CISSP Absolute notes

=====================

Security management life cycle

- Plan and organize
- Implement
- Operate and maintain
- Monitor and evaluate

The main components of each phase are outlined below:

- Plan and organize
    - Management commitment
    - Oversight committee
    - Assess business drivers
    - Threat profile
    - Risk Assessment
    - Security architectures at an organizational, application, network and component level
    - Identify solutions
    - Obtain management approval

Implement

- Assign roles and responsibilities
- Develop and implement security policies, procedures, standards, baselines and guidelines
- Identify sensitive data at rest and in transit
- Implement programs
    + Asset identification and management
    + Risk management
    + Vulnerability management
    + Compliance
    + Identity management and access control
    + Change control
    + Software development life cycle
    + Business continuity planning
    + Awareness and training
    + Physical security
    + Incident response
- Implement solutions per program
- Develop auditing and monitoring solutions per program
- Establish goals and metrics per program

Operate and Maintain

- Baselines are met
- internal and external audits
- Tasks
- (SLA)service level agreements per program

Monitor and evaluate

- Review logs, audit results, collected metric values and SLAs per program from previous step
- Goal accomplishments
- Quarterly meetings with steering committee

-Develop improvement steps and integrate into the plan and organize phase

Life cycle structure for developing a security management :

Written policies and procedures are mapped

Individuals responsible for protecting company assets communicate and are connected

Progress and the ROI of spending and resource allocation can assessed

Know what’s missing and put standardized methods to fix what’s missing.

Compliance to regulations, laws, and policies is assured.

No dependency on technology for security

Security breaches result in emergency measures in a proactive approach.

=====================

HIPAA

-The Kennedy-Kassebaum Act, national standards for the storage, usage, and transmission of medical data.

-The Office of Civil Rights (OCR) of the Department of Health and Human Services (HHS)
is responsible for the enforcement of the Health Insurance Portability and Accountability Act (HIPAA).

Title II, Administrative Simplification, of the Health Insurance Portability and Accountability

-code sets, unique health Identifiers,security and electronic signatures, and privacy,health care providers ,health plans, and health care
clearing houses.

-It does NOT cover employers.

The American National Standards Institute Accredited Standards Committee X12 (ANSI ASC X12) Standard version 4010 applies to the transactions category
of HIPAA.

An employee can request a restriction on the disclosure of his health records.

Patients can request a restriction on certain uses and the disclosure of the information as provided by 45 CFR 164.522.

The HIPAA task force keeps an inventory of the following data in a company:

-Systems
-Processes
-Policies
-Procedures
-Data

The compiled health record is the property of the health care practitioner,
but the information belongs to the employee as a patient.

HIPAA gap analysis applies to transactions, security, and privacy and does not address either accountability or availability.

Gap Analysis:
With reference to HIPAA, a gap analysis defines the current status of the organization in a specific area and compares the current operations to the requirements mandated by the state or the federal law.

Gap Analysis transactions:
Gap analysis for transactions identifies and matches the data content required by the Health Insurance Portability and Accountability Act (HIPAA).
Deals with computer software data in medical field

Gap Analysis Security:
A gap analysis for security refers to the practice of identifying the security policies and practices currently in place in the organization to protect the data from unauthorized access, alteration, and disclosure.

Covered Entities:
Some health care providers, health plans, and clearinghouses are covered entities.
The term covered entity is defined in section 160.103 of the regulation.

Points to note:
Health plans do not provide health care services, but they organize the health care services.
The health care providers acting on behalf of the health plan do NOT become business associates of the health plans by simply joining the network.

A health plan can acquire the services of a provider to conduct transactions. If a health plan conducts the covered transactions through a clearinghouse or acquires the services of a provider to assist the clearinghouse to conduct these transactions, there will be an incremental increase in the cost. The cost increase is borne by the health plan.

IMP

Until the compliance date, it is not mandatory for these entities to comply with the HIPAA Privacy Rule. The covered entities may only agree to voluntarily protect the patient health information before the compliance date.

=====================

Computer Attacks

The four categories of computer crime are as follows:
computer-assisted crime - Computer is used as a tool
computer-targeted crime - Computer is the victim
computer-incidental crime - Computer is involved in the crime incidentally.
computer-prevalence crime - Occurs because computers are so prevalent in today's world.
Examples include violating commercial software copyrights and software piracy.

Examples of computer-targeted crimes include the following:
    carrying out a buffer overflow attack
    carrying out a distributed denial of service (DDoS) attack
    installing a virus on a computer to destroy the data on the computer

A computer-targeted crime could not take place without a computer, whereas a computer-assisted crime could.

Data diddling
    +Manipulation of data while it’s being entered in the app

A salami attack
    +committing numerous small crimes multiple number of times to ensure that no one notices the larger crime.

Scavenging
    +seeking sensitive information without knowing the format of the information.

Sniffing
    +extracting confidential information, such as user credentials, bank account numbers, and personal identification numbers.

An escalation of privileges
    +attacker has used a design flaw in an application to obtain unauthorized access to the application.
    +vertical - higher levels
    +horizontal- different users same level

A backdoor/maintenance hooks
    +lines of code that are inserted into an application to allow developers
    +bypass the security mechanisms. Backdoors are also referred to as maintenance hooks.

A buffer overflow occurs when an application erroneously allows an invalid amount of input in the buffer.

A trapdoor function is a mechanism that enables the implementation of the reverse function in a one-way function.

A brute force attack is an attack that repeatedly tries different values to determine the key used.

A man-in-the-middle attack is an attack where messages between two entities are intercepted so that an attacker can discover the legitimate entities' keys.

Phone phreakers are crackers or hackers who specialize in telephone fraud.
+Red boxing: Payphones. simulate coin placing and international calls free
+Blue boxing: The phreakers sent a 2600Hz tone over a telephone line by using a blue box device.
+White boxing: This technique was used by the phreakers to convert a touch-tone keypad into a portable dialer unit.
+Black boxing: This technique manipulated line voltage to enable phreakers to make long-distance calls free of charge. T

Fault generation
+smart card attack
+uncover the encryption key using reverse engineering. T
+introducing an input voltage, clock rate, or temperature fluctuation error into the card.

Microprobing
+intrusive smart card attack in which the card is physically manipulated until the ROM chip can be accessed.

A side-channel attack
+examinessmart card communication process to discover confidential information.
+ differential power analysis, electromagnetic analysis, and timing attacks.

A dictionary attack is a method where the attacker attempts to identify user credentials by feeding lists of commonly used words or phrases.

Spoofing occurs when an attacker implements a fake program that steals user credentials.

A phishing attack is an e-mail attack where a hacker attempts to gain user credentials by requesting them via e-mail.

A covert channel is not controlled by a security mechanism. A covert channel is a communication path that accesses information in an unauthorized manner and violates the security policy.
+One message talks to another.

The two types of covert channels are as follows:
-Covert timing channel

+a process sends information to another process but modulates the use of system resources.
–Covert storage channel:
+security risk arises due to the storage location.
A Loki attack is an example of a covert channel.

RedPill and Scooby Doo attacks target virtual machines
+identify the virtual machines

A covert timing channel is used when a process transmits data to another process.

DLL injection
+inserts a dynamic link library (DLL) into a running process's memory.
+Some of the standard defenses against DLL injection include application and operating system patches
+firewalls, and intrusion detection systems.

Cookies store information on a Web client for future sessions with a Web server.

A TOC/TOU attack is another name for an asynchronous attack.
+interrupts a task and changes something to affect the result.
+tasks occur in the correct order but the data transmitted by the tasks is changed in some manner.

XSS takes advantage of your trust on website. CSRF is advantage of website trust in you.

Blue jacking is an attack that sends unsolicited messages over a Bluetooth connection.
+spamming in a Bluetooth environment.

Bluesnarfing is the act of gaining unauthorized access to a device through its Bluetooth connection.

War driving is the act of discovering unprotected wireless network by driving around with a laptop.

Spamming is the act of sending unsolicited e–mail messages through a mail server.

Attacks against cryptosystems include the following:

+cipher–only attacks – The aim of the attack is to discover the key used in the encryption. This is the most common type of attack but is the hardest to accomplish.
+known plaintext attacks – This attack occurs when an attacker has the plaintext and ciphertext version of a message. The aim of the attack is to discover the key used in the encryption.
+chosen plaintext attacks – This attack occurs when an attacker has the plaintext and ciphertext and can select the plaintext that gets

encrypted to see the corresponding ciphertext. The aim of the attack is to discover the key used in the encryption.

+chosen ciphertext attacks - This attack occurs when an attacker chooses the ciphertext to be decrypted and has access to the resulting decrypted plaintext. The aim of the attack is to discover the key used in the encryption.

+differential cryptanalysis - This attack looks at ciphertext pairs and analyzes the result of the differences in the corresponding plaintext pairs. The aim of the attack is to discover the key used in the encryption.

+linear cryptanalysis - known plaintext attack on several encrypted messages encrypted using the same key.

+side-channel attacks - This attack uses inference to determine the value of the encryption key. This method applies reverse engineering instead of mathematical techniques.

+replay attacks - This attack occurs when an attacker captures some messages and resends the messages, hoping to fool the receiver into thinking the attacker is a legitimate entity. Usually this information involved authentication information.

+algebraic attacks - vulnerabilities of the mathematics used in the algorithm and attempts to exploit the algebraic structure.

+analytic attacks - structural weaknesses in an algorithm's design.

+statistical attacks - statistical weakness in an algorithm's design.

=====================

Laws

Patriot Act

Reduce restrictions to search telephone, e-mail communications, medical, financial, and other records. Wiretapping allowed

Government is aware

Private individual searches

search warrant

The Sarbanes-Oxley Act

-Accounting practices and methods that publicly traded companies must use when they report
their financial status.

-Prevent companies from committing fraud by knowingly providing inaccurate financial
reports to shareholders and the public.

-Section 404 Information Technology

The Gramm-Leach-Bliley Act established privacy policies for financial institutions.

