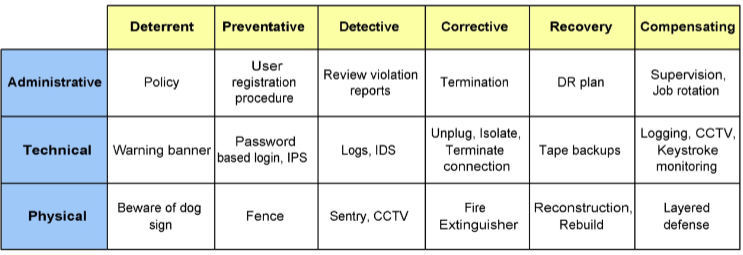
**EXAM 2 MATERIAL:**

**Module 16 – Introduction to Access Controls:**

* Access Controls: A collection of mechanisms that work together to protect the assets of the enterprise.
  + Purpose: Access controls help protect against threats and vulnerabilities
  + Access controls enable management to:
    - Specify which users can access the system
    - Specify what resources they can access
    - Specify what operations they can perform
    - Provide individual accountability
* Principles:
  + Separation of Duties:
    - Define elements of a process or work function
    - Divide elements among different functions
  + Least Privilege: Limit users and processes to access only resources necessary to perform assigned functions.
* Environment: Includes all aspects and levels of an organization
  + Facilities
  + Support systems
  + Information systems
  + Personnel: Management, users, customers, business partners etc.

**Module 17 – Access Control Categories & Types:**

* Control Categories:
  + Deterrent: Discourage incident
  + Preventive: Avoid incident
  + Detective: Identify incident
  + Corrective: Remedy circumstance / mitigate damage; restore controls.
  + Compensating: Alternative control (e.g., Supervision)
  + Recovery: Restore conditions to normal
* Types of Controls:
  + Administrative: Policies and procedures, including personnel controls such as security clearances, background checks.
  + Technical (Logical): Anti-virus software, password protection, firewalls, auditing.
  + Physical: Locks, alarms, badge systems.
* Control Examples:



**Module 18 – Access Control Threats:**

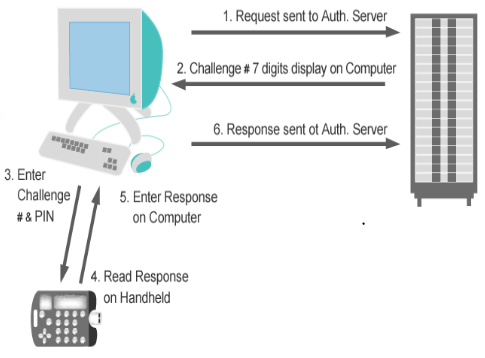
* Threats Related to Access Control: Denial of Service, Buffer Overflows, Mobile Code, etc.
  + Malicious Software: Viruses, Worms, Trojan Horses, Logic Bombs, Password Crackers, Sniffers, Backdoor/Trapdoor
  + Other Threats: Spoofing/Masquerading, Eavesdropping, Emanations, Shoulder Surfing, Tapping, Object Reuse, Data Remanence, Unauthorized Targeted Data Mining, Dumpster Diving, Theft, Intruders, and Social Engineering.
* Social Engineering: Uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.
  + Techniques: Phone conversations, shoulder surfing, dumpster diving, phishing, etc.
* Social Engineer: Someone who uses deception, influence, and persuasion, against business or individuals, usually targeting their information.

**Module 19 – Access Control Systems:**

* Access Control Services: A system that provides these services
  + Identification: Asserts user/process identity (unique)
    - Provides accountability (with protected audit trail) - traces activities to individuals and holds users responsible for actions
    - Types of Identification:
      * Most common for system users is a user identification (UserID) such as the username, account number, or Personal Identification Number (PIN)
      * Badge system
      * Biometric Devices: Can be used for both identification and authentication
    - User Identification Guidelines:
      * Unique: Not shared to ensure accountability
      * Standard naming convention
      * Non-descriptive of job function
      * Secure and documented process for issuance
  + Authentication: Verifies who the user is and whether access is allowed.
    - Types of Authentication:
      * Authentication by Knowledge: What a person *knows*
        + Password: Standard form of authentication
        + Passphrase: Used as an alternative to a password. They are longer to enter and usually harder to crack.
        + Password Encryption Schemes: Stored passwords are *not* in clear text; *limits* physical access to servers that store passwords/passphrases.
      * Authentication by Ownership: What a person *has*
        + One-Time Passwords: Changed after every use (*dynamic*); usually *token* or *hardware* based; generated by a token, often in conjunction with a pin or other secret.

Generation Methods:

Asynchronous: Challenge-response scheme; based on one-time pad



Synchronous: Event, Location or Time-Based synchronization; Authentication Server knows the expected value from the token and the user must input it or be in close proximity.

