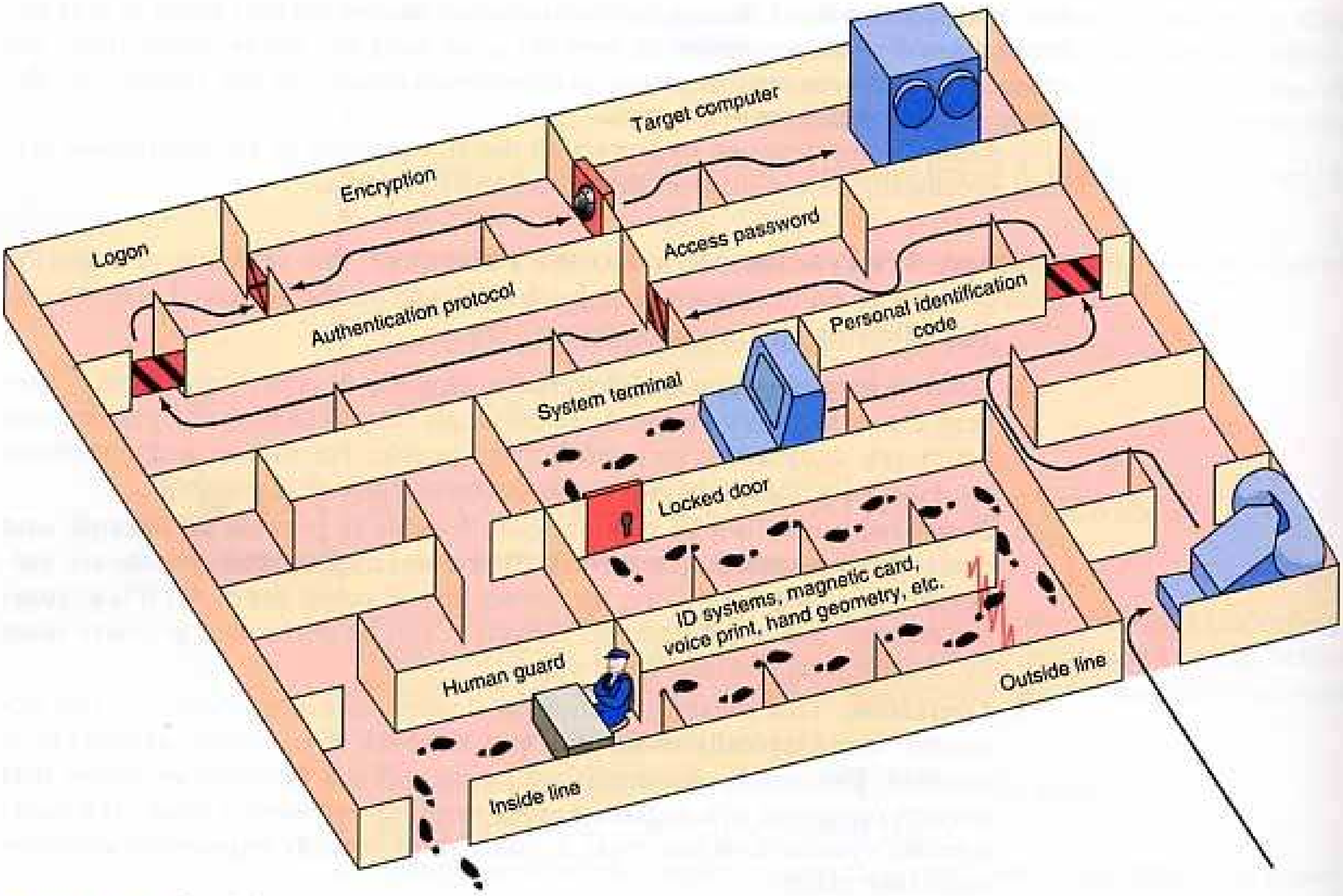


FIGURE 15.6 The defense. (*Source*: Joe Lertola.© 1983 *Discover* magazine.)