-prevent the financial institutions from sharing information with third parties.

The Basel II Accord

minimum capital requirements-lowest amount of funds that a financial institute must keep in hand.

supervision- ensures oversight and review of risks and security measures.

market discipline. - disclose risk exposure and to validate market capital.

These pillars apply to financial institutions.

OMB Circular A-130 was developed to meet information resource management requirements for the federal government. According to this circular, independent audits should be performed every three years.

The European Privacy Principles are as follows:

-The reason for gathering data must be stated when the data is collected.

-Data cannot be used for other purposes other than those specifically stated at collection.

-Data that is not needed should not be collected.

-Data should only be kept while it is needed to accomplish a stated task.

-Only individuals who are required to accomplish a stated task should be given access to the data.

-The individuals responsible for securely storing the data should not allow unintentional leaking of data.

-Individuals are entitled to receive a report on the information that is held about them.

-Data transmission of personal information to locations where equivalent personal data protection cannot be assured is prohibited.

-Individuals have the right to correct errors contained in their personal data.

The Safe Harbor requirements are mandated in Europe when dealing with US

Privacy Act-

-Only authorized persons should have access to personal information.(similar to EU)

-The personal records should be up-to-date and accurate.

-The security and confidentiality of personal records should be ensured.

The Computer Security Act

federal agency,develop a security policy for sensitive computer systems.

Individual employees should be trained on methods to operate and manage the computer systems,acceptable computer practices

The Economic Espionage Act

-espionage attacks on corporations.

-Investigated by FBI

The U.S. Communications Assistance for Law Enforcement Act (CALEA)

- law enforcement agencies to conduct electronic surveillance. (Similar to Patriot Act)

- Devices may need to be modified.

The 1991 U.S. Federal Sentencing Guidelines

- white collar crimes that take place within an organization:
    +Antitrust
    +Federal securities
    +Mail and wire fraud
    +Bribery
    +Contracts
    +Money laundering

-Meant for Senior Management

==

Types of Laws

Civil Law

-payment of compensation and fines without sentencing the offenders to jail.

-Liability of senior organizational officials relative to the protection of information systems is prosecutable under civil law.

Criminal Law

-Offenders who violate the government laws meant to protect the public.

-Jail Sentence

Common Law-

-criminal, civil, and administrative laws.

-Common law is used in the United States, Canada, United Kingdom, Australia, and New Zealand.

Copyright Law

-control either the distribution or the reproduction of his or her work

Administrative/Regulatory Law

Adhere to the regulatory standards prescribed by the government.

Senior officials can be jailed if the administrative law fails o adhere.

Customary Law

-Customary law is based on regional traditions and customs.

=====================

BCP and DRP

The steps of business continuity are as follows:

-Develop the continuity planning policy statement.
    +Develop the continuity planning policy statement.
    +BCP project scope,
    +Roles of team members

+ Project goals.
+ BCP coordinator and business continuity team.
+ Define objectives and scope

- Conduct the BIA.
  + Identify Vulnerabilities, Threats, Risks
  + Identify Business units
    + Information gathering stage (surveys interviews)
    + The analytical stage (Identify the BU process, Threats, Vulnerabilities,Determining the risk associated with each threat, then prioritize, MTD,RTO)
    + The documentation stage includes documenting your findings and reporting back to managing.
    + Risk Management Process
    + Vulnerability Assessment
    + Threat Management
  + Prioritize the cost to enterprise
- Identify preventative controls.
- Develop Disaster recovery strategies.
  + processing transactions in the short term.
  + No part of the BCP relies on this
- Develop the contingency plan
  + Recover major system and applications after a disruption
  + How business will be carried out
  + Addresses Residual risks
- Test the plan, and conduct training and exercises.
- Maintain the plan.

  The business continuity plan should be maintained for several reasons including:
    + Infrastructure changes
    + Environment changes
    + Organizational changes
    + Hardware, software, and application changes
    + Personnel changes

Damage assessment

- Amount of Damage caused

Disaster Recovery

- Recover major applications systems

Occupant emergency plan (OEP)

- Injury to life minimized when disaster occurs.

All business units must be represented in the business continuity plan committee. This will ensure that all systems vital to the operation of the business units are identified.

Senior business management is ultimately responsible for identifying and prioritizing critical systems.
In the business continuity and disaster recovery process, senior management should perform the following:

+ Delegate recovery roles.
+ Publicly praise successes.
+ Closely control media and analyst communications.

Because all business units are vital to its operation, all business units should be represented.

```
=====================
Controls

Security Controls

    Physical Control
    Administrative Control
    Technical Control

Physical Control(Physically stops a threat)
    -Deterrent(discourage a threat)
        +Fences
        +Lighting
    Preventive (Foresee a Threat and put in a control)
        +Locks
        +Badge System
        +Security Guard
        +Biometric System
        +Mantrap Doors
        +BCP
    Detective(find out the threat)
        +Motion Detectors
        +CCTV
    Recovery(Recover back to the old working state)
        +Offsite Facility

Administrative Control
    Preventive
    --Security policy
    --Separation of duties
    --Information Classification
    --Personnel Procedures
    --Testing
    --Security Awareness Training
    Detective
    --Monitoring and Supervising
    --Job Rotation
    --Investigations

Technical Control
    Preventive
        +ACLs
        +Encryption
        +Antivirus
        +Smart Cards
        +Dail-up Call-Back Systems
        +Routers
        +Firewall
    Detective
        +Audit Logs
        +Audit trail
```

+IDS
Corrective
+Server Images
Recovery
+Data Backup
Deterrent
+Firewall

Operational Control (security as a continuous process)
+Technical-Backup controls,
+software testing
+anti-virus management
+Maintenance accounts

Directive control
+mandatory controls based on regulations or environmental requirements.

Monitoring and supervising is both a detective administrative control and a compensative administrative control.
A security badge is both a preventative physical control and a compensative physical control.

A reciprocal agreement occurs when two organizations agree to establish offsite facilities for each other.

Security controls can be classified into preventive, detective, corrective, deterrent, recovery, and compensating. Each of these controls can be further categorized into physical, administrative, and technical controls.

=====================

Incident Response

The five steps of incident response are as follows:
+Detection
+Response
+Mitigate
+Reporting
+Recovery
+Remediation and review
+Document

=====================

Security Awareness Program
+ make employees aware of their security responsibilities and of the expected ethical conduct and acceptable activities.
+ focuses on compliance and the acceptable use of resources
+ ethical conduct in the organization.

=====================

Roles

The security analyst
+develop policies, standards, and guidelines
+ensures the security elements are implemented properly.
+participate in design phase

User/End User/Information user
+A user routinely accesses corporate data
+must have the appropriate level of access assigned
+participate in the system requirement definition stage .

The data owner
+approves data classes and alters the classes as needs arise.
+ensure that appropriate security controls and user access rights are in place.

The security administrator
+creates new user accounts and passwords
+implements security software
+Tests patches and software components.
+Security assessment implementation
+Access control implementation and maintenance
+Security labels configuration and maintenance in a mandatory access control (MAC) environment
+Initial password creation
+Audit log review
+functional and not broader like Security Analyst

The role of the chief security officer (CSO)
+self-governing and independent of all the other departments in the organization.
+The CSO should report to the CXO In an organization
+infrastructure implementation based on directives issued by the CSO.
+as a part of the information security program, the CSO is the only authority.

The data custodian
+directly responsible for maintaining and protecting the data
+delegated to the IT department staff.
+implementing and maintaining security controls. T
+Maintaining activity records
+Verifying data accuracy and reliability
+Backing up and restoring data regularly

A system owner
+maintaining and protecting one or more data processing systems
+integration of the required security features into the applications
+purchase decision of the applications.
+remote access, password management, and operating system configurations provide the necessary security.

Senior Management - final say on scope

The following risk management components are provided by senior management:

+established risk acceptance level
+resource allocation
+monetary funding allocation

====================

Unions

+The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences Project (P3P) for user privacy on Web sites.

+The Internet Architecture Board (IAB) coordinates Internet design, engineering, and management. It oversees the Internet Engineering Task Force (IETF).

-Unethical according to IAB

Seeking to gain unauthorized access to the resources of the Internet
Destroying the integrity of computer-based information
Disrupting the intended use of the Internet
Wasting resources, including people, capacity, and computers, through such actions
Compromising the privacy of users
Being negligent in the conduct of Internet experiments
IAC is not associated with Internet design and management.

+The European Union (EU) has developed its own EU Principles on Privacy

+The Software Protection Association (SPA)

-primarily concerned with software piracy.
-Software piracy refers to the illegitimate use of either licensed software or an application.

+Central Intelligence Agency (CIA) is to preserve the national security US

+The Department of Defense (DoD) controls the United States military and coordinates its activities. DoD does not investigate computer crimes.

+National Computer Security Center (NCSC)

-evaluates computer security products
-provides technical support to government offices and private firms.

+The Institute of Electrical and Electronics Engineers (IEEE)

-develops standards for new technologies, including wireless.

+The Internet Corporation for Assigned Names and Numbers (ICANN)

+responsible for the allocation of IP addresses and management of DNS.

National Institute of Standards and Technology (NIST)

+measurement standards laboratory that is part of the United States Department of Commerce.

+Online Transaction Processing (OLTP)
-multiple database systems are clustered.
-Transactions are recorded and committed in real time by using OLTP.
-The primary purpose of OLTP is to provide resiliency and a high level of performance.

=====================

Downstream liability
+ensures that organizations working together under a contract are responsible for their information security management and security controls
deployed. Extranet
+legal or business obligations and not contractual obligations of business operations.

=====================

Separation of Duties
+Prevent conflicts of interest
+complete certain security tasks
+Static separation of duties
+an individual can be either an initiator of the transaction or the authorizer of the transaction.
+Dynamic separation of duties
+an individual can have a dual role where he can initiate as well as authorize transactions

Collusion
+In spite of putting separation of duties two people support in fraud

Due diligence
+evaluate information to identify vulnerabilities, threats, and issues related to risk.