* + - * Authentication by Characteristic: What a person *is/does*
        + Biometric Devices: The individual’s identity is confirmed by either…

Physiological Trait: Fingerprint, retina, iris (something *unique*)

Behavioral Characteristic: Keystroke, signature or pattern.

* + - * + Important Elements of Biometric Devices:

Accuracy: Separate authentic users from imposters

Processing Speed: How fast the accept or reject decision is determined

User Acceptability

Protection of biometric data

* + - * + Types of Biometric Devices: Fingerprint, Hand Geometry, Palm Scan, Voice Pattern, Retina Pattern/Scan, Iris Pattern/Recognition, Signature Dynamics, Facial Recognition, and Keystroke Dynamics.
  + Authorization: What the user is allowed to do
  + Accountability: Tracks what the user did and when it was done

**Module 20 – Identity Management:**

* Need: A convergence of business drivers has stretched the capabilities of existing security infrastructures.
  + Potential Negative Impacts:
    - Loss of business productivity
    - Long deployment cycles adversely affecting business productivity
    - Increasing number of access points creating more potential breach points
    - Increasing number of single point of failures
  + Dissatisfaction of employees, customers, and partners resulting from their need to maintain an excessive number of user IDs (8 to 12 IDs)
  + Inability to evaluate regulatory compliance due to lack of properly identified user populations and their association to resources
  + Weaknesses in security routinely identified during audits as a result of disparate and inefficient administrative processes
* Challenges:
  + Different types of principles – outsiders and insiders.
  + Different kinds of identity data:
    - Personal information
    - Legal information
    - Login credentials to managed systems
  + Identity Life Cycle: Initial setup, change and maintenance, tear-down.
  + Key Identity Management Challenges: Consistency, efficiency, usability, reliability, and scalability.

**Module 21 – Access Control Technologies:**

* Identity Management Technologies: Systems focus on streamlining the identity management process and managing data consistently across multiple systems.
  + Technologies:
    - Directories:
      * Centralize management of data
        + Users
        + Other objects in the enterprise, such as user groups, servers, printers, etc.
      * Store data on one or more directory servers.
      * Provide data access
        + Using client applications
        + Normally through standard protocols, such as LDAP (Lightweight Directory Access Protocol), or X.500
      * Key Limitation: Integration with legacy systems.
      * Directory Services: Provides the means to hierarchically organize and manage information, and to retrieve the information by name association.
        + Network Directory Service: Contains a set of information about resources and services on the network, such as users, workstations, and servers; the directory service is used to simplify access and administration by providing a unified organization of the network resources.
    - Password Management: System to manage passwords consistently across multiple platforms.
      * Generally support the following features:
        + Synchronization of passwords among multiple systems.
        + Authentication of users who have forgotten passwords with some other means and then allow password resets.
        + Allowing IT support staff to authenticate callers for password management.
        + Permitting users to register for access.
    - Single Sign-On: Allows users to authenticate once to a central Single Sign-On system, which stores every user’s login ID and password to all supported applications
      * Applications are launched through Single Sign-On client software
      * Limited success in large production environments:
        + Deployment and integration costs are high.
        + Concerns about security (single point of failure/access).
        + Concerns about availability (system fails, access to all connected legacy systems also fail).
      * Pros:
        + Efficient log-on process
        + Users may create stronger passwords
        + No need for multiple passwords
        + Timeout and attempt thresholds enforced across entire platform
        + Centralized administration
      * Cons:
        + A compromised password allows intruder into all authorized resources.
        + Inclusion of unique platforms may be challenging.
    - Account Management:
      * Account Management Systems:
        + Provide for *timely* changes, additions and deletions of system access
        + Often *include* workflow processes
        + Centralized *management* facility
        + Integration with other systems – HR, corporate directory
        + For:

Legacy Systems

Network Operating System Mainframes

Database Servers

ERP Applications

* + - Profile Update: User identity normally includes *storing* personal information, such as name, phone numbers, email addresses, home address, etc.; profile update systems allow users to *enter* and *manage* those parts of their own profiles where new data is not sensitive or does not have to be validated.
    - Security Domains: Domain of trust that *shares* a single security policy and single management.
      * Access control parameters *in which* a program is operating (set of objects a subject can access).
      * Principle of Separation protects resources; resources encapsulated in distinct address spaces.
* Common Subsets of Subjects:
  + Hierarchical Domain Relationship:
    - Subjects can access objects in equal or lower domains
    - Domains of higher privilege protected from domains of lower privilege