Data Security Controls

- Data security addresses the following
  - Confidentiality of data
  - Access control
  - Critical nature of data
  - Integrity of data
- Two basic principles should be reflected in data security
  - Minimal privilege
    - Ensures that only the required information is accessible to the user
  - Minimal exposure
    - Ensures that only those that require the information should obtain it

Network Controls

- **Ensure that the network will continue to operate at an acceptable level**
- **This topic will be discussed in detail later under the *Networks* section of the course**

Administrative Controls

- Deal with the issuance of guidelines and monitoring of their compliance
- Examples of administrative controls
  - Immediate revocation of access rights of terminated or resigned employees
  - Virus protection guidelines
  - Separation of duties – divide sensitive duties among as many as economically feasible to decrease chance of intentional/unintentional damage
  - Periodic audit of information systems
  - Fostering company loyalty
  - Insurance for key employees

Other General Controls

- Programming controls
- Documentation controls
- System development controls

Programming Controls

- Aim to reduce errors in programming
- Causes include use of incorrect algorithm, carelessness, inadequate testing and configuration management, etc.
- Example of programming controls
  - Training
  - Establishing standards for testing and configuration management
  - Enforcing documentation standards

Documentation Controls

- Ensure that manuals are easy to read and understand and always up-to-date
- Appropriate documentation controls include accurate writing, standardization updating, testing, etc.
- Use of CASE tools to document system

Documentation Controls

- Most common systems documents
  - System standards
  - Program specifications and actual code documentation
  - Data and database documentation
  - Operations manual
  - User’s manual
  - Training manual
  - Conceptual, logical, and physical ERD

System Development Controls

- Ensure that a system is developed according to established policies and procedures
- Conformity with budget, timing, security measures, and quality as well as documentation requirements must be maintained

Application Controls

- Controls built into applications and are usually written as validation rules
- Ensure that all transactions are accurately recorded, classified, processed, and reported
- Subdivided into
  - Input controls
  - Processing controls
  - Output controls

Input Controls

- Designed to prevent data alterations or loss
- Very important because they prevent “garbage-in, garbage-out” situations
- Categories of input controls
  - Recording of transactions
  - Batching of transaction data
  - Conversion of transaction data
  - Editing of transaction data
  - Transmission of transaction data

Recording of Transactions

- Manual forms
  - Use well-structured, pre-numbered source documents
  - Provide space for necessary authorizations
  - Ensure blank forms are controlled and kept safe, preferably under lock and key
- Online forms
  - Use pre-formatted, menu-driven screens
  - Use standard readers (e.g. bar-code) to reduce input errors
  - Provide feedback mechanisms to approve transactions

Batching of Transaction Data

- Batch control totals help prevent data loss and erroneous posting of transactions
  - Amount control totals
  - Hash totals
  - Record count
- Use of batch control logs for batch number and totals

Conversion of Transaction Data

- Data conversion by keying, scanning, or copying from one source document to another
- All converted data must be verified either visually or by key verification

Editing of Transaction Data

- Use of edit tests (program validation routines) to compare incoming data with a standard
- Examples include:
  - Self-checking digit (check digit)
  - Range check
  - Limit check or reasonableness check
  - Format or data type check
  - Dependency or relationship check

Transmission of Transaction Data

- When data must be transmitted from point of origin to the processing center through data communications facilities, the following must be considered
  - Echo check
    - Sending data back to originating terminal for comparison with transmitted
  - Redundancy data check
    - Transmitting additional data to aid in verification process
  - Completeness check
    - Verifying that all required data have been entered and transmitted

Processing Controls

- Ensure that data are complete, valid, and accurate when being processed and that programs have been properly executed
- Examples of processing controls
  - Manual cross-checks
  - Processing logic checks
  - Run-to-run totals
  - File and program changes
  - Audit trail linkages

Output Controls

- Ensure that the results of computer processing are accurate, valid, complete and consistent
- Examples of output controls
  - Review of processing results
  - Controlled distribution of outputs