Due care
+organization has taken the necessary steps to protect the organization, its resources, and personnel.

Job rotation
+when more than one person completes the tasks of a single position

A two-man control
+implies that two operators review and approve each other's work.

=====================

Policies

An information policy
+defines the sensitivity of a company's data and proper procedures for storage, transmission, disposal, and marking of a company's data.

Backup policy
+back up information stored on a company's network.

Security policy
+defines the technical means that are used to protect data on a network.
+defines the broad security objectives of an organization, establishes authority and responsibilities of individuals,
+strategic in nature.
+should be developed before procedures and guidelines are developed

Use policy/acceptable use policy,
+defines the manner in which employees are allowed to use a company's network equipment and resources
+expected performance and consequences of non-compliance.
+details guidelines on the rights, privileges, and restrictions for using company equipment and assets
+no expectation of privacy policy
+should indicate that data stored on a company computer is not guaranteed to remain confidential.
+data transferred to and from a company network is not guaranteed to remain confidential.
+computers are owned by the company and should be used only for company purposes.
+Information ownership is a component of a computer use policy that states that all information stored on company computers is owned by the company.

Information policy
+Classification of information :public and proprietary.
+Give only needs to know information

Security Policy

Management Policy

A system-specific policy
+defined by management
+rules governing the protection of information processing systems
+strategic in nature and is designed with a long-term focus
+implementation of firewalls, intrusion detection systems, and network and virus scanners.
An example of a system-specific security policy is a computer policy that defines the acceptable use of computer systems and has approved hardware and
software according to the security objectives of an organization.

Organizational security policy
+Formulated by the management

+procedure used to set up a security program and its goals.

Issue-specific policy
+ detailed evaluation of security problems addresses specific security issues.
+ensures that all employees understand these security issues and that they comply with the security policies defined to address these security issues.

Top-down approach.
+all initiatives come from top management and work their way down through middle management to other personnel.
+If a security program does not use this approach, it will probably fail.

A bottom-up approach
+IT department has to implement a security program without top management's initiation or support.
+This approach is less effective than the top-down approach.

======================
Agreements

Software license agreement
+agreement between a software vendor and a business customer.

End-user license agreement
+agreement between a software vendor and the end user. The end user is the computer owner.

A non-disclosure agreement
+agreement between two parties that information being shared will not be disclosed to third parties.

A service level agreement (SLA)
+agreement between a company and a vendor in which the vendor agrees to provide certain functions for a specified period.

Software escrow
+provide a software vendor's source code in the event the vendor goes out of business.
+third party is responsible for holding the source code and other applicable materials.

A reciprocal agreement
+agreement in which two companies agree to provide offsite facilities to each other in the event a disaster occurs.

Easy to bring up from easy to hard
+Hot site
+Warm site
+Cold site

=====================

Threats

+A terrorist attack is a politically motivated threat.
+Natural environmental threats include floods, earthquakes, tornadoes, hurricanes, and extreme temperatures.
+Supply system threats include power outages, communications interruptions, and water and gas interruption.
+Manmade threats include unauthorized access, explosions, disgruntled employee incidents, employee errors, accidents, vandalism, fraud, and theft.
While terrorist attacks are caused by man and could therefore be considered a manmade attack.

======================
Third Party integration

-Risk Assessment for Third party
+visit to the third-party organization's location
+assess physical and network security and access and administrative controls.
-Establish written IT security policy after risk assessment
-Minimal access for third-party users to appropriate resources
-Monitor the user access

=====================
Goals

Operational goals
+daily goals
+completed to maintain company functions.

Tactical goals
+midterm goals.
+more time and effort than operational goals, but less time and effort than strategic goals.

Strategic goals
+long-term goals.

An organizational goal is a generic term used to address all of the goals of an organization.

=====================
Frameworks

The Control Objectives for Information and related Technology (CobiT)
+IT governance
+operational goals.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO)
+corporate governance and focuses more on strategic goals.
-Control Environment
-Risk Assessment

-Control Activities
-Information and Communication
-Monitoring

International Standards Organization (ISO) 17799
+recommendations on enterprise security. The domains covered in ISO 17799 are as follows:
-Information security policy for the organization
-Creation of information security infrastructure
-Asset classification and control
-Personnel security
-Physical and environmental security
-Communications and operations management
-Access control
-System development and maintenance
-Business continuity management
-Compliance

Cobit and Coso are 'what' and ITIL/ISO are how

British Standard 7799 (BS7799) is the standard on which ISO 17799 is based.

Statement of Auditing Standards 70
+specifically on risks related to financial reporting. It was retired in 2011.
+SOC 1 focuses on financial reporting risks and controls. It is a detailed report for users and auditors.
+SOC 2-This report focuses on security, availability, confidentiality, processing integrity, and privacy.
+SOC 3 is a short report for public dissemination that focuses on security, availability, confidentiality, processing integrity, and privacy.

Construction Cost Model (COCOMO)
+cost estimation
+costs associated with software development
+estimates software development effort and cost as a function of the size of the software product in source instructions.

=====================

Property Law

Trade secret law
+information necessary for company's survival
+need specific skills to make Trade secret
+Does not protect an idea or an expression

Copyright
+protects an idea's expression rather than the idea itself.

IMP
The ideas are protected by the use of patents, and the corresponding expression is controlled by copyrights.

Trademark
+word or to a symbol that is used to represent a company to the world.

Patent
+20 years
+Just the idea. The expression protected by Copyright

=====================
Malware

Zombies are remote-controlled programs that hackers can use to attack networks.

Trojan horse
+disguised as a useful utility, but contains embedded malicious code.
+Trojan horses use covert channels

A virus is malicious software (malware) that relies upon other application programs to execute and infect a system.
The main criterion for classifying a piece of executable code as a virus is that it spreads itself by means of hosts. The hosts could be any application or file on the system. A virus infects a system by replicating itself through application hosts. Viruses usually include a replication mechanism and an activation mechanism designed with a particular objective in mind.

A debugging or maintenance hook
+software code that is intentionally embedded in the software
+Allows the dev to bypass security

A logic bomb
+malicious program that remains dormant and is triggered following a specific action

A pseudo-flaw refers to vulnerability code embedded intentionally in the software to trap intruders.

A multipart virus can infect both executable files and boot sectors of hard disk drives.

A retrovirus virus attacks or bypasses anti-virus software.

A phage virus modifies other programs and databases. The only way to remove the virus is to reinstall the infected applications.

An armored virus includes protective code that prevents examination of critical elements. The armor attempts to protect the virus from destruction.

A companion virus attaches to legitimate programs and creates a program with a different file extension. Makes use of windows search .com,.cmd
When the user attempts to access the legitimate program, the companion virus executes in place of the legitimate program.

A stealth virus prevents detection by hiding from applications. It may report a different file size than the actual file size as a method of preventing detection.

Open Vulnerability and Assessment Language (OVAL) is a standard written in XML that provides open and publicly available security content.
Its purpose is to standardize information between different security tools.

Spyware and Trojan horses are security threats that are NOT self-replicating.

Viruses and worms can both self-replicate, meaning that the virus or worm can actually copy itself to multiple locations.

Adware is a software application that displays advertisements while the application is executing.
Some adware is also spyware that monitors your Internet usage and personal information.

=====================

Risk Management

Quantitative risk
+predict the likelihood a threat will occur
+assigns a monetary value in the event a loss occurs.

The Delphi technique
+qualitative risk analysis
+anonymous opinions.

A vulnerability assessment is a method of determining system vulnerabilities and their risk(s). Steps are then taken to reduce the risk.

Qualitative risk analysis
+does not assign monetary values.

=====================

Incident Response
+Emergency procedures in response to a computer system or network attack are performed by the incident response team.
+contain and repair any damage caused by an event.
+A meeting should be held within a week to discuss the intrusion and its investigation.
+The following items are on the agenda of the incident response team while investigating an incident:
-Points of contact and reporting outside the company
-Points of contact for system forensics
-Process used to search for and secure the evidence, including search and seizure team members

```
        -Content and format of the report to be presented to management
        -Methods to deal with different types of systems
    +The incident response team must also be concerned with the fact that
a suspect may attempt to destroy evidence.

The incident prevention, intrusion detection, and cyber security teams are
not concerned with the incident response.
=====================

Security Training
+ensure that all employees understand their security responsibilities,
+communicating in a technical/non technical way
+may be customized for different groups of employees, such as senior
management, technical staff, and users.

Security awareness
    +reinforce the fact that security supports the mission of the
organization by protecting valuable resources.
Security training
    +teach people the skills that will enable them to perform their jobs
more securely.
    +Training focuses on security awareness.

Security education
    +in-depth
    +targeted for security professionals and those whose jobs require
expertise in security.

=======================
Scoping provides instruction to an organization on how to apply and
implement security controls.
Tailoring matches security controls to the needs of the organization.
Scoping and tailoring will allow an organization to narrow its focus to
identify
and address the appropriate risks.
=======================

NIST frameworks

NIST SP 800-137. NIST SP 800-137 Information security continuous
monitoring (ISCM) for federal information systems and organizations.
    +Define an ISCM strategy.
    +Establish an ISCM program.-determines the metrics, monitoring, and
assessment frequencies in addition to the ISCM architecture
    +Implement an ISCM program.
    +Analyze data, and report findings.
    +Respond to findings.
    +Review and update the ISCM strategy and program.

=======================

Validation

Pre-validation controls
```

+client side.
+prior to submission to the application
+client server both
+Parameter Validation

Access controls
+limiting access to resources to authorized users.

Post-validation controls
+application's output is validated to be within certain constraints.

Input validation
+not a control
+verifies the values that the user's input.
+different from parameter validation -Parameter validation validates parameters that are defined within the application.

=======================
=======================
Data Removal Methods

Degaussing
+reducing or eliminating an unwanted magnetic field o
+applying strong magnetic forces.
+Degaussing is the most preferred method for erasing data from magnetic media, such as floppy disks and magnetic tapes.