**Module 22 – Data Access:**

* Types of Access Controls:
  + Discretionary Access Control: Owner determines who has access & what privileges they have.
  + Mandatory Access Control: Owner & system determine who has access
    - System decision based on privilege (clearance) of subject (user) & sensitivity (classification) of object (file)
    - Requires labeling
    - Based on the organization’s security policy
    - Puts limitations on authorizers
    - Used for systems that process *highly* sensitive data
    - Assign *sensitivity* labels to all objects and clearance labels to all subjects
    - Object’s sensitivity level and the subjects *clearance* level determine access
    - Permits processing of multiple levels on one system
* MAC vs. DAC:
  + Differences:
    - Discretionary Access Controls involve only the resource owner’s permission.
    - Mandatory Access Controls require the owner’s and system’s permission (based on labeling).
* Access Control Lists (ACLs):
  + Most common implementation of Discretionary Access Controls
  + Specifies a list of users who are allowed access to each object
  + Often implemented with Access Control Matrices
  + Access to ACL files should be protected
* Rule-Based Access Control:
  + Access is based on a *list of rules* that determine authorization.
  + System *owners* create or authorize the rules – specify privileges granted to users.
  + Mediation mechanism *enforces* the rules to ensure authorized access; intercepts every request, compares it to user authorizations, and makes decision.
* Role-Based Access Control:
  + Access control decisions are *based* on job function.
  + Each role (*job function*) will have its own access capabilities.
  + Access capabilities are *inherited* by users assigned a job function.
  + Determination of role is *discretionary* and is in compliance with security access control policy.
  + Groups of users need similar or identical privileges
    - Generally associated with DAC
    - Privileges appropriate to functional roles are assigned
      * Individual users are enrolled in appropriate roles
      * Privileges are inherited

**Module 23 – Auditing Access Control Systems:**

* Audit Trail Monitoring:
  + Audit Trail: A record of system activities.
  + Configuration: Capture data generated by system, network, application, and user activities.
  + Function:
    - Alert staff to suspicious activity for investigation.
    - Provide details on extent of intruder activity.
    - Provide information for legal proceedings.
* Audit Event Types:
  + Network connection event data
  + System-level event data
  + Application-level event data
  + User-level event data (Keystroke activity, etc.)
* Auditing Issues & Concerns:
  + Control the volume of data
    - Event filtering or clipping level determine the amount of log detail captured.
    - Auditing tools can reduce log size.
  + Establish procedures in advance.
  + *Train* personnel in pertinent log review.
  + Protect and ensure against unauthorized access.
    - Disabling auditing or deleting/clearing logs.
  + Protect the audit logs from unauthorized changes.
  + Store/archive audit logs securely.

**Module 24 – Introduction to Cryptography:**

* The cryptography domain addresses the principles, means, and methods of disguising information to ensure its confidentiality, integrity, authenticity and non-repudiation.
* Cryptography:
  + Art and science of writing secrets
  + Storing and transmitting information in a form that allows it to be revealed only to those intended.
  + Accomplished by cryptosystem.
* Definitions:
  + Plaintext/Cleartext: Data in unscrambled form
  + Ciphertext/Cryptogram: Scrambled data
  + Encipher/Encrypt/Encode: Act of scrambling using key
  + Decipher/Decrypt/Decode: Descrambling with key
  + Algorithm:
    - Set of rules by which enciphering and deciphering is done.
    - ‘Mathematical’ function that takes plaintext and a key as input, and produces ciphertext as output
  + Cryptanalysis:
    - Practice of defeating attempts to hide information.
    - Reduction or solution of secret messages without knowledge of the system or the key or the possession of a code book.
  + Cryptology: Includes both cryptography and cryptanalysis.
* Traditional & Modern Cryptography:
  + Cryptography originally used for secrecy
  + Now typically used for many applications such as:
    - Prevent unauthorized disclosure of information
    - Prevent unauthorized access to information, computers, web sites, applications, etc.
    - Detect tampering, injection of false data, deletion of data, etc.
    - Prevent repudiation
* Purpose of Cryptography:
  + Protect sensitive information from disclosure
  + Identify the corruption or unauthorized change of information
  + Make compromise too expensive or too time consuming
* Security Requirements E-mail Example:
  + Privacy: Only the intended recipient can read the message
  + Integrity: The message cannot have been changed
  + Authentication: We know the message is from who we expected it from.
  + Non-Repudiation: Originator cannot deny having sent a message.

**Module 25 – History of Cryptography: OMITTED**

**Module 26 – Stream and Block Ciphers:**

* Stream Ciphers:
  + Operate on *continuous* streams of plain text (as 1’s and 0’s).
  + Usually implemented in hardware.
  + Well suited for serial communications.
  + A stream cipher algorithm *should* have these features:
    - Long periods with no repeating
    - Functionally complex
    - Statistically unpredictable
    - Statistically unbiased keystream (as many 0’s as 1’s)
    - Keystream not linearly related to key
* Block Ciphers:
  + Operate on *fixed* size *blocks* of plain text
  + More suitably implemented in software to execute on general-purpose computer
  + Overlap when block operated as stream
  + Characteristics:
    - Operates on fixed size text blocks – usually 8-byte (64-bit) ASCII text in block ciphers with length a multiple of 8 bits
    - Block mode ciphers are generally slower than stream mode
    - Data Encryption Standard (DES) is best-known block cipher

**Module 27 – Encryption Systems:**

* Types of Encryption Systems:
  + Secret Writing
    - Steganography (hidden)
    - Cryptography (scrambled)
      * Transposition
      * Substitution: Code (replace words) & Cipher (replace letters)
  + Cryptographic Algorithms
    - Symmetric: Block & Stream
    - Asymmetric: Discrete Logarithm & Factorization
* Encryption Systems Subtopics:
  + Classical Substitution Ciphers:
    - Original Caesar Cipher:
      * Shift the alphabet (move letters 3 spaces)
      * *Scramble* the alphabet (substitute one letter for another)
  + Transposition (Permutation) Ciphers: Rearranges the letters
  + Polyalphabetic Ciphers: Uses several different alphabets to defeat frequency analysis
  + Running Key Cipher:
  + One-Time Pad:
  + Concealment Cipher: True letters of plaintext hidden/disguised by device or algorithm
  + Steganography: Art of *hiding* communications; deny the message exists while it is hidden in picture files, sound files, slack space on floppies, etc.
  + Codes: List of words/phrases (code) with corresponding random groups of numbers/letters (code groups)

**Module 28 – Types of Algorithms:**

* Symmetric Key Cryptography:
  + Symmetric Systems:
    - DES, Double DES (2DES), Triple DES (3DES)
    - AES / Rijndael
    - IDEA
    - RC4, RC5 / RC6
  + Also referred to as *private* key/*single* key/*secret* key
  + Uses a *single* key shared by originator and receiver
  + Algorithms Include: Rjindael, DES, Triple DES, Blowfish, IDEA, RC4, RC6, SAFER, Serpent, Twofish, etc.
  + Strengths:
    - Very *fast* which allows for large amounts of data to be encrypted in very little time
    - Very *difficult* to break data encrypted with large keys
    - Availability: Algorithms and tools used for symmetric encryption are freely available.
  + Weaknesses:
    - Key Management & Implementation: Ensure that sender and receiver can agree upon a key, and how they exchange a key.
    - Key Distribution:
      * Same key used to both encrypt and decrypt.
      * Requires very secure mechanism for key distribution.
      * Keys and data must be delivered separately.
    - Scalability: Since a unique key must be used between the sender and each recipient, number of keys grows exponentially with the number of users: N(N – 1) / 2
      * 10 users = 45 keys, 1000 users = 499,500 keys
    - Limited Security:
      * Symmetric keys only encrypt data and restrict its access.
      * Does not provide proof of origin or non-repudiation.

**Module 29 – Asymmetric Cryptography:**

* Asymmetric Key Cryptography:
  + Instead of a single key, there is a ‘key pair’.
  + The two keys are *related* to each other mathematically.
  + One of the keys is kept secret (*Private* key).
  + The other is made available to everyone (*Public* key).
  + *Computationally infeasible* to derive the private key from knowledge of the public key.
  + When data is encrypted with either one of the keys, the other key is the *only* one that can decrypt the ciphertext.
  + Strengths:
    - Provides efficient encryption and digital signature services
    - Efficient symmetric key distribution
    - Scalability: Only two keys needed per user – 1,000 people need total of 2,000 keys (easier to manage than the 499,500 needed for symmetric).
    - Can provide five security elements:
      * Confidentiality/Privacy: Data cannot be decrypted without the appropriate private key.
      * Access Control: The private key should be limited to one person.
      * Authentication: Identity of sender is confirmed.
      * Integrity: Data has not been tampered with.
      * Non-Repudiation: Sender cannot deny sending.
  + Weaknesses: Computationally intensive & slow (1000 or more times slower than symmetric)
  + Public key (asymmetric) systems are based on problems that are difficult to solve (hard problems):
    - Factoring the product of large prime integers
    - Discrete log problem (difficulty of taking logarithms in finite fields)
* One Way Function:
  + A mathematical function that is *easier* to compute in one direction (forward direction) than in the opposite direction (inverse direction).
  + Forward direction could take *seconds*, the inverse could take *months*.
  + ‘*Trap-door* one way function’ is a one way function for which the inverse direction is easy given a piece of information (the trap door).
  + Asymmetric key cryptography is based on ‘trap-door one way functions’…
    - Public Key: Gives info about the function.
    - Private Key: Gives info about the trap door.
    - Whoever knows the trap door can compute function easily in both directions.
    - Anyone lacking trap door can compute function in only one direction.
    - Forward direction used for encryption and signature verification.
    - Inverse direction used for decryption and signature generation.