Zeroization implies
+storage media is repeatedly overwritten with null values.
+Zeroization is generally used in a software development environment.

Formatting is not recommended for removing data from a storage media - Residual data is called Data Remanence

Sanitization
+umbrella process of wiping the storage media to ensure that its data cannot be recovered or reused.

Media destruction
+physically destroying the media to make it unusable.

Media viability controls
+protect the viability of data storage media.
-proper labeling or marking
-secure handling and storage
-storage media disposal.

=======================

Penetration Testing

A penetration test includes the following steps:
-Discovery
+Gather initial information.

+Determine the network range.
+Identify active devices.
-Enumeration
+Discover open ports and access points.
+Discover which services are using the open ports.
-Vulnerability Mapping
+Identify the operating systems and their settings.
+Map the network.
-Exploitation
+Exploit the found vulnerabilities
+Boom Boom POW
-Report
+Send report to higher management
+Put in counter measures

NOTE: A penetration tester would need to be used outside your network.

A vulnerability scanner checks your network for known vulnerabilities and provides methods for protection against the vulnerabilities. A port scanner identifies ports and services that are available on your network. A protocol analyzer captures packets on your network.

=======================

Testing types

Double-blind
+demonstrate the success or failure of a possible attack.
+network security team does NOT know about the test
+how the team reacts to the attack.

Blind test
+the security team of the network being tested knows about the test
+Assessors have only publicly available information on the network.

Targeted test
+Tests are carried out on specific areas or systems.

=======================
Reporting
Ad-hoc reporting
+needs business intelligence (BI) solution
+connect it to the data sources, establish security settings,
+determine which objects users can access.

Automated reporting delivers
+setup the reports required in advance
+automatically generating and delivering these reports.
+users do not create the reports they need, predefined

Recurring reporting
+reports to be generated on a regular basis for information that is always needed.
+users do not create the reports they need.

Sources of information

A data feed allows users to receive updated data from data sources.
A web feed or RSS feed are popular forms of data feeds. With data feeds, users receive information, not reports.

=======================

LIFECYCLES

Product Development Lifecycle

Identification
+Obtaining management approval
+Initial risk analysis.
+The sensitivity of the data required
+Countermeasure techniques

Implementation
+Certification- Evaluate and review to confirm the products are meeting stated security standards
+Accreditation
- formal acceptance of the product and its responsibility by management
- final step in authorizing a system for use in an environment

Functional Design Analysis
+Formal Security Baseline
+testing to confirm security requirements are met

Software Development
+Functionality and performance tests

In a product development lifecycle, it is important that security be a part of the overall design and be integrated at each stage of product development.

=======================

Software Acquisition Phase

During the planning phase
+Software requirements are documented.
+acquisition strategy
+evaluation criteria.

Contracting phase
+issue the request for proposal (RFP)
+evaluate the proposals
+final contract negotiations with the selected seller.

Monitoring phase
+the product is actually deployed.
+ensure that the supplier completes the contract
+formally accept the final product.

Maintaining phase
+maintain the software, including possibly decommissioning the software at some future date.

=======================

Software development models

Capability Maturity Model (CMM)
-Principles, procedures, and practices that should be followed by an organization in a software development life cycle.
-Quality of a software product is directly proportional to software development and maintenance processes
-Maturity Levels
+Initial
-The development procedures are not organized
-and the quality of the product is not assured at this level.
+Repeatable:
-process involves formal management control
-proper change control
-quality assurance implemented while developing applications.
+Defined:
-Formal procedures for software development
-This category also provides the ability to improve the process.
+Managed:
-procedure involves gathering data and performing an analysis.
-Formal procedures are established
-qualitative analysis is conducted to analyze gaps by using the metrics at this level.
+Optimized: The organization implements process improvement plans and lays out procedures and budgets.

Cleanroom model
+well-defined formal procedures for development and testing of software.
+strict testing procedures
+used for critical applications that should be certified.

The Waterfall model
+proper reviews and the documenting of reviews at each phase of the software development cycle.
This model divides the software development cycle into phases.

The Spiral model
+analyzing the risk, building prototypes, and simulating the application tasks during the various phases of development cycle.

Software Development Lifecycle

Initiation:
+security requirements, such as encryption.
+identifies the relevant threats and vulnerabilities based on the environment
+the sensitivity of the data required, and the countermeasures
System development phase
+coding and scripting of software applications.
+written according to the defined security and functionality requirements of the product.
System design specification phase
+which kind of security mechanism will be a part of the software product.
+includes conducting a detailed design review
+developing a plan for validation, verification, and testing.
+Security Analyst getting involved gives maximum benefit
Implementation stage
+use of an application on production systems.
+Analyzed to see if it fits business requirements
Operations and maintenance
+addresses problems related to providing support to the customer after the implementation of the product,
+patching up vulnerabilities and resolving bugs, and authenticating users
+ensure appropriate access control decisions.
+The maintenance phase controls consist of request control, change control, and release control.
Disposal of software
+software would no longer be used for business requirements

Expert System:
-expert system consists of a knowledge base and adaptive algorithms
+Forward-chaining technique.
-if-then-else rules to obtain more data than is currently available. A
+Backward chaining
-works backwards by analyzing the list of the goals identified and verifying the availability of data to reach a conclusion on any goal.
-Knowledge-based system (KBS) or expert systems include the knowledge base, inference engine, and interface between the user and the system.
-A knowledge engineer and domain expert develops a KBS or expert system.
-Expert systems are used to automate security log review to detect intrusion.
-A fuzzy expert system is an expert system that uses fuzzy membership functions and rules, instead of Boolean logic, to reason about data. (no if
else)

=======================

=======================

Change Management

+Make a formal request.(usually the owner/implementer)
+Analyze the request.

-reviewing the security implication of implementing the change.
+Record the change request.
+Submit the change request for approval.
+Make changes.
+Submit results to management(results go to management)

Configuration management is tracking change. Change management is actual change request.

=======================

Database Model
Object-oriented database
+store multiple types of data, such as images, audio, video, and documents.
+The data elements and the different components are referred to as objects.
+These objects are used to create dynamic data components.

The distributed database model
+situated at remote locations and are logically connected.

Hybrid
+object-oriented based database and a relational database

hierarchical database
+the data is organized in a logical tree structure rather than by using rows and columns.
+Records and fields are related to each other in a parent-child tree structure.
+Used when too many relations exist

=======================

Software development monitoring

Gantt Charts
+bar charts that represent the progress of tasks and activities over a period of time.
+depict the timing and the interdependencies between the tasks.
+considered a project management tool to represent the scheduling of tasks and activities of a project,

A PERT chart
+project management model
+invented by the United States Department of Defense.
+PERT can also be used to determine the minimum time required to complete the total project.

The Delphi technique
+Anonymous feedback
+Qualitative

Cost-estimating techniques
+Delphi technique

+expert judgment
+function points.

=======================

Protocols

Simple Object Access Protocol (SOAP)
+XML-based protocol that encodes messages in a Web service setup.

Object request brokers (ORBs)
+middleware that establishes the relationship between objects in a client/server environment.
+Common Object Request Broker Architecture (CORBA).
+A distributed object model that has similarities to CORBA is DCOM.

The Object Request Architecture (ORA)
+framework for a distributed environment.
+It consists of ORBs, object services, application objects, and common facilities.

distributed data processing (DDP):
+multiple processing locations ,alternatives for computing in the event that a site becomes inoperative.
+Distances from a user to a processing resource are transparent to the user.
+Data stored at multiple, geographically separate locations is easily available to the user

Dynamic data exchange (DDE)
+enables direct communication between two applications using interprocess communications (IPC).
+Client Server Model

=======================

=======================

Security Processes

A baseline
+minimum level of security and performance of a system in an organization.

Guidelines
+suggested when standards are not applicable in a particular situation.
+Guidelines are applied where a particular standard cannot be enforced for security compliance.
+Guidelines can be defined for physical security, personnel, or technology in the form of security best practices.

Standards
+mandated rules that govern the acceptable level of security for hardware and software.
+Standards also include the regulated behavior of employees.
+Standards are enforceable

Procedures are the detailed instructions used to accomplish a task or a goal.

Procedural security ensures data integrity.

=======================

Data Classification

The types of commercial data classification are as follows:
    Confidential
    Private
    Sensitive
    Public

Military data classification are as follows:
    +top-secret
    +secret
    +confidential
    +sensitive but unclassified
    +unclassified

=======================

DB Techniques

OLTP
    +transactional technique used when a fault-tolerant, clustered database exists.
    +OLTP balances transactional requests and distributes them among the different servers based on transaction load.
    +OLTP uses a two-phase commit to ensure that all the databases in the cluster contain the same data.

Object Linking and Embedding Database (OLE DB)
    +method of linking data from different databases together.

Open Database Connectivity (ODBC) is an application programming interface (API)
    +configured to allow any application to query databases.

Data warehousing
    +data from several databases is combined into a large database for retrieval and analysis.

Noise and perturbation technique
    +randomized bogus information
    +mislead attackers and protect database confidentiality and integrity.

Partitioning
    +splitting the database into many parts
    +tough for attacker to put back in context

Cell suppression

+hiding the database cells that can be used to disclose confidential information.

A trusted front-end

+providing security the functionality of the front-end client software that is used to issue instructions to the back-end server by using a structured query language.

Save points

+database can return to a point when the system crashes.

Database views

+ limit user access to portions of data instead of to the entire database.

Metadata

+useful information extracted from the existing database by using data mining techniques.

+Metadata provides an insight into data relationships.

Data mining techniques are used to extract new information from the existing information.

Knowledge base refers to collection of facts, rules, and procedures and is not related to data warehouse.

Data normalization ensures that attributes in a database table depend only on the primary key.

Polyinstantiation

+users with lower access level are not able to access and modify data categorized for a higher level of access

Bind variable

+single statement to execute multiple variables.

+placeholders for values sent to a database server in a SQL query.