**Module 30 – Hybrids & Hashes: OMITTED (MAYBE)**

**Module 31 – Digital Signatures:**

* Digital Signatures: Authentication tool to verify a message *origin and sender* identity.
  + Resolve authentication issues.
  + Block of data attached to message (document, file, record, etc.); binds message to individual whose signature can be verified by receiver or third party (difficult to forge).
  + Each user has public-private key pair – private key signs (creates signature), public key verifies it.
  + A digital signature is created by encrypting a digest or hash value of a message with the senders private key.
  + Operation: To “*sign*” a message.
    - Sender computes digest of message using public hash function
    - Crypto “signature” is made by sender’s private key – applied to digest creates digital signature.
    - Digital signature sent along with message.
    - The message itself is not made private.
    - To *verify* a message…
      * Receiver computes digest of received message
      * Decrypts the signature with the sender’s public key to extract the original sender’s digest
      * Verifies if the recomputed and decrypted digests match – signature decryption identifies sender and verifies integrity of the message.
  + Benefits:
    - Provides *non-*repudiation; ensures that the sender cannot deny sending the message; recipient cannot claim receiving a different message than the original.
    - Used to *authenticate* software, data, images, users, machines; protects software against viruses (Ex: A smart card with a digital signature can verify a user to a computer).

**Module 32 – Comprehensive Example: OMITTED**

**Module 33 – Physical Security:**

* Introduction: The physical security domain provides *protection* techniques for the *entire* facility, from the outside perimeter to the inside office space, including all of the information system *resources*.
* Physical Security: The physical measures & their associated procedures to safeguard & protect against damage, loss & theft.
  + Implementing controls that discourage attackers by convincing them that the cost of attacking is greater than the value received from the attack.
* Requirement: Safety of people is the primary concern.
* Goals:
  + Deter
  + Delay
  + Detect
  + Assess
  + Respond
* Physical Security Threats:
  + Unintentional:
    - Natural/Environmental (e.g., earthquakes, floods, storms, hurricanes, fires).
    - Utility Systems (e.g., communication outages, power outages).
    - Human-Made/Political Events (e.g., explosions, vandalism, theft, terrorist attacks, riots).
  + Intentional:
    - Theft: Internal/external results in increased costs
    - Espionage: Loss of intellectual property & market share
    - Dumpster Diving: Access to sensitive corporate information
    - Social Engineering: Intelligence attacks
    - Shoulder Surfing: Results in unauthorized access
    - HVAC: Access via HVAC vents
* Countermeasures:
  + Theft: IDs, locked doors and keys, and access controls.
  + Espionage: Employee tracking & job rotation with strict internal controls
  + Dumpster Diving: Layered defense system and a disposal policy
  + Social Engineering: Employee accountability & security awareness
  + Shoulder Surfing: Keyboard keystroke placement and awareness of your surroundings
  + HVAC Access: Narrow shafts and section lock downs

**Module 34 – Support Systems:**

* Support System Threats:
  + Fire: Damage & destruction of facilities/equipment
    - Best Practices: Fire Containment System (floors, vents, HVAC), Fire Extinguishing System (permanent & mobile), Abiding by the Fire Codes, Fire Prevention Training and Drills
    - Fire Prevention: Reduce causes of fire
    - Fire Detection: Receive warning of fire before it becomes a problem.
    - Fire Suppression: How to extinguish and contain a fire to minimize damage.
      * Water Sprinkler Systems:
        + Water could be a conductor of electricity – it may compound the problems in computer rooms.
        + Water can cause damage to electrical equipment.
        + “Pre-action” or “dry-pipe” system – water is held back by a valve and is released when the sensor activates.
  + Water: Flooding/dripping
    - Make sure water pipes are not located above server rooms
    - Water Detection Sensors: Raised floors, emergency Shut-Off valves, server room above ground level, etc.
  + Power Loss: Disruption/stop in operations
    - Disruptions in electrical power can have a *serious* business impact.
    - Goal is to have “clean and steady power”.
      * Dedicated feeders
      * Alternate power source
      * Access controls
      * Secure breaker and transformer rooms
    - Countermeasures: Surge suppressors, UPS and UPS Testing, Electrical Facilities separated from Data Center, Generators
    - Blackout: Prolonged loss of commercial power
    - Fault: Momentary loss of power
    - Brownout: Intentional reduction of voltage by the utility company for a prolonged period of time.
    - Sag/Dip: A short period of low voltage.
    - Surge: Sudden rise in voltage in the power supply.
  + Gas Leakage: Explosion
    - Identify the location and test the main Shut-Off valve
    - Secure the Natural Gas Line (using layered defenses)
    - Communicate Natural Gas Line Design to Fire Department
    - Clearly mark Shut-Off valves
  + HVAC: Overheating/overcooling
    - Best Practices: Temperature Controls Protection, Emergency Detection System, Auto Shutoff Mechanisms, Proper Maintenance

**Module 35 – Layered Defense Concepts Part 1:**

* Approaching security through ‘layers’ of controls; multi-layered.
* Starts with the perimeter, then building grounds, then building entry points, etc.
* Perimeter and Building Grounds Boundary Protection:
  + Perimeter security controls are the first line of defense.
    - Natural protective barriers offer terrains that are difficult to cross, such as mountains, bodies of water, deserts, etc.
    - Structural barriers are devices such as fences, gates, bollards, and facility walls.
  + Landscaping: Shrubs or trees can provide a barrier or an entry point; spiny shrubs make it harder for an intruder to cross the barrier.
  + Fences:
    - Are used to enclose security areas and designate property boundaries.
    - Should meet specific gauge and fabric specifications.
    - High-security areas may need a “top guard” (barbed wire at the top).
    - Should meet certain height and location provisions.
    - Fences must be checked and repaired on a regular basis.
    - Fence fabric must be securely attached to poles.
    - Be sure that vegetation or adjacent structures cannot provide a “bridge” over the fence.
  + Gates: The portions of a wall or fence system that control entrance and/or egress by persons or vehicles and complete the perimeter of the defined area.
  + Bollards: A rising post designed for use in traffic control and protecting property premises; provides security against vehicles ramming into, or stopping near buildings; lighted bollards can be used for lighting controls along parks, paths, sidewalks, etc.
  + Subtopics:
    - Perimeter Intrusion Detection Systems: Sensors that detect access into an area (Ex: Photoelectric, Ultrasonic, Microwave, Passive infrared (PIR), & Pressure-sensitive Systems).
    - Surveillance Devices: Closed-Circuit Television (CCTV)
      * A television transmission system that uses cameras to transmit pictures by a transmission medium to connected monitors.
      * The transmission media can use wired or wireless technologies.
      * CCTV Levels:
        + Detection: The ability to detect the presence of an object.
        + Recognition: The ability to determine the type of object.
        + Identification: The ability to determine the object details.
      * Lighting: The illumination of a locale, typically by artificial means such as light fixtures or lamps.
        + A consistent level of light supplying reasonably good visibility needs to be available.
        + Features: Good lighting is one of the most successful crime preventive measures; when used properly, light discourages unlawful activity, improves natural observation, and decreases fear; they are typically used with other controls, such as fences, patrols, alarm systems.
        + Types: Continuous Lighting (Glare projection lighting, flood lighting, etc.), trip lighting, standby lighting, & emergency lighting

**Module 36 – Layered Defense Concepts Part 2:**

* Building Entry Point Protection:
  + Locks:
    - Most accepted and used physical security device
    - Considered delay devices and not foolproof bar to entry – they are easily defeated
    - All lock types are subject to force and special tools that can be used to gain entry
    - Should be just one aspect of many physical security controls
    - Types:
      * Keyless Locks: Push-button (cipher) locks have buttons that are pushed in sequence to open the locks.
      * Smart Locks: Permit only authorized people into certain doors at certain times. An example is a magnetic stripe card that is time-sensitive.
    - Security Measures:
      * Lock and key control system
      * Key control procedures must be documented and followed – procedures for issue, sign out, inventory, destruction, and lost keys.
      * Combinations must be changed at specified times and under specified circumstances.
  + Guard Stations: Security forces (guards) can provide a deterrence to unauthorized entry. In some cases, may also prevent unauthorized entry.
  + Card Access Controls or Biometric Systems:
    - Smart cards, magnetic stripe cards, proximity cards, etc.
    - Fingerprint, retina scans, signature dynamics, voice recognition, hand geometry, etc.
* Facility/Construction Issues:
  + Entry Points:
    - Primary & secondary entrances
    - Windows
    - Roof access
    - Maintenance entrance
    - Emergency exits
    - Loading docks
  + Doors: Hollow-core versus solid-core, isolation of critical areas, lighting of doorways, contact devices (switches), & mantraps (double door systems)
  + Windows: Standard plate glass, tempered glass, acrylic materials
    - Polycarbonate Windows: Glass and polycarbonate combinations combine the best quality of glass and acrylics.

**Module 37 – Layered Defense Concepts Part 3:**

* Inside the Building – Building Floors, Office Suites, Offices:
  + Compartmentalized Areas:
    - Defines a location where sensitive equipment is stored and where sensitive information is processed.
    - Must have a higher level of security controls.
    - To be effective, they need an appropriate access control system.
  + Support System Controls
  + Fire Protection
  + Intrusion Detection Systems
* Data Center or Server Room Security:
  + Walls:
    - To the extent possible, walls should not form part of an external building.
    - Walls should extend from the floor to the underside of the above floor slab (slab to slab).
  + Access Controls:
    - Depending on the sensitivity of the information, and value of the equipment, electronic access controls may need to be installed.
      * Smart Cards
      * Biometric Devices
      * Locks
* Computer Equipment Protections:
  + Portable Device Security: Involves protecting the device, protecting the data on the device, and keeping the security controls easy for the user.
    - Includes items such as:
      * Locking mechanisms for docking stations
      * Tracing software
      * Audible motion alarm
      * Encryption software
      * Constant control procedures
      * Inventory system
      * Anti-virus software
* Object Protection: Objects are placed inside security containers such as safes, vaults, or locking file cabinets.
  + Should be theft-resistant and fire-resistant.
  + Steel containers with a locking device.
  + Create good lock combinations, change them frequently, and monitor the distribution.