+reuse of previously issued SQL statements

A two-phase commit (if any part fails rollback)

+transaction is executed to ensure data integrity.

+If a portion of a transaction cannot complete, the entire transaction is not performed.

Concurrency (up to date view)

+most up-to-date information is shown to database users.

+locks implemented,updates happen one at a time.

Aggregation

+user can take information for different sources and combines them to accurately predict that the user does not have the clearance to view directly.

=======================

Windows server logs
Event ID 539 occurs when a user account is locked out.
Event ID 531 occurs when a user account is disabled.
Event ID 532 occurs when a user account has expired.
Event ID 535 occurs when the account's password has expired.

=======================

=======================

DB Language

+The data definition language (DDL) identifies the schema of the database.

+The schema of a database defines the type of data that the database can store and manipulate.

+The query language (QL) query to obtain relevant output.

+The data control language (DCL) manages access control to records in a database.

+Examples of DCL commands are grant, deny, revoke, delete, update, and read.

+The data manipulation language (DML) -suite of computer languages used by database users to retrieve, insert, delete, and update data in a database.

==========================

Security Modes

Dedicated security mode
+clearance and the formal approval required to access all the data processed by the system.
+single level of information classification.
+sign nondisclosure agreements.
+single level of security.
+system have the highest level of security clearance that matches the classification of data.

System high mode
+system operates at the highest level of information classification.
+all users must have security clearances for the highest level of classified information.
Multi-level mode
+ users with different clearances and data at multiple classification levels.

==========================

Security Models

Information Flow Model:
+flow of information between the different security levels and the objects

+irrespective of direction

+based on an access control matrix.

+Biba model and the Ball-LaPadula based on information flow model and the state machine model.

Clark-Wilson access control model

+integrity through the implementation of integrity-monitoring rules and integrity-preserving rules.

+integrity-monitoring rules are known as certification rules

+integrity-preserving rules are known as enforcement rules. T

+defines a constrained data item, an integrity verification procedure, and a transformation procedure.

+subject-program-object triple

+Separation of duties maintained

+access triple rule is used to control the flow of information in the Clark-Wilson model.

Noninterference model

+multilevel security a

+commands and activities performed at one security level do not affect the activities at another security level.

The Biba model

+no write up

+no read down

+star (*) integrity and simple integrity

Brewer and Nash model

+Chinese Wall model

+access controls for a system will dynamically change according to a user's activities and the previous access requests.

+No Conflict of interest

The TCSEC-defined levels and the sublevels of security are as follows:

A: Verified protection offering the highest level of security

+A1

+security assurance, design, development, implementation, evaluation, and documentation of a computer is performed in a very formal and detailed manner.

+most secure environment and is typically used to store highly confidential and sensitive information.

+trusted distribution controls.

B:

+MAC Bell-LaPadula security model

+enforced by the use of security labels.

-B1

+labeled security

+subject should have an equal or higher level of security clearance than the object.
+offers process isolation
+the use of device labels, the use of design specification and verification, and mandatory access controls.

-B2
+structured protection.
+subject to access objects by using the trusted path without any backdoors.
+lowest level to implement trusted facility management;
+separation of operator and administrator duties, sensitivity labels
+covert storage channel analysis (but NOT covert timing analysis).

-B3
+security domains.
+trusted recovery.
+monitoring and auditing functionality.
+covert timing analysis

C:
+Discretionary protection based on discretionary access of subjects, objects, individuals, and groups.
C1
-discretionary security protection.
+separated from the auditing facility by using a clear identification and authentication process.
+Low security concerns
+Low security

C2
+controlled access protection.
+resource protection and does not allow object reuse.
+Object reuse implies that an object should not have remnant data that can be used by a subject later.
+Commercial environments

D
+Minimal protection rating that is offered to systems that fail to meet the evaluation criteria

The Bell-LaPadula model
+multilevel security mode
+MAC - labels
+information flow from higher levels to low.
+This model formalizes the U.S. Department of Defense multi-level security policy.
+The simple security, star property, and strong star property rules
+Tranquility principle used in the Bell-LaPadula model prevents the security level of subjects and objects from being changed once they have been created.

+Static in nature

The multilevel security mode

+assigns sensitivity labels to subjects and objects.

+subject is able to access the object if the sensitivity label of the subject is higher than or equal to the sensitivity label of the object.

Lattice based Access Control

+least upper bound and greatest lower bound operators control the flow of information

+Not all access controls are equal

+stress on confidentiality.

+Access is based on security classes or security labels.

+Based on classification/subject object level access is allowed or denied.

The Common Criteria

+functionality and assurance attributes of a product.

+Combine TCSEC and ITSEC into a standards

Protection Profile:

+set of security requirements for a product and the rationale behind such requirements.

-EAL1: The product is functionally tested.

-EAL2: The product is structurally tested.

-EAL3: The product is methodically tested and checked.

-EAL4: The product is methodically designed, tested, and reviewed.

-EAL5: The product is semi-formally designed and tested.

-EAL6: The product has a semi-formally verified design and is tested.

-EAL7: The product has a formally verified design and is tested.

(functionally,structurally,methodologically,semi-formally)

Target of evaluation (TOE)

+product that is to be evaluated for rating.

Vendor's security target

+functionality and assurance mechanisms that meet the security solution.

The Take-Grant model

+states and state transitions in designing the protection system.

+It specifies the rights that a subject can transfer to an object.

Graham Denning

This model addresses the security issues associated with how to define a set of basic rights on how specific subjects can execute security functions on an object. The model has eight basic protection rules (actions) that outline:

How to securely create an object.

How to securely create a subject.

How to securely delete an object.

How to securely delete a subject.

How to securely provide the read access right.

How to securely provide the grant access right.

How to securely provide the delete access right.

How to securely provide the transfer access right.

Sutherland

set system of states initial states and transitions

Safe Harbour Principles

Notice - Individuals must be informed that their data is being collected and how it will be used.The organization must provide information about how individuals can contact the organization with any inquiries or complaints.

Choice - Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.

Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

Security - Reasonable efforts must be made to prevent loss of collected information.

Data Integrity - Data must be relevant and reliable for the purpose it was collected.

Access - Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.

Enforcement - There must be effective means of enforcing these rules.

==========================

Secure Components

Security kernel:

+The security kernel should provide isolation for the processes.

+Every attempt to access the system should invoke the reference monitor.

+The reference monitor should be verified, and all the decisions logged.

+The security kernel should be small enough to be tested in a comprehensive manner.

The reference monitor should have the following features:

+mediator between subjects and objects providing AC control

+Isolation:limited subjects have access privileges to the objects.

+Completeness: This ensures that the reference monitor is able to provide information regarding the process cycles of a system.

+Verifiability: This ensures that actions of the subjects accessing the objects are auditable.

An execution domain

+isolated area that is used by trusted process when they are run in privileged state.

A protection domain

+memory space isolated from other running processes in a multiprocessing system.

A trusted path is the communication channel between applications and the kernel in the TCB.

Trusted Recovery

Maintenance mode=emergency restart
+process lower privilege attempts to access the restricted memory segments, the system transits into maintenance mode
+emergency system restart occurs in response to a system failure.
+media failure

A system reboot occurs
+TCB failures
+controlled reboot of the system.
+release system resources and perform the necessary system activities.

A system cold start
+system administrator intervenes.
+recovery procedures are inadequate to recover the system from a TCB or a media failure.
+inconsistent state during an attempt by the system to recover.

Fail-safe systems provide the ability to automatically terminate the processes in response to a failure.(allow all)
Fail-secure state refers to the ability of a system to maintain and preserve the secure state of the system in the event of a system failure. (block everything)
Fail-over systems provide the ability to recover by switching over to backup systems(fault tolerance)
Fail soft is the termination of selected, non-critical processes when a hardware or software failure occurs and is detected.

==========================
Cryptographic Lifecycle

The steps in the cryptographic key life cycle are as follows:
+Creation
+Initialization
+Distribution
+Activation
+Inactivation
+Termination

Effective key management has the following requirements:
The key should be distributed and managed in a secure manner.
The key should be generated randomly and should use the full keyspace of the algorithm.

The duration of the key should be based on the sensitivity of data.
The key should be backed up in the event of a lost or destroyed key.
The key should be disposed in a secure manner.

Cross Certification
+does not check the authenticity of the certificates in the certification path.
+performed by certification path validation.
+used to establish trust between different PKIs and build an overall PKI hierarchy.

X.509 is a digital certificate standard.
Level 1 assurance for a digital certificate only requires an e-mail address.

Bitlocker needs TPM(Trusted Platform module)

Encrypting File System (EFS)
+enabled on a per-user basis and can only encrypt files belonging to the user that enables EFS.
+EFS does not require any special hardware or administrative configuration.

Capstone
implemented by U.S. Escrowed Encryption Standard and was developed by the NSA.
It implements the same algorithm as a Clipper chip.

Trusted Platform Module (TPM) and Hardware Security Module (HSM) are two chips that are used with full-disk encryption.
While the Clipper chip was developed by the NSA, it uses the Skipjack algorithm.

==========Necessary steps for a proper classification program:
1. Identify the custodian, and define their responsibilities.
2. Specify the evaluation criteria of how the information will be classified and labeled.
3. Classify and label each resource. (The owner conducts this step, but a supervisor should review it.)
4. Document any exceptions to the classification policy that are discovered, and integrate them into the evaluation criteria.
5. Select the security controls that will be applied to each classification level to provide the necessary level of protection.
6. Specify the procedures for declassifying resources and the procedures for transferring custody of a resource to an external entity.
7. Create an enterprise-wide awareness program to instruct all personnel about the classification system.

==========
Business Impact Analysis Steps
The more detailed and granular steps of a BIA are outlined here:
1. Select individuals to interview for data gathering.

2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company s critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

==========

COBIT5 in Order
Meeting Stakeholders needs, 2) Covering the enterprise end to end, 3) Apply a single integrated framework, 4) Enabling a holistic approach, 5) Separating governance from management.