**Module 38 – Crime Prevention & Physical Security:**

* Crime Prevention Through Environmental Design:
  + The physical environment of a building is changed or managed to produce behavioral effects that will assist in reducing the incidence and fear of crime.
  + Focuses on the relationships between the social behavior of people and the environments.
  + Three Key Strategies:
    - Territoriality: People protect territory that is their own
    - Surveillance: High degree of visual control
    - Access Control: Limit access and control the flow of access
* Site Location: Security should include where the building is and how it should be built.

PAST QUIZ/ASSIGNMENT QUESTIONS:

1. Which of the following is not part of an Access Control System Service?
   1. Authentication
   2. Authorization
   3. Identification
   4. Non-Repudiation
2. What is the primary use of a password?
   1. Authenticate the user
   2. Identify the user
   3. Allocate systems resources to a user
   4. Create an audit trail of user activity
3. A user access log is an example of which category of Access Control?
   1. Detective
   2. Corrective
   3. Compensating
   4. Deterrent
4. An employee attempts to navigate to a restricted website and receives a message that reads “This site is not approved by the company for access – Press OK to continue”. This is an example of what type of control?
   1. Compensating
   2. Technical
   3. Administrative
   4. Corrective
5. Which one of the following entities has the primary responsibility for determining access to a data file in a DAC environment?
   1. The Security Manager
   2. The Custodian
   3. The System
   4. The Owner
6. Which is the best known example of a symmetric key cipher?
   1. DES
   2. RSA
   3. AES
   4. PKI
7. A stream mode cipher would be most applicable for which of the following tasks?
   1. Encrypting a real-time broadcast of a digital video conference between heads of state
   2. Encrypting electronic transactions between consumers and an e-commerce website
   3. Encrypting intra-company emails that contain propriety information regarding the development of a new product
   4. Encryption the transmission of a downloadable corporate payroll file to an outsourced payroll processor
8. Digital Signatures do not allow for:
   1. Confidentiality of the message
   2. Detection of modification of a message
   3. 3rd Party verification of the sender
   4. Authentication of the sender
9. Which of the following is TRUE regarding symmetric cryptography:
   1. The key must be made available to a third part escrow authority
   2. The same key is used by both the sender (encryptor) and receiver (decryptor)
   3. Symmetric cryptography supports non-repudiation
   4. In large groups of users, it is easy to manage the keys
10. Using Asymmetric (Public Key) Encryption to provide the recipient of a message with “Proof of Origin” requires that the sender…
    1. Encrypt the message with the recipient’s Public Key
    2. Encrypt the message with the sender’s Private Key
    3. Encrypt the message with the sender’s Public Key
    4. Encrypt the message with the recipient’s Private Key
11. Which of the following examples would best fit the “Deter” goal of physical security?
    1. A biometric lock system installed at an entry door in a building
    2. A ultrasonic sensor system that is deployed on the loading dock at the rear of a manufacturing facility
    3. A dry pipe sprinkler systems that is installed in a data center server room
    4. A sign on a fence that reads “WARNING: Electrified Fence” that is installed around the HVAC system on the side of a building
12. Which of the following is NOT a key strategy for developing a physical security program?
    1. Management support for physical measurements of security
    2. Surveillance with high visual control
    3. Controlled flow of movement through limited access
    4. Territoriality culture among employees
13. All of the following are goals of physical security, EXCEPT
    1. Deter
    2. Detect
    3. Delay
    4. Detain
14. A camera located outside a server room door supports which of the following physical security objectives
    1. Review
    2. Delay
    3. Detect
    4. Process
15. Examples of types of physical access controls include all of the following EXCEPT
    1. Passwords
    2. Guard stations
    3. Locks
    4. Gates
16. Security blue prints…
    1. Are mapped from frameworks like NIST
    2. Provide management with a tool to conduct gap analysis on system controls
    3. Do not address technical requirements of a security program
    4. Are completely independent of any regulatory, business, or IT requirements
17. David is a systems analyst at XYZ Corp and he is reviewing the documentation on how to execute a server backup. The documentation David is reviewing represents which of the following items?
    1. A standard
    2. A policy
    3. A procedure
    4. A guideline
18. Samantha is installing the most current Sophos anti-virus data definition to XYZ Corp’s servers and workstations. In executing this action, Samantha is complying with which of the following?
    1. A guideline
    2. A standard
    3. A procedure
    4. A policy
19. Jason, a network Administrator for XYZ Corp, is adding a rule to block all inbound pings from 10.x.x.x IP address locations to the XYZ Corp intrusion detection appliance. By adding this rule, Jason is complying with which of the following?
    1. A guideline
    2. A procedure
    3. A policy
    4. A baseline
20. In most corporate settings, the OWNER of data is responsible for all of the following EXCEPT
    1. Ensuring that appropriate security, consistent with the organization’s security policy, is applied to the data
    2. Determining appropriate classification levels
    3. Determining access privileges
    4. Creating classification levels for the data
21. The concept of “Least Privileged” involves:
    1. User service
    2. Authentication processes
    3. User accountability
    4. Authorization levels
22. In an Accounting Department, several people are required to participate in the completion of a transaction. This is most likely an example of:
    1. Job rotation
    2. Collusion
    3. Separation of duties
    4. Least privilege
23. During risk analysis, we conclude that it is likely that our servers will be negatively affected 5 times this year by distributed denial of service (DDoS) attacks. This is an example of the what variable for quantitative risk analysis for DDoS attacks.
    1. Annual Loss Expectancy
    2. Single-Asset Exposure
    3. Repetitive Loss Expectancy
    4. Annual Rate of Occurrence
24. What is best addressed through the concept of Least Privilege?
    1. Network Traffic Logging
    2. Protecting sensitive data
    3. Compliance with data retention regulations
    4. Monitoring of employees activities
25. An effective security management program relies on all of the following EXCEPT
    1. Implementing technical controls
    2. Compliance with required regulations
    3. Alignment with business requirements
    4. User developed policies
26. Janet, a database administrator for XYZ Corp., has applied all the appropriate patches and updates to the XYZ Corp. database server. In doing so she has mitigated, using the best available methods, the risk for SQL Injection attacks. However, an SQL Injection attack is still possible. What would we call this risk?
    1. Software
    2. Residual
    3. System
    4. Hardware
27. In any organization, Information Security is the responsibility of…
    1. All employees
    2. Management
    3. The IT Staff
    4. The Board of Directors
28. Regarding data privacy in the U.S., which of the following statements is TRUE?
    1. Data privacy is not highly legislated or regulated in the U.S.
    2. Data privacy in the U.S. is regulated by General Data Protection Regulation (GDPR)
    3. Data privacy standards in the U.S. only apply to healthcare and banking data
    4. Data privacy standards are uniform and comprehensive across industries in the U.S.
29. Which of the following is true of the Federal Information Security Management Act?
    1. It requires the executive management of a publicly traded company to be accountable for errors and omissions in the financial statements that result from lack of internal controls testing
    2. It created a federal reporting agency that oversees internal controls auditing for public companies
    3. It requires governmental agencies to perform risk assessments
    4. It requires publicly trade companies to have internal controls audit annually
30. The CFO of XYZ Corp., a publicly traded company, willfully disregards organizational policy and uses and authorized Accounts Receivables clerk’s system credentials to access the Accounts Receivable Ledger to increase the recorded value of receivable balances. This action should be prosecuted as?
    1. Fraud
    2. Criminal negligence
    3. Civil negligence
    4. Corporate negligence
31. What is the key objective of a risk management program?
    1. Ensure that all risks are addressed appropriately
    2. Support management objectives
    3. Calculate a standard annual loss expectancy
    4. Identify risks to information systems
32. Information classification may assist an organization in…
    1. Organizing the cost budget for protecting assets
    2. Eliminating regulatory requirements
    3. Lowering user accountability for sensitive data
    4. Normalizing data stored in databases
33. In most states in the USA, a computer-related crime would be prosecuted under:
    1. State common law
    2. Federal Customary Law
    3. The Federal Civil Code
    4. Federal Mixed Law
34. The absence of a fire suppression system would be best characterized as a:
    1. Vulnerability
    2. Threat
    3. Risk
    4. Countermeasure
35. In addition to protecting corporate assets, security policies and procedures should ALWAYS:
    1. Apply to everyone in the organization
    2. Be justified by users
    3. Identify business objectives
    4. Be approved by 3rd party auditors
36. Assessing that the security functions work as intended.
37. These individuals control the access to systems and data but do not own either.
38. Form of risk analysis should be undertaken first.
39. Separations of duties controls can be defeated through.
40. Risk decisions should always be justified by…
41. Asset Value ($) x Exposure Factor (%) =
42. A small start up company decides it cannot afford to buy anti-virus software for its system. What form of risk management is this?
43. Anyone corporate office with fiduciary responsibility is required to exercise this.
44. An industry standard that establishes requirements for data protection.
45. The section of HIPAA that specifies a series of administrative, physical and technical safeguards.

PAST QUIZ/ASSIGNMENT ANSWERS:

1. D.
2. A.
3. A.
4. B.
5. D.
6. A.
7. A.
8. A.
9. B.
10. B.
11. D.
12. A.
13. D.
14. C.
15. A.
16. A.
17. C.
18. B.
19. D.
20. D.
21. D.
22. C.
23. D.
24. B.
25. D.
26. B.
27. A.
28. A.
29. C.
30. A.
31. A.
32. A.
33. A.
34. A.
35. A.
36. Assurance Requirements
37. Custodians
38. Qualitative
39. Collusion
40. Cost Benefit Analysis
41. SLE
42. Risk Acceptance
43. Due Care
44. PCI DSS
45. Security Rule