Three sub-dimensions of quality in COBIT 5 are as follows:

1. Intrinsic quality - The extent to which data values are in conformance with the actual or true values. It includes

Accuracy - The extent to which information is correct or accurate and reliable
Objectivity - The extent to which information is unbiased, unprejudiced and impartial.
Believability - The extent to which information is regarded as true and credible.
Reputation - The extent to which information is highly regarded in terms of its source or content.

2. Contextual and Representational Quality - The extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, reorganizing that information quality depends on the context of use. It includes

Relevancy - The extent to which information is applicable and helpful for the task at hand.
Completeness - The extent to which information is not missing and is of sufficient depth and breadth for the task at hand
Currency - The extent to which information is sufficiently up to date for task at hand.
Appropriate amount of information - The extent to which the volume of information is appropriate for the task at hand
Consistent Representation - The extent to which information is presented in the same format.
Interpretability - The extent to which information is in appropriate languages, symbols and units, with clear definitions.
Understandability - The extent to which information is easily comprehended.
Ease of manipulation - The extent to which information is easy to manipulate and apply to different tasks.

3. Security/accessibility quality - The extent to which information is available or obtainable. It includes:

Availability/timeliness - The extent to which information is available when required, or easily available when required, or easily and quickly retrievable.
Restricted Access - The extent to which access to information is restricted appropriately to authorize parties.
===============

Code of Ethics Canons:
There are 4 high-level canons within the ISC2 code of ethics, below you have the details of what apply to each of them.

1. Protect society, the commonwealth, and the infrastructure

Promote and preserve public trust and confidence in information and systems
Promote the understanding and acceptance of prudent information security measures
Preserve and strengthen the integrity of the public infrastructure
Discourage unsafe practice

2. Act honorably, honestly, justly, responsibly, and legally

Tell the truth; make all stakeholders aware of your actions on a timely basis
Observe all contracts and agreements, express or implied
Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order
Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort
Take care to be truthful, objective, cautious, and within your competence
When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your
service

3. Provide diligent and competent service to principals

Preserve the value of their systems, applications, and information
Respect their trust and the privileges that they grant you
Avoid conflicts of interest or the appearance thereof
Render only those services for which you are fully competent and qualified

4. Advance and protect the profession

Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession
Take care not to injure the reputation of other professionals through malice or indifference
Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others

=================

When an intrusion has been detected and confirmed, if you wish to prosecute the attacker in court, the following actions should be performed in the following order:

Capture and record system information and evidence that may be lost, modified, or not captured during the execution of a backup procedure. Start with the most volatile memory areas first.

Make at least two full backups of the compromised systems, using hardware-write-protectable or write-once media. A first backup may be used to re-install the compromised system for further analysis and the second one should be preserved in a secure location to preserve the chain of custody of evidence.

Isolate the compromised systems.

Search for signs of intrusions on other systems.

Examine logs in order to gather more information and better identify other systems to which the intruder might have gained access.

Search through logs of compromised systems for information that would reveal the kind of attacks used to gain access.

Identify what the intruder did, for example by analyzing various log files, comparing checksums of known, trusted files to those on the compromised machine and by using other intrusion analysis tools.

Regardless of the exact steps being followed, if you wish to prosecute in a court of law it means you MUST capture the evidence as a first step before it could be lost or contaminated. You always start with the most volatile evidence first.

==================

The Committee of Sponsoring Organizations of the Treadway Commission (COSO)2 was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, which studied factors that lead to fraudulent financial reporting and produced recommendations for public companies, their auditors, the Securities Exchange Commission, and other regulators.

COSO identifies five areas of internal control necessary to meet the financial reporting and disclosure objectives.

These include:

(1) control environment,
(2) risk assessment,
(3) control activities,
(4) information and communication, and
(5) monitoring.

The COSO internal control model has been adopted as a framework by some organizations working toward Sarbanes-Oxley Section 404 compliance.

COSO deals more at the strategic level, while CobiT focuses more at the operational level. CobiT is a way to meet many of the COSO objectives, but only from the IT perspective.

COSO deals with non-IT items also, as in company culture, financial accounting principles, board of director responsibility, and internal communication structures.

Its main purpose is to help ensure fraudulent financial reporting cannot take place in an organization.

COBIT

Control Objectives for Information and related Technology (COBIT)4 is published by the IT Governance Institute and integrates the following IT and risk frameworks:

■ CobiT 4.1
■ Val IT 2.0
■ Risk IT
■ IT Assurance Framework (ITAF)
■ Business Model for Information Security (BMIS)

The COBIT framework examines the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability aspects of the high-level control objectives. The framework provides an overall structure for information technology control and includes control objectives that can be utilized to determine effective security control objectives that are driven from the business needs.

The Information Systems Audit and Control Association (ISACA) dedicates numerous resources to the support and understanding of COBIT.

===============
SABSA - Sherwood Applied Business Security Architecture

Carry out continuous monitoring to test and validate the effectiveness of current security measures.

The Risk Management Framework (RMF) developed by NIST, describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Ongoing monitoring is a critical part of that risk management process. In addition, an organization’s overall security architecture and accompanying security program are monitored to ensure that organization-wide operations remain within an acceptable level of risk, despite any changes that occur.

Timely, relevant, and accurate information is vital, particularly when resources are limited and agencies must prioritize their efforts. Information security continuous monitoring (ISCM) is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Any effort or process intended to support ongoing monitoring of information security across an organization begins with leadership defining a comprehensive ISCM strategy encompassing technology, processes, procedures, operating environments, and people.

SABSA is a proven methodology for developing business-driven, risk and opportunity focused Security Architectures at both enterprise and solutions level that traceably support business objectives. It is also widely used for Information Assurance Architectures, Risk Management Frameworks, and to align and seamlessly integrate security and risk management into IT Architecture methods and frameworks.

SABSA is comprised of a series of integrated frameworks, models, methods and processes, used independently or as an holistic integrated enterprise solution, including:

Business Requirements Engineering Framework (known as Attributes Profiling)

Risk and Opportunity Management Framework

Policy Architecture Framework

Security Services-Oriented Architecture Framework

Governance Framework

Security Domain Framework

Through-life Security Service Management & Performance Management Framework

==============

An Enterprise Security Architecture (ESA) Framework is the processes used to plan, allocate and control information security resources.

Whichever architecture you implement, the purpose is to support the business goals of the organization through the use of effective security investment.

Some metrics used to determine if you are successful are:

- Strategic alignment
- Effective risk management
- Resource Management
- Performance measurement

Using these metrics, you can get an understanding about how your security planning is supporting the business goals of the organization.

=======

Contingency planning
prioritization of apps = asset valuation

assessment of threat impact = threat modeling

development of recovery scenarios = risk mitigation

==========
HVAC stands for heating, ventilation, and air-conditioning. Heat can cause extensive damage to computer equipment by causing processors to slow down and stop execution or even cause solder connections to loosen and fail. Excessive heat degrades network performance and causes downtime. Data centers and server rooms need an uninterrupted cooling system.
Generally, there are two types of cooling: latent and sensible. Latent cooling is the ability of the air-conditioning system to remove moisture. This is important in typical comfort-cooling applications, such as office buildings, retail stores, and other facilities with high human occupancy and use. The focus of latent cooling is to maintain a comfortable balance of temperature and humidity for people working in and visiting such a facility. These facilities often have doors leading directly to the outside and a considerable amount of entrance and exit by occupants.
Sensible cooling is the ability of the air-conditioning system to remove heat that can be measured by a thermometer. Data centers generate much higher heat per square foot than typical comfort-cooling building environments, and are typically not occupied by large numbers of people. In most cases, they have limited access and no direct means of egress to the outside of the building except for seldom used emergency exits. Data centers have a minimal need for latent cooling and require minimal moisture removal.
Sensible cooling systems are engineered with a focus on heat removal rather than moisture removal and have a higher sensible heat ratio; they are the most useful and appropriate choice for the data center. Cooling systems are dove tailed into the power supply overhead. If there is a power interruption, this will affect the cooling system. For the computers to continue operation, they need to be cooled. Portable air-conditioning units can be used as a backup in case of HVAC failure but good design should ensure cooling systems are accounted for as backup devices.
=====

smoke detection

Photoelectric and Ionization

There are two main types of smoke detectors: ionization detectors and photoelectric detectors.

A smoke alarm uses one or both methods, sometimes plus a heat detector, to warn of a fire. The devices may be powered by a 9-volt battery, lithium battery, or 120-volt house wiring.

Photoelectric detectors are classified as either beam or refraction. Beam detectors operate on the principle of light and a receiver. Once enough smoke enters the room and breaks the beam of light, the alarm is sounded. The refraction type has a blocker between the light and the receiver. Once enough smoke enters the room, the light is deflected around the beam to the signal. Finally, we have the ionization type detector; these detectors monitor the air around the sensors constantly. Once there is enough smoke in the room, the alarm will sound.
=======

Split knowledge involves encryption keys being separated into two components, each of which does not reveal the other. Split knowledge is the other complementary access control principle to dual control.

In cryptographic terms, one could say dual control and split knowledge are properly implemented if no one person has access to or knowledge of the content of the complete cryptographic key being protected by the two processes.

======================

The three main components of CPTED are:

1) natural access control - the guidance of people entering and leaving a space by the placement of doors, fences, lighting, and even landscaping

2) natural surveillance - the goal is make criminals feel uncomfortable by providing many ways observers could potentially see them

3) natural territorial reinforcement - creates physical designs that emphasize or extend the company's physical sphere of influence so users feel a sense of ownership of that space.

=====================

Cited as a major weakness of WEP, using the same key for encryption as it does for client authentication doomed WEP from the start.

Some of the other WEP weakness are:
- The IV is a 24-bit field, too small to be effective. It is also sent in the clear text portion of a message.
- Identical key streams are produced with the reuse of the same IP for data protection because the IV is short and key streams are repeated after a short period of time.
- Lack of centralized key management and encryption key distribution.
- WEP is based on a password, prone to password cracking attacks.
- Uses RC4 which is a stream cipher and designed to be a one-time cipher not intended for multiple message use. One-time ciphers are never supposed to be reused.

======================

Firewalking is a term used to describe how internal networks can be mapped from outside a firewall protected network by sending crafted ICMP packets with their TTL - Time To Live decremented to the number of hops to the external interface of the external firewall.
The goal is to elicit ICMP Time Exceeded. (Type 11 - Code 0. Technically it's TTL Exceeded.)

Basically, the attacker would traceroute to the border firewall to determine the number of hops (Hop count) to the external interface of the target network. Then he would send ICMP packets with their TTL decremented to that number plus one or more and gather the ICMP time-exceeded packets to map out the internal network.

======================

A Synchronous token generates a one-time password that is only valid for a short period of time. Once the password is used it is no longer valid, and it expires if not entered in the acceptable time frame.

The following answers are incorrect:
Variable callback system. Although variable callback systems are more flexible than fixed callback systems, the system assumes the identity of the individual unless two-factor authentication is also implemented. By itself, this method might allow an attacker access as a trusted user.

Fixed callback system. Authentication provides assurance that someone or something is who or what he/it is supposed to be. Callback systems authenticate a person, but anyone can pretend to be that person. They are tied to a specific place and phone number, which can be spoofed by implementing call-forwarding.

Combination of callback and Caller ID. The caller ID and callback functionality provides greater confidence and auditability of the caller's identity. By disconnecting and calling back only authorized phone numbers, the system has a greater confidence in the location of the call. However, unless combined with strong authentication, any individual at the location could obtain access.

====================
Controls provide accountability for individuals accessing information. Assurance procedures ensure that access control mechanisms correctly implement the security policy for the entire life cycle of an information system.

===================
Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.

Here is a breakdown largely based on explanations provided by Doug Landoll (see forum archive on www.cccure.org). I am reproducing below using my own word and not exactly how Doug explained it:

FIRST: The Lattice

A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label. The pairing could also be a file and its permissions or it could be a process and its integrity level for examples.

SECOND: DAC (Discretionary Access Control)

Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the person they share the file with from further sharing it with other users on the network. Very quickly you lose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control:

Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity level and the categories the object belongs to. The categories are used to implement the Need to Know.

All of the following are forms of Non-Discretionary Access Control:

Role Based Access Control (RBAC)

Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non-Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non-Discretionary Access Control. Non-Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control.

In the same line of taught, you should be familiar with the difference between Explicit permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).
=====================

Continuous authentication is a type of authentication that provides protection against impostors who can see, alter, and insert information passed between the claimant and verifier even after the claimant/verifier authentication is complete. These are typically referred to as active attacks, since they assume that the imposter can actively influence the connection between claimant and verifier. One way to provide this form of authentication is to apply a digital signature algorithm to every bit of data that is sent from the claimant to the verifier. There are other combinations of cryptography that can provide this form of authentication but current strategies rely on applying some type of cryptography to every bit of data sent. Otherwise, any unprotected bit would be suspect. Robust authentication relies on dynamic authentication data that changes with each authenticated session between a claimant and a verifier, but does not provide protection against active attacks. Encrypted authentication is a distracter.

====================

Logon ID should not be job descriptive. The job descriptive logon ID will help attacker to find out powerful account in the system.

Below are the logon ID requirements from the CISA Review Manual:

1. Logon Id should be restricted to provide individual, but not group identification. Never share a password.

2. Default system accounts, such as guest, Administrator and Admin should be renamed whenever technically possible

3. The system should automatically disconnect a logon session if no activity has occurred for a period of time

User Identification Guidelines

There are three essential security characteristics regarding identities: uniqueness,non-descriptiveness, and secure issuance. First and foremost, user identification must be unique so that each entity on a system can be unambiguously identified. Although it is possible for a user to have many unique identifiers, each must be distinctive within an access control environment. In the event there are several disparate access control environments that do not interact, share information, or provide access to the same resources, duplication is possible.

For example, a user’s ID at work may be “mary_t,” allowing her to be identified and authenticated within the corporate infrastructure. She may also have a personal e-mail account with her Internet service provider (ISP) with the user ID of “mary_t.” This is possible because the corporate access control environment does not interact with the ISP’s access control environment. However, there are potential dangers with using the same ID on multiple systems.

Users are prone to duplicating certain attributes, such as passwords, to minimize their effort. If an attacker discovers Mary’s ISP ID and password, he or she may rightly conclude that she is using the same ID and password at work. Therefore, any duplication, although possible in certain circumstances, represents a fundamental risk to the enterprise. User identification should generally be no descriptive and should try as much as possible to disclose as little as possible about the user. The ID should also not expose the associated role or job function of the user. Common practice is to issue user IDs that are a variant of the user’s name, for example, “bsmith” or “bob.smith.” Once this scheme is identified by an attacker it becomes easy to begin enumerating through possible variations on the theme to discover other valid user IDs in the organization. In addition, a person’s job function should never be used as the basis for a user ID. If a user ID were to be named “cfo,” an attacker would be able to focus energy on that user alone based on the assumption that he is the CFO of the company and would probably have privileged access to critical systems. However, this is practiced quite often. It is very common to have user IDs of “admin,” “finance,” “shipment,” “Web master,” or other representations of highly descriptive IDs. The naming of these IDs is voluntary and self-imposed by the organization.

There are some IDs, however, that cannot be easily changed. The most predominant is the username “root.” It is the name given to the administrative account with unlimited access rights on a UNIX system. Everyone, including attackers, knows what the username “root” represents, and it is for this very reason that attaining root’s password is so desirable. Unfortunately, in most UNIX systems, changing the user or masking that role is impossible. In Microsoft operating systems it is possible to change the username of the default “administrator” account (nearly the equivalent of “root” in UNIX) to some other nondescriptive name, and should be considered a best practice.

=========================

Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. It has the following characteristics:

It is secure: it never sends a password unless it is encrypted.

Only a single login is required per session. Credentials defined at login are then passed between resources without the need for additional logins.

The concept depends on a trusted third party €" a Key Distribution Center (KDC). The KDC is aware of all systems in the network and is trusted by all of them.

It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client.

Kerberos introduces the concept of a Ticket-Granting Server/Service (TGS). A client that wishes to use a service has to receive a ticket from the TGS €" a ticket is a time-limited cryptographic message €" giving it access to the server. Kerberos also requires an Authentication Server (AS) to verify clients. The two servers combined make up a KDC.

Within the Windows environment, Active Directory performs the functions of the KDC. The following figure shows the sequence of events required for a client to gain access to a service using Kerberos authentication. Each step is shown with the Kerberos message associated with it, as defined in RFC 4120 €the Kerberos Network Authorization Service (V5)€ .

Kerberos Authentication Step by Step

€¢ Step 1: The user logs on to the workstation and requests service on the host. The workstation sends a message to the Authorization Server requesting a ticket granting ticket (TGT).

€¢ Step 2: The Authorization Server verifies the user€™s access rights in the user database and creates a TGT and session key. The Authorization Sever encrypts the results using a key derived from the user€™s password and sends a message back to the user workstation.

The workstation prompts the user for a password and uses the password to decrypt the incoming message. When decryption succeeds, the user will be able to use the TGT to request a service ticket.

Step 3: When the user wants access to a service, the workstation client application sends a request to the Ticket Granting Service containing the client name, realm name and a timestamp. The user proves his identity by sending an authenticator encrypted with the session key received in Step 2.

Step 4: The TGS decrypts the ticket and authenticator, verifies the request, and creates a ticket for the requested server. The ticket contains the client name and optionally the client IP address. It also contains the realm name and ticket lifespan. The TGS returns the ticket to the user workstation. The returned message contains two copies of a server session key €" one encrypted with the client password, and one encrypted by the service password.

Step 5: The client application now sends a service request to the server containing the ticket received in Step 4 and an authenticator. The service authenticates the request by decrypting the session key. The server verifies that the ticket and authenticator match, and then grants access to the service. This step as described does not include the authorization performed by the Intel AMT device, as described later.

Step 6: If mutual authentication is required, then the server will reply with a server authentication message.

The Kerberos server knows "secrets" (encrypted passwords) for all clients and servers under its control, or it is in contact with other secure servers that have this information. These "secrets" are used to encrypt all of the messages shown in the figure above.

To prevent "replay attacks," Kerberos uses timestamps as part of its protocol definition. For timestamps to work properly, the clocks of the client and the server need to be in synch as much as possible. In other words, both computers need to be set to the same time and date. Since the clocks of two computers are often out of synch, administrators can establish a policy to establish the maximum acceptable difference to Kerberos between a client's clock and server's clock. If the difference between a client's clock and the server's clock is less than the maximum time difference specified in this policy, any timestamp used in a session between the two computers will be considered authentic. The maximum difference is usually set to five minutes.

Note that if a client application wishes to use a service that is "Kerberized" (the service is configured to perform Kerberos authentication), the client must also be Kerberized so that it expects to support the necessary message responses.

Kerberos
=========================
Operational controls are controls over the hardware, the media used and the operators using these resources.

Operational controls are controls that are implemented and executed by people, they are most often procedures.

Backup and recovery, contingency planning and operations procedures are operational controls.

=============

The exclusionary rule is designed to exclude evidence obtained in violation of a criminal defendant's Fourth Amendment rights. The Fourth Amendment protects against unreasonable searches and seizures by law enforcement personnel. If the search of a criminal suspect is unreasonable, the evidence obtained in the search will be excluded from trial.

The exclusionary rule is a court-made rule. This means that it was created not in statutes passed by legislative bodies but rather by the U.S. Supreme Court. The exclusionary rule applies in federal courts by virtue of the Fourth Amendment. The Court has ruled that it applies in state courts although the due process clause of the Fourteenth Amendment.(The Bill of Rights—the first ten amendments— applies to actions by the federal government. The Fourteenth Amendment, the Court has held, makes most of the protections in the Bill of Rights applicable to actions by the states.)

The exclusionary rule has been in existence since the early 1900s. Before the rule was fashioned, any evidence was admissible in a criminal trial if the judge found the evidence to be relevant. The manner in which the evidence had been seized was not an issue. This began to change in 1914, when the U.S. Supreme Court devised a way to enforce the Fourth Amendment. In Weeks v. United States, 232 U.S. 383, 34 S. Ct. 341, 58 L. Ed. 652 (1914), a federal agent had conducted a warrantless search for evidence of gambling at the home of Fremont Weeks. The evidence seized in the search was used at trial, and Weeks was convicted. On appeal, the Court held that the Fourth Amendment barred the use of evidence secured through a warrantless search. Weeks's conviction was reversed, and thus was born the exclusionary rule.

The best evidence rule concerns limiting potential for alteration. The best evidence rule is a common law rule of evidence which can be traced back at least as far as the 18th century. In Omychund v Barker (1745) 1 Atk, 21, 49; 26 ER 15, 33, Lord Harwicke stated that no evidence was admissible unless it was "the best that the nature of the case will allow". The general rule is that secondary evidence, such as a copy or facsimile, will be not admissible if an original document exists, and is not unavailable due to destruction or other circumstances indicating unavailability.

The rationale for the best evidence rule can be understood from the context in which it arose: in the eighteenth century a copy was usually made by hand by a clerk (or even a litigant). The best evidence rule was predicated on the assumption that, if the original was not produced, there was a significant chance of error or fraud in relying on such a copy.

The hearsay rule concerns computer-generated evidence, which is considered second-hand evidence.

Hearsay is information gathered by one person from another concerning some event, condition, or thing of which the first person had no direct experience. When submitted as evidence, such statements are called hearsay evidence. As a legal term, "hearsay" can also have the narrower meaning of the use of such information as evidence to prove the truth of what is asserted. Such use of "hearsay evidence" in court is generally not allowed. This prohibition is called the hearsay rule.

For example, a witness says "Susan told me Tom was in town". Since the witness did not see Tom in town, the statement would be hearsay evidence to the fact that Tom was in town, and not admissible. However, it would be admissible as evidence that Susan said Tom was in town, and on the issue of her knowledge of whether he was in town.

Hearsay evidence has many exception rules. For the purpose of the exam you must be familiar with the business records exception rule to the Hearsay Evidence. The business records created during the ordinary course of business are considered reliable and can usually be brought in under this exception if the proper foundation is laid when the records are introduced into evidence. Depending on which jurisdiction the case is in, either the records custodian or someone with knowledge of the records must lay a foundation for the records. Logs that are collected as part of a document business process being carried at regular interval would fall under this exception. They could be presented in court and not be considered Hearsay.

Investigation rule is a detractor.

====================

In physical security fail secure is same fail safe is fail open

================

Active monitors interpret DoS and read-only memory (ROM) BIOS calls, looking for malware like actions. Active monitors can be problematic because they cannot distinguish between a user request and a program or a malware request. As a result, users are asked to confirm actions, including formatting a disk or deleting a file or set of files.

For CISA exam you should know below mentioned different kinds of malware Controls

A. Scanners Look for sequences of bit called signature that are typical malware programs.

The two primary types of scanner are

1. Malware mask or Signatures - Anti-malware scanners check files, sectors and system memory for known and new (unknown to scanner) malware, on the basis of malware malware masks or signatures. Malware masks or signature are specific code strings that are recognized as belonging to malware. For polymorphic malware, the scanner sometimes has algorithms that check for all possible combinations of a signature that could exist in an infected file.

2. Heuristic Scanner - Analyzes the instructions in the code being scanned and decide on the basis of statistical probabilities whether it could contain malicious code. Heuristic scanning result could indicate that malware may be present, that is possibly infected. Heuristic scanner tend to generate a high level false positive errors (they indicate that malware may be present when, in fact, no malware is present). Scanners examines memory disk- boot sector, executables, data files, and command files for bit pattern that match a known malware. Scanners, therefore, need to be updated periodically to remain effective.

B. Immunizers - Defend against malware by appending sections of themselves to files - sometime in the same way Malware append themselves. Immunizers continuously check a file for changes and report changes as possible malware behavior. Other type of Immunizers are focused to a specific malware and work by giving the malware the impression that the malware has already infected to the computer. This method is not always practical since it is not possible to immunize file against all known malware.

C. Behavior Blocker - Focus on detecting potential abnormal behavior such as writing to the boot sector or the master boot record, or making changes to executable files. Blockers can potentially detect malware at an early stage. Most hardware based anti-malware mechanism are based on this concept.

D. Integrity CRC checker - Compute a binary number on a known malware free program that is then stored in a database file. The number is called Cyclic Redundancy Check (CRC). On subsequent scans, when that program is called to execute, it checks for changes to the file as compare to the database and report possible infection if changes have occurred. A match means no infection; a mismatch means change in the program has occurred. A change in the program could mean malware within it. These scanners are effective in detecting infection; however they can do so only after infection has occurred. Also, a CRC checker can only detect subsequent changes to files, because they assume files are malware free in the first place. Therefore, they are ineffective against new files that are malware infected and that are not recorded in the database. Integrity checker take advantage of the fact that executable programs and boot sectors do not change often, if at all.

===========================

EMO - Emergency Management Organization

The emergency management organization (EMO) is formed to provide both a formal response process for management; and on-site coverage, support and expertise during large-scale emergencies. The EMO ensures that all locations and operating areas will receive an appropriate, coordinated response in the event of a serious outage of any type.

EOC - Emergency Operations Center

The organizational emergency operations center (EOC) has been established to provide a location, equipped with all of the necessary resources to manage the organization resumption process whenever the EMO is activated.
===================
Operational controls are put in place to improve security of a particular system (or group of systems). They often require specialized expertise and often rely upon management activities as well as technical controls. Implementing dual control and making sure that you have more than one person that can perform a task would fall into this category as well

====================
Intrusion detection
Information, as collected and interpreted through analysis, is key to your decisions and actions while executing response procedures. This first analysis will provide information such as what attacks were used, what systems and data were accessed by the intruder, what the intruder did after obtaining access and what the intruder is currently doing (if the intrusion has not been contained).

The next step is to communicate with relevant parties who need to be made aware of the intrusion in a timely manner so they can fulfil their responsibilities.

Step three is concerned with collecting and protecting all information about the compromised systems and causes of the intrusion. It must be carefully collected, labelled, catalogued, and securely stored.

Containing the intrusion, where tactical actions are performed to stop the intruder's access, limit the extent of the intrusion, and prevent the intruder from causing further damage, comes next.

Since it is more a long-term goal, eliminating all means of intruder access can only be achieved last, by implementing an ongoing security improvement process.

==================

If you are "retrofitting" that means you are adding to an existing database management system (DBMS). You could go back and redesign the entire DBMS but the cost of that could be expensive and there is no telling what the effect will be on existing applications, but that is redesigning and the question states retrofitting. The most cost effective way with the least effect on existing applications while adding a layer of security on top is through a trusted front-end.

Clark-Wilson is a synonym of that model as well. It was used to add more granular control or control to database that did not provide appropriate controls or no controls at all. It is one of the most popular model today. Any dynamic website with a back-end database is an example of this today.

Such a model would also introduce separation of duties by allowing the subject only specific rights on the objects they need to access.

The following answers are incorrect:

trusted back-end. Is incorrect because a trusted back-end would be the database management system (DBMS). Since the question stated "retrofitting" that eliminates this answer.
==================
DSS emphasizes flexibility in the decision–making approach of users. It is aimed at solving less structured problems, combines the use of models and analytic techniques with traditional data access and retrieval functions and supports semi–structured decision–making tasks.

DSS is sometimes referred to as the Delphi Method or Delphi Technique:

The Delphi technique is a group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result of a particular threat will be. This avoids a group of individuals feeling pressured to go along with others,„¢ thought processes and enables them to participate in an independent and anonymous way.

Each member of the group provides his or her opinion of a certain threat and turns it in to the team that is performing the analysis.

The results are compiled and distributed to the group members, who then write down their comments anonymously and return them to the analysis group.

The comments are compiled and redistributed for more comments until a consensus is formed. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

Here is the ISC2 book coverage of the subject:

One of the methods that uses consensus relative to valuation of information is the consensus/modified Delphi method. Participants in the valuation exercise are asked to comment anonymously on the task being discussed. This information is collected and disseminated to a participant other than the original author. This participant comments upon the observations of the original author. The information gathered is discussed in a public forum and the best course is agreed upon by the group (consensus).
===================

A protection domain consists of the execution and memory space assigned to each process. The purpose of establishing a protection domain is to protect programs from all unauthorized modification or executional interference. The security perimeter is the boundary that separates the

Trusted Computing Base (TCB) from the remainder of the system. Security labels are assigned to resources to denote a type of classification. Abstraction is a way to protect resources in the fact that it involves viewing system components at a high level and ignoring its specific details, thus performing information hiding.

=================

Mitigate Buffer overflow
By closely controlling what software gets installed you can heavily mitigate the threat. Here are a few ways you can control what software gets installed:

1. Enable computer security policies which restrict it to privileged users
2. Ensure ALL users use the least privileged accounts possible for their jobs.
3. Run a proxy server that blocks known malicious websites.
4. Run secure operating systems and browsers which are locked down.

============

To check input accuracy, data validation and verification checks should be incorporated into appropriate applications.

Character checks compare input characters against the expected type of characters, such as numbers or letters. This is sometimes also known as sanity checking.

Range checks verify input data against predetermined upper and lower limits.

Relationship checks compare input data to data on a master record file.

Reasonableness checks compare input data to an expected standard—another form of sanity checking.

Transaction limits check input data against administratively set ceilings on specified transactions.

==============

Nonessential	30 Days
Normal	7 Days
Important	72 Hours
Urgent	24 Hours
Critical	Minutes to